BOURNEMOUTH UNIVERSITY

DOCTORAL THESIS

Digital Forensic Readiness in Smart, Circular Cities

by:
Amalia DAMIANOU

Supervisor:
Prof. Vasilios KATOS

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in the

Bournemouth University Cyber Security Research Group-BUCSR
Department of Computing & Informatics

June 27, 2022

Declaration of Authorship

I, Amalia DAMIANOU, declare that this thesis titled, "Digital Forensic Readiness in Smart, Circular Cities" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:Amalia Damianou

Date:

"Somewhere, something incredible is waiting to be known."

Carl Sagan

Abstract

Cities all around the world strive to evolve in order to respond to the upcoming challenges that the increase of population brings. The integration of technological solutions addresses these challenges and facilitates citizens' needs. The smart cities concept refers to the technological evolution of cities for improving services and quality of life by integrating innovative technological paradigms. Furthermore, sustainability plays a key role for preserving the balance within an advanced urban environment. To this end, Circular Economy, referring to the economic model where everything has value and nothing is wasted, is a promising paradigm. The coexistence of technological enablers and Circular Economy, and the adoption of a maturity model designate the technological roadmap for a city's technological advancement. On the other hand, the increase of technology integration and the employment of novel and innovative technological paradigms come along with the increase of vulnerability exposure of a city. The increase in the vulnerability exposure of a city, the maturity level that a city has achieved, when combined with various dimensions, such as behavioural, cultural, and economic variables, increase the need for a well-established incident response plan that should be deployed and applied. In addition, heterogeneity of smart cities, and the lack of standardised digital forensic investigation techniques, designate the demand for a predefined digital forensic readiness framework.

In this thesis, we shed light on the optimisation of a vulnerability-driven incident response process and the deployment of a digital forensic readiness framework, depending on the maturity level that a city has achieved. In a context of a smart city, a digital forensic readiness framework - and consequently the underlying incident response plan - is dependent upon two aspects, the maturity level that a city has achieved, as well as a consensus of the different stakeholders who will be involved in executing the incident response playbooks.

We commence the research by conducting an investigation of the evolution of cities during the last decades, and the presentation of Circular Economy paradigm, as well as technological enablers that have been employed in smart cities case studies. Furthermore, we adopt, adapt, and present a maturity model, from *Ideal Cities project* (Ideal-Cities, 2018). Also, we investigate novel and innovative technological paradigms, such as IoT and DLT, in smart city concepts. We present a novel smart city architecture that relies on Blockchain, where IoT devices act as Blockchain nodes, employing Edge Computing for storing ledger. The proposed architecture is critically assessed by comparing it against existing and established similar architectures. In addition, we focus on Intelligent Transportation Systems, identifying potential attack vectors, categorising them into three tiers, Devices, Network, and DLT layers, and applying DREAD threat model for their evaluation. Moreover, we deploy a DLT and IoT Proof of Concept that enhance the performance of IoT devices. In addition, we conduct an empirical vulnerability-driven analysis based on existing vulnerabilities datasets. For our research to be facilitated, we extend and enrich the initial dataset with quantitative research data from independent studies. Reflecting

on the results of the aforementioned analysis, we identify the necessity for the deployment of a digital forensic readiness framework, employed by local authorities, service providers, and stakeholders.

Furthermore, a digital forensic readiness playbook is introduced, allowing and guiding local authorities, service providers, and stakeholders to handle pre-incident phase, for identifying, collecting, and preserving digital evidence and responding faster during the post-incident phase than usually, by starting digital forensic investigation as soon as possible, after the incident detection, obtaining available digital evidence in advance. The proposed DFRP has been created taking into consideration the principles of the digital forensic readiness requirements, based on ISO/IEC 27043:2015. The proposed approach has been evaluated by adopting a qualitative macroeconomics approach in order to assess the support of the CE paradigm by the proposed DFRP.

Overall, our findings highlight the needs for the deployment of a crowdsourced-driven digital forensic readiness framework, adopted by all the members and parties of a smart city, always taking into consideration the maturity level that it has achieved. In this research, we introduce the processes that should be followed by data owners and custodians, before and after an incident, through the use of a playbook. In addition, we identify the importance of integrity preservation of the Chain of Custody, and collected digital evidence, keeping in mind that the integrity of digital evidence objects is essential during all the digital forensic readiness framework stages, from the identification of digital evidence sources and the acquisition, until the final presentation as artifacts at a court of law. Thus, Blockchain along with smart contracts and NFTs paradigms are proposed for illustrating their contribution to the digital forensic readiness framework, by preserving Chain of Custody integrity, providing some of fundamental build in features, such as the immutability, transparency, non-repudiation, and resilience.

Acknowledgements

I would first like to thank my supervisory team, Professor Vasilis Katos and Dr Marios Angelopoulos for their support, guidance and advice throughout the PhD journey and for motivating me during our collaboration. I also want to thank my lab colleagues for their support during all this time. I was privileged to work with a team that it was truly there for me.

I owe a huge thank to Amir Khan and Paul-David Jarvis for their technical support and our collaboration during this research.

I would like also to thank my *IDEAL CITIES* project colleagues for their support and for the collaboration that we had during the last 3 years, gaining a lot of experience and knowledge.

My greatest thanks is reserved for my family, my mother Vasiliki and my sister Ioanna, Christos and my friends for keeping me sane through this journey, with their continued support, patience and love. Thank you all so much!

Contents

Declaration of Authorship iii

Abstract vii

Acknowledgements ix

1 Introduction 1
- 1.1 Thesis motivation . . . 1
- 1.2 Novel aspects of the thesis . . . 4
- 1.3 Research Question . . . 4
- 1.4 Thesis Structure . . . 5
- 1.5 Related Publications . . . 8

2 Methodology 9
- 2.1 Introduction . . . 9
- 2.2 Research Methodology . . . 9
  - 2.2.1 Literature review . . . 12
  - 2.2.2 Datasets . . . 13
  - 2.2.3 Analysis and evaluation . . . 13
- 2.3 Concluding Summary . . . 13

3 Data-driven Circular Economy in Smart Cities 15
- 3.1 Introduction . . . 15
- 3.2 Circular Economy . . . 15
- 3.3 Data-driven Circular Economy . . . 16
- 3.4 Business Models of Circular Economy . . . 17
  - 3.4.1 Business Models . . . 18
  - 3.4.2 Circular Supply Chain . . . 19
  - 3.4.3 Recovering and Recycling . . . 19
  - 3.4.4 Product life-extension . . . 20
  - 3.4.5 Sharing Model . . . 20
  - 3.4.6 Product as a service . . . 20
- 3.5 Smart Cities . . . 20
  - 3.5.1 Cyber-Physical Systems and Socio-Technical Systems . . . 23
  - 3.5.2 Data-driven Circular Economy in an Urban Ecosystem- Circular Cities . . . 24
- 3.6 Smart Cities Use Cases . . . 27
  - 3.6.1 Amsterdam . . . 27
  - 3.6.2 Copenhagen . . . 28
  - 3.6.3 Barcelona . . . 28
- 3.7 Technological Enablers . . . 28
  - 3.7.1 IoT . . . 29
    - IoT Security and Privacy Challenges . . . 29

3.7.2 Crowdsourcing and Crowdsensing . . . 30
3.7.3 Cloud Computing . . . 31
Cloud Security and Privacy Challenges . . . 31
3.7.4 Edge Computing . . . 32
Edge Computing Security and Privacy Challenges . . . 32
3.7.5 5G . . . 33
Millimetre Waves . . . 34
Small Cell . . . 34
Massive MIMO . . . 34
Beamforming . . . 34
Full Duplex . . . 34
5G Security and Privacy Challenges . . . 34
3.7.6 Blockchain . . . 35
3.7.7 Blockchain Features . . . 36
Blockchain Security and Privacy Challenges . . . 37
3.7.8 Blockchain Vulnerabilities . . . 37
51% Vulnerability . . . 37
Transaction Privacy Leakage . . . 38
Smart Contracts . . . 38
3.7.9 Big Data . . . 39
3.7.10 Artificial Intelligence (AI) . . . 40
Artificial Intelligence Security and Privacy Challenges . . . 40
3.7.11 Machine Learning . . . 40
3.7.12 Robotics . . . 41
3.7.13 SDN & NFV . . . 42
3.7.14 Machine To Machine (M2M) Communication . . . 42
3.7.15 Human To Machine (H2M) Communication . . . 42
3.8 Chapter Summary . . . 43

4 Use Cases **45**
4.1 Introduction . . . 45
4.2 Superblocks . . . 46
4.2.1 Related Work . . . 46
4.2.2 Software Defined Superblocks . . . 46
4.2.3 Use Case . . . 47
4.2.4 Example Pattern . . . 49
4.3 Interconnected Healthcare System . . . 50
4.3.1 Use Case . . . 50
4.3.2 The Incident . . . 51
4.4 Energy Factory . . . 51
4.4.1 Use Case . . . 51
4.5 Healthcare System Breach . . . 52
4.5.1 Use Case . . . 52
4.5.2 The Incident . . . 53
4.6 Discussion . . . 54
4.7 Chapter Summary . . . 55

5 Technological Integration within Cities- An Architecture for Blockchain over Edge-enabled IoT for Smart Circular Cities 57
5.1 Introduction . . . 57
5.2 Related Work . . . 58
5.3 Model and Architecture . . . 60
5.3.1 Mining Process . . . 61
5.3.2 Comparison . . . 62
5.4 Discussion . . . 63
5.5 Chapter Summary . . . 65

6 The adoption of Distributed Ledger Technologies and IOTA for Threat Modelling of IoT Systems 67
6.1 Introduction . . . 67
6.2 State of the Art . . . 68
6.2.1 Intelligent Transportation Systems Risk Assessment . . . 68
6.3 Threat Modelling for Intelligent Transportation Systems using DLTs . . 70
6.4 An IoT and DLT Proof of Concept for Intelligent Transportation System 76
6.4.1 Comparison to a Real World Use Case . . . 78
6.4.2 Applying the ITS Threat Model . . . 78
6.5 Chapter Summary . . . 79

7 Vulnerabilities Exposure Driven Intelligence in Smart, Circular Cities 81
7.1 Introduction . . . 81
7.2 Architecture and threat landscape of smart cities . . . 82
7.3 Smart City threat landscape . . . 83
Security Incident . . . 84
Attack . . . 84
Vulnerability . . . 84
Threat . . . 84
7.3.1 Interdependency and Heterogeneity as Cybersecurity Threats Landscape . . . 85
7.4 The CVSS scoring system . . . 85
7.4.1 Advantages and Limitations of CVSS . . . 86
7.5 A Smart City Maturity Level and Vulnerability Exposure Profile . . . 88
7.5.1 Datasets - limitations of research . . . 89
7.5.2 Analysis and Findings . . . 91
Scope: Country . . . 92
Scope: City . . . 93
Scope: Human aspects . . . 97
7.6 Discussion . . . 100
7.7 Chapter Summary . . . 100

8 Digital Forensic Readiness Framework 101
8.1 Introduction . . . 101
8.2 Incident Response . . . 101
8.2.1 Incident Response Stages . . . 102
8.3 Digital Forensics . . . 104
8.3.1 A brief description of the digital forensics process . . . 105
8.3.2 Digital Forensic Readiness (DFR) . . . 107
8.3.3 Discussion . . . 112

8.3.4 Validation of Blockchain feasibility for digital forensic readiness framework . . . 114
8.3.5 Assets Identification and Digital Forensic Readiness Framework 114
8.4 Non Fungible Token (NFT) . . . 116
8.4.1 Ethereum . . . 117
8.4.2 EOS . . . 117
Smart Contracts . . . 118
8.4.3 EOS vs Ethereum: The Comparison . . . 119
Scalability . . . 119
Transaction Cost . . . 119
Consensus Mechanism . . . 119
8.5 Proxy Re-encryption(PRE) . . . 120
8.6 Digital Forensic Readiness Framework for Smart Circular Cities . . . 122
8.6.1 Digital Forensic Readiness Playbook (DFRP) . . . 122
8.6.2 Digital Evidence Object . . . 122
8.6.3 Core and Extended Teams and Roles . . . 122
8.6.4 Smart City Critical Sectors and Infrastructures . . . 126
Energy Sector . . . 126
Water and Wastewater . . . 127
Waste Management . . . 127
Communications . . . 128
Healthcare . . . 128
Transportation and Mobility . . . 128
Public Safety . . . 129
Financial Services . . . 129
8.6.5 Digital Forensic Readiness Playbook (DFRP) for Smart Circular Cities . . . 129
8.6.6 Digital Evidence Object Collection . . . 136
8.6.7 Digital Evidence Objects Preservation . . . 138
8.6.8 Post-Incident Phase and Transmission of Digital Evidence Objects . . . 139
8.6.9 Digital Evidence Deletion . . . 141
Soft deletion . . . 143
Hard Deletion . . . 144
8.7 Evaluation . . . 147
8.8 Chapter Summary . . . 150

9 Conclusions **153**
9.0.1 Novel aspects of the thesis . . . 153
9.1 Evaluation . . . 153
9.1.1 **Aim 1** . . . 153
9.1.2 **Aim 2** . . . 154
9.1.3 **Aim 3** . . . 155
9.2 Challenges and Limitations . . . 157
9.3 Future Work . . . 159
9.3.1 A vulnerability integrated model development in smart, circular cities . . . 159
9.3.2 Introduction of Environmental Score for the assessment of identified vulnerabilities . . . 159
9.3.3 Deployment and implementation of the Proposed Digital Forensic Readiness Framework . . . 160

9.3.4 Formal validation of proposed Readiness Framework algorithms 160
9.3.5 Empirical estimation of supply and demand curves 160
9.3.6 How acceptable would be a playbook by stakeholders - user/human acceptance 160
9.4 Concluding Summary 161

References **163**

A Performance Evaluation of PoC **179**
A.1 Performance Evaluation 179

List of Figures

1.1 PhD Overview 8

2.1 Methodology Overview 12

3.1 CE system diagram (Ellen-MacArthur-Fundation (*Introdution to Circular Economy*)) 17
3.2 The CE Cycle (Ideal-Cities (2018)) 18
3.3 Circular economy business model impact in the linear economy (OECD (2019)) 19
3.4 Coexistence of Cyber-physical and Socio-technical Systems within a smart city environment (Ideal-Cities (2018)) 24
3.5 A maturity model for a smart, circular city (adapted from Ideal-Cities (2018)) 26
3.6 How Blockchain Works (Baru (2018)) 36
3.7 Block sequence in the chain 36

4.1 Networks scheme, current and future. based on superblocks. (*Agencia de Ecología Urbana de Barcelona* (2012)) 47
4.2 Software Defined Superblock Orchestration System Model 48
4.3 Overview of Hypothetical Scenario 3 (adapted from Bit_of_Hex (2019)) 54

5.1 Employed Edge Computing as storage enabler of the Blockchain ledger for IoT networks in a smart, circular city 61
5.2 Edge Computing for Mobile Blockchain (Xiong et al. (2017)) 64

6.1 PoC architecture presented into separate tiers (a top-down perspective) 77
6.2 The interaction between the microcontrollers and message broker . . . 77
6.3 Facilitation of an emergency vehicle demonstrating the ideal route from point A to point B 79

7.1 A high level smart city architecture (adapted from Neshenko et al. (2020)) 83
7.2 Vulnerability impact, dependent on the city maturity level (adapted from Ideal-Cities (2018)) 89
7.3 Pairwise comparisons of the four city classes 94
7.4 Hierarchical clustering of cities having a smart and CE agenda (class:`both`) 97

8.1 Readiness Processes Groups ISO/IEC27043 (2015) 108
8.2 Readiness Processes- Planning and Implementation processes groups (adapted from ISO/IEC-27043 (2015)) 109
8.3 Readiness Processes-Initialisation and Acquisitive processes groups (adapted from ISO/IEC-27043 (2015)) 110
8.4 Readiness Processes- Investigative processes group (adapted from ISO/IEC-27043 (2015)) 111

8.5 Is Blockchain an appropriate technical solution for solving an issue? (Lone and Mir (2019); Wüst and Gervais (2017)) . . . 115
8.6 Overview of EOS System Architecture (Xu et al. (2018)) . . . 118
8.7 Main entities and interactions in PRE, (adapted by (Nuñez, Agudo, and Lopez (2017))) . . . 121
8.8 Interdependencies between critical infrastructures (Guthrie and Konaris (2012)) . . . 127
8.9 Identification and preparation of digital forensic readiness roles . . . 130
8.10 Definition of digital evidence sources & risk factors . . . 131
8.11 Definition of digital evidence type, potential compromised evidence sources, critical city sectors, & maturity level . . . 132
8.12 Pre-incident digital forensic readiness phase . . . 133
8.13 Digital Evidence Preservation . . . 133
8.14 Post-incident digital forensic readiness phase . . . 134
8.15 dNFT ownership transmission for digital and physical evidence objects (adapted from Singh (2019)) . . . 142
8.16 Deployed Digital Forensic Readiness algorithms and their employment based on the city's maturity level . . . 146
8.17 Demand of Incident Response technologies . . . 148
8.18 Supply of IR technologies . . . 149
8.19 The overall equilibrium . . . 149
8.20 The effect of crowdsourcing . . . 150

9.1 Requirements and Proposed Technologies for the deployment of a digital forensic readiness framework . . . 157

A.1 Overview of connected devices . . . 179
A.2 The MQTT messages queue that are published and subscribed . . . 180
A.3 1 hour time slot capture of messages sent from IoT devices to Tangle . 180
A.4 A 10-minute time slot capture of a message sent from an IoT device to the Tangle . . . 180

List of Tables

3.1 Dimensions of a smart city (Chourabi et al. (2012)) 23

6.1 The DREAD threat rating scheme (Huq, Vosseler, and Swimmer (2017)) 71
6.2 Identified attack vectors over the device tier and DREAD evaluation. . 72
6.3 Identified attack vectors over network tier and the DREAD evaluation 73
6.4 Identified attack vectors over DLT tier and the DREAD evaluation . . . 74

7.1 Dataset description 91
7.2 Country regression model 92
7.3 Regression model 1 95
7.4 Regression model 2 95
7.5 Factor Analysis (loadings) of top 20 cities with the most potential vulnerabilities 98
7.6 Weakness profile per city class 99
7.7 Backward regression results 99

9.1 Employed technologies for addressing digital forensics investigation requirements 156

List of Abbreviations

CE	Circular Economy
CPS	Cyber-Physical System
STS	Socio-Technical System
DLT	Distributed Ledger Technology
ASVS	Application Security Verification Standard
ICT	Information and Communication Technology
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
WSN	Wireless Sensor Network
DRL	Deep Reinforcement Learning
RAS	Robotics and Autonomous System
M2M	Machine-to-Machine
H2M	Human-to-Machine
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
RDP	Remote Desktop Protocol
CPU	Central Processing Unit
DFR	Digital Forensic Readiness
OCTAVE	Operationally Critical, Threat, Asset and Vulnerability Evaluation
SEI	Software Engineering Institute
GDPR	General Data Protection Regulation
TTP	Trusted Third Party
CVE	Common Vulnerabilities & Exposure
CVSS	Common Vulnerability Scoring System
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CWE	Common Weakness Enumeration
cpe	common platform enumeration
capec	common attack pattern enumeration & classification
ENISA	European Union Agency for Cyber Security
MB	Memory Buffer
IS	Improper Synchronisation
NIST	National Institute of Standards & Technology
PLC	Programmable Logic Controller
NID	Network Intrusion Detection
HAN	Home Area Network
PAN	Personal Area Network
GSM	Global System for Mobile Communications
OMAP	Open Multimedia Applications Platform
ACC	Adaptive Cruise Control
MQTT	MQ Telemetry Transport
NFT	Non- Fungible Token

CoC	Chain of Custody
IoT	Internet of Things
SM	Security Manager
MM	Manufacturer Manager
PM	Products Manager
POMS	Product Ownership Management System
MIMO	Multiple input multiple output
SDN	Software Defined Network
NFV	Network Functions Virtualisation
QoS	Quality of Service
NVD	National Vulnerability Database
GDP	Gross Domestic Product
GCI	Global Cybersecurity Index
VIF	Variable Inflation Factor
IMD	Index of Multiple Deprivation
PoW	Proof of Work
PoET	Proof of Elapsed Time
DPoS	Delegated Proof of Stake
PoS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
AI	Artificial Intelligence
CAN	Controller Area Network
LAN	Local Area Network
WLAN	Wireless Local Area Network
LPWAN	Low Power Wide Area Networks
PoC	Proof of Concept
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
XSS	Cross-site scripting
OTA	Over The Air
DDoS	Distributed Denial of Service
VM	Virtual Machine
CiM	Cities in Motion
ITS	Intelligent Transportation System
NOC	Network Operation Centre
SOC	Security Operation Centre
VPN	Virtual Private Network
TOR	The Onion Router
CNI	Critical National Infrastructure
CII	Critical Information Infrastructure
dNFT	distributed Non- Fungible Token
IDPS	Intrusion Detection and Prevention System
SIEM	Security Information and Event Management
OS	Operating System
DFRP	Digital Forensic Readiness Playbook
MAC	Media Access Control
SME	Scanning Made Easy
TTP	Third Trusted Part
CLI	Command Line Interface
PRE	Proxy Re-encryption
KeyGen	Key Generation

ReKeyGen	Re-encryption Key Generation
Enc	Encryption
ReEnc	Re-encryption
Dec	Decryption
DFIF-IoT	Digital Forensic Investigation Framework for IoT
SEM	Structured Equation Modelling
DFRF	Digital Forensic Readiness Framework
CTI	Customer Type Indicator

to my mother, Vasiliki
to my sister, Ioanna

Chapter 1

Introduction

1.1 Thesis motivation

Urbanisation has been consistently increasing over the last decades (Caragliu and Del Bo (2012)). Such unprecedented concentration of people within urban environments raises concerns regarding their living conditions, traffic air and noise pollution, the increased generation and accumulation of rubbish, and so forth. As such, it has become imperative to develop and adopt efficient solutions in order to address sustainability challenges and it is argued that Information and Communication Technologies will play a key role in addressing such challenges. During the last years, the transition from a traditional to a technologically advanced city has come into the spotlight, although this concept is not a new one. The International Telecommunication Union (ITU) has captured more than 100 definitions for describing a smart city concept (International-Telecommunication-Union (2014)). In addition, the term *smart* is not the only one that describes urban environments which employ technological enablers. These terms include *wired city, connected city, intelligent city, digital city*, and so forth (Mohanty, Choppali, and Kougianos (2016)). Undoubtedly, Information and Communication Technologies have substantially contributed to the development and modernisation of many city sectors such as energy, healthcare, transportation, to name a few. Paradigms like IoT, Big Data, Cloud and Edge Computing and Distributed Ledger Technologies (DLT), such as Blockchain, have transformed the way in which people communicate, exchange ideas, travel, work, take their medication and pay their bills. In addition to these definitions, current research not only focuses on defining the dimensions that characterise cities as smart, but also measures the level of achievement of these dimensions, which are captured and described under a maturity model.

In general, a smart city concept refers to the adoption of technological enablers by an urban environment for the quality of services that a city provides and the quality of life of citizens and visitors to be improved. According to Mohanty, Choppali, and Kougianos (2016), most of the smart cities projects consider four main attributes, namely sustainability, quality of life, smartness, and urbanisation (Silva, Khan, and Han (2018)). Sustainability is related to the ability to maintain the balance of a system, such as a city in our case, while it serves and performs various operations. Sustainability is one of the main goals that a smart city must address and it is considered as one of the basic attributes, not only of the development of smart cities but, of urban environments in general. The need for sustainability fuels the development of smart cities and the adoption of new and innovative solutions. There are major challenges that come along with the rise of urbanisation and include waste management, air and noise pollution, adequacy of resources, traffic issues, citizens' health and mental issues, transportation, and so forth. The adoption of technological enablers on a city-wide scale addresses urbanisation challenges for sustainability

to be achieved. In addition, research regarding the correlation between urbanisation and smart cities (Silva, Khan, and Han (2018) and British-Standards-Institution (2014)), concludes that the adoption of ICT has a positive influence on urban wealth (Caragliu and Del Bo (2012)).

From a system perspective, a smart city may be considered as a system of systems, comprised by cyber-physical (CPS) and socio-technical (STS) systems that cover physical devices, city's ICT infrastructure services, and users or human assets, which interact between each other through the cyber plane (see figure 3.4).

A smart city should be considered as the sustainability epitome since any deviation from this would entertain scenarios of dystopian futures. There is a requirement to develop a suitable agenda and accompanied business models, since sustainability is one of the main business and societal drivers for transforming a city into a smart one. The Circular Economy (CE) paradigm is considered as the sustainability approach, whereas ICT may provide the means. The Circular Economy term describes the production and consumption model where every asset has value and none is wasted. As such, assets, such as devices, materials, services, even digital assets, are not disposed of after the first usage, but they are used again, for various purposes that may facilitate different services. The main goal of the Circular Economy paradigm is to maintain assets' utility without wasting new resources before the end of their life cycle by smartly designing them so as to be used again and again for various purposes, instead of creating new products (Ideal-Cities (2018)). The Circular Economy concept was first introduced in the late 1970s (Ellen-MacArthur-Fundation (*Introdution to Circular Economy*)), but has evolved over the years and received a considerable amount of attention nowadays. The coexistence of ICT and Circular Economy can facilitate the extended usage of assets within an environment, providing valuable information regarding their location, condition and performance both in real-time and over time. According to the Ellen MacArthur Foundation, *"A Circular Economy is restorative and regenerative by design, and which aims to keep products, components, and materials at their highest utility and value at all time. It distinguished between technical and biological cycles as an attempt to minimise leakage and wastage"* (Morlet et al. (2016a)). The management of finite resources and assets within a data-driven CE ecosystem is coordinated by data flows. Since data is considered as an asset of high value also reinforced by Clive Humby, who back in 2006 coined the phrase "*data is the new oil*" Olowononi, Rawat, and Liu (2020) to emphasise how valuable data is, it can be seen that CE would need to be data-enabled or data-driven, to be able to deliver what it evangelises.

For the needs of this research the smart city maturity model as described in *IDEAL CITIES* project (Ideal-Cities (2018)) has been adopted, which indicates the technological roadmap for a city adopting a CE agenda. This specifies four levels, each of which indicates the technological and data-driven circularity integration within an urban environment. The four levels of the maturity model, from the lowest to the highest, are the *Instrumented, Connected, Smart* and *Responsive* level. Since every level of maturity indicates different level of technological integration, it is apparent that reaching the Responsive maturity level requires higher connectivity and integration with software services that are delivered across the whole vertical to be achieved. At the same time, technological integration may result to a potential increment of vulnerabilities and risks, especially those related to cybersecurity. As such, the impact of the exploitation of a vulnerability at a particular maturity level differs between the four levels, carrying a larger amount of risk at higher levels of maturity and a smaller at a lower maturity level. The impact of a given vulnerability may differ among the maturity levels. To investigate this claim, a quantitative

vulnerability assessment was conducted using the Common Vulnerability Scoring System (CVSS) (FIRST (2020), Chandramoull et al. ("Common Vulnerability Scoring System")), where the vulnerability severity may need to be adjusted and subject to the so-called environmental variable. Addressing citizens' needs brings challenges to the way in which cities fundamentally operate. Cities governance and business models for sustainability preservation are revised or re-engineered to meet citizen's expectations by introducing ICT infrastructures. Regarding the deployment of ICT infrastructures and devices on a massive scale, cyber situational awareness and incident response capabilities must be adequately defined from the outset. In essence, identification of a common ground between cybersecurity and local governance is essential. Cyber situational awareness and incident response practices may require the establishment of a city level CSIRT and its coordination with other peer CSIRTs employed by services providers and stakeholders. Also, the heterogeneity of a smart city, where various technological enablers are involved, and the lack of standardised digital forensic investigation techniques, reinforce the importance of well-defined incident response processes and the existence of a digital forensic readiness framework.

In order for a city to deploy a successful digital forensic readiness framework, some processes have to be performed in advance, such as identification of data sources, digital infrastructure architectures definition and identification of hypothetical attack scenarios. In addition, regarding the generation, collection, management, and exchange of digital evidence within a smart city, the challenges related to its integrity must be addressed. Integrity of the Chain of Custody (CoC) is critical for future digital forensic investigations and the overall success of the underlying digital forensic readiness framework. As such, the implementation of technologies and techniques that assure the integrity of CoC is essential. Blockchain may be considered as the technology that can facilitate the preservation of integrity of CoC, and eventually the admissibility of digital evidence to a court of law. Blockchain-enabled technologies and techniques, such as smart contracts and NFTs, can certify the authenticity and integrity of digital evidence through all the stages of the process, before and after an incident. Since this research is already dealing with a considerably complex environment, it is essential to tessellate the problem domain.

Also, none of the existing readiness frameworks and models is standardised and may not be able to facilitate the adoption of a digital forensic readiness processes within the realm of a smart city, due to the heterogeneity and complexity of this particular domain. In addition, this research takes into consideration the achieved maturity level, which indicates the level of the technological integration, as well as the level of exposure of a city related the vulnerabilities and risks that may affect it and the damage that their exploitation may cause to the digital infrastructures, and introduces a crowdsourced approach, where various members and parties are involved to the collection and preservation of digital evidence. The proposed digital forensic readiness framework is adjusted to the needs of a city dependent on the maturity level that a city has achieved, since more mature cities members may need to identify and collect digital evidence more frequently than less mature cities. The existing frameworks and models are static and rely on centralised solutions, where particular entities and authorities identify the available digital evidence sources, collect and maintain it until its involvement to an investigation. Furthermore, the Circular Economy paradigm is involved to the development of the proposed digital forensic readiness framework, since already generated data that facilitate specific purposes within a smart city ecosystem may be identified as potential digital evidence and may be collected and stored for a future investigation.

The main goal of this research relates to the optimisation of a vulnerability-driven incident response process and the deployment of a digital forensic readiness framework, depending on the maturity level that a city has achieved. In a context of a smart city, a digital forensic readiness framework - and consequently the underlying incident response plan - is dependent upon two aspects. First, the maturity level will dictate the needs, investment and resources, since the establishment of the incident response plan is risk-driven. Second, a consensus of the different stakeholders who will be involved in executing the incident response playbooks will need to be reached. The latter indicates the human factors element of the forensic readiness framework.

1.2 Novel aspects of the thesis

The novel aspects of this thesis include

- an approach for incorporating the vulnerability management dimension in smart cities based on the adopted maturity model. This was achieved by:
  - conducting an empirical analysis of the current smart cities and their technological assets' exposure based on existing vulnerabilities;
  - identification of aspects that can increase and decrease the vulnerability exposure of cities, especially on higher maturity levels.
- A maturity level dependent digital forensics readiness framework for smart cities. This entailed:
  - an application of Distributed Ledger Technologies on the digital forensics domain, to address preservation of integrity of Chain of Custody challenges;
  - a digital forensics playbook, describing both pre-incident and post-incident processes, with an indicative distribution of the underlying tasks among a smart city's stakeholders and actors;
  - a critical evaluation on the differences between Ethereum and EOS, advantages and limitations of each DLT network and adoption of EOS NFT scheme;
  - a suite of algorithms for handling on-chain digital evidence related data, describing the digital evidence objects creation and possession, during the pre-incident phase, as well as the digital evidence objects transmission and deletion during the post-incident phase, dependent on the maturity level of the city;
  - a decision making and evaluation tool based on a macroeconomics methodology, to evaluate and validate the compatibility of the aforementioned playbook and algorithms with the Circular Economy paradigm.

1.3 Research Question

The research conducted in this thesis strives to answer the following question:

Can an incident response plan to be deployed dependent on the "smartness" of a city, while respecting the Circular Economy paradigm?

The research question is broken into the following, aimed at addressing three main research areas.

- **Aim 1:** Provide a suitable definition of a smart city, what sustainability entails, and investigate the technological enablers adopted by smart cities, as well as their contribution of Circular Economy model.
  - **Objective 1.1:** Adopt a maturity model as defined in (Ideal-Cities (2018)), and develop use cases that may facilitate this research.
- **Aim 2:** Identify the common ground between the technological integration and the increase of the vulnerability exposure of smart cities;
  - **Objective 2.1:** Understand the risk and investigate the risk impact differences between identified maturity levels;
  - **Objective 2.2:** Establish how the technological integration affects a city's vulnerability exposure.
- **Aim 3:** Propose and deploy a digital forensic readiness playbook for local authorities, service providers and stakeholders in general, and introduce a Blockchain and smart contracts based approach for digital evidence integrity preservation, dependent on the smart city maturity level.
  - **Objective 3.1:** Identify suitable technologies and service models supporting the CE paradigm;
  - **Objective 3.2:** Create a playbook that is dependent on maturity model;
  - **Objective 3.3:** Evaluate the compatibility of playbook against the CE paradigm.

1.4 Thesis Structure

The thesis is organised in Chapters. Data-driven Circular Economy in Smart Cities is presented in Chapter 3 and involves the presentation of two main pillars of this thesis, Circular Economy and smart cities, as well as the technological enablers that are involved.

In Chapter 4, some of the use cases have been taken into consideration for the needs of this research are presented, and are related to various city's sectors, such as healthcare, and transportation. The presented use cases introduce scenarios related to the exploitation of vulnerabilities and risks within a smart city ecosystem, affecting critical infrastructures of it and causing serious issues to the digital infrastructures and threatening citizens safety and life. The scenarios are presented taking into consideration cities that have achieved various levels of maturity, designating the interconnection and the interdependency between the adopted technologies and systems, as well as the interconnection and interdependency between critical sectors and infrastructures within the same context. The presented use cases designate the vulnerabilities exploitation risks among critical infrastructures and critical sectors of a city and inform the proposed vulnerability management that is presented in Chapter 7, as well as the Digital Forensic Readiness Framework (DFRF) and Digital Forensic Readiness Playbook, presented in Chapter 8, which takes into consideration the maturity level of a city, the interconnectivity among critical sectors and infrastructures of it, the technological integration, the heterogeneity of technological enablers and the different digital forensics approaches that exist, and the cascading effect that the exploitation of a single vulnerability or risk can cause, not only to a particular city sector, but to others as well.

Chapters 5 and 6 are based on related to this thesis publications and include the presentation of a proposed architecture for smart, circular cities, the advantages and the limitations of DLTs deployment that may provide to the improvement of smart city services, the identification of threats related to a particular smart cities use case, intelligent transportation system and the deployment of IOTA distributed ledger technology for improving the communication between vehicles and infrastructures.

In Chapter 5, some fundamental technological enablers within the realm of a smart city are identified, as well as their inherited constraints. In this Chapter, Blockchain is considered as the technological enabler that can overcome the challenges regarding the employment of other technological enablers and enhance their performance and assure the security and privacy maintenance.

In Chapter 6, the research is conducted under the prism of Intelligent Transportation Systems, which are considered as critical sector of a smart city ecosystem. In the realm of a technologically advanced city, Intelligent Transportation Systems are equipped with *smart* devices, such as IoT devices, and are enabled with Internet connection. Based on the integration of technological enablers, such as IoT and the vulnerable *nature* of IoT paradigm, the identification of potential attack vectors, considering three tiers, devices, network and DLT layers takes place. For the evaluation of the identified ITSs based attack vectors, the DREAD threat modelling scheme has been employed, which are evaluated by using the DREAD ranking scheme. In addition, in Chapter 6, the usage of DLT over a critical sector of a smart city is presented. It should be mentioned that the adoption of DLT facilitates not only the protection of the ITSs infrastructures, but identifies the employment of DLT as a means of maintaining data as potential digital evidence and preserving the integrity of the Chain of Custody.

The Chapter 7 is based on the *"Vulnerability Exposure Driven Intelligence in Smart, Circular Cities"* publication, and introduces the vulnerability and risk dimension of a smart city and how a vulnerability can affect different maturity levels that a city has achieved. In addition, in Chapter 7, various factors that affect the vulnerability exposure are presented through a statistical analysis. Since the vulnerability exposure of a city is dependent on several dimensions, as presented within the Chapter 7, the vulnerability management is critical, especially for those cities that obtain higher level of technological integration for addressing the needs of citizens.

According to the hypotheses presented in this Chapter, especially according to H_4, the integration of technological enablers decreases the vulnerability exposure of a city, however, the technological integration alone might not be able to reduce the city exposure enough. Furthermore, the information and communication technologies integration within the realm of urban environments may increase the interdependency and heterogeneity of the environment, generating useful data that facilitate various services and the cooperation of different stakeholders. Although, the technological integration facilitates various purposes of a smart city, it is not enough to reduce the vulnerability exposure of it, as discussed above. In particular, the adopted approach focuses on smart cities and their vulnerability exposure against the maturity model, presented in Chapter 3, for enabling the development of a meaningful and contextualised risk based approach using vulnerability impact and exposure data. Cities are challenged is the way they fundamentally operate. Cities governance and business model have been revised to meet the expectations of citizens who are in line with the end users of the deployed ICT infrastructure. Deploying devices on a massive scale requires well-defined cyber situational awareness and incident response capabilities from the outset.

As such, the deployment of an efficient incident response plan and a digital forensic readiness framework, which can indicate the needs of a city regarding the teams that are involved, the identification of potential risks, the identification of critical infrastructures and services and the identification and prioritisation of digital evidence sources and digital evidence types, as well its collection and maintenance until an incident takes place may be considered as essential.

The presented vulnerability management and the hypotheses of this research may inform the development of the aforementioned digital forensic readiness framework and indicate the actions that should be taken by local authorities, stakeholders and members for a city to be considered as digitally forensic ready, having identified the level of exposure and the underlining risks.

The Chapter 8 defines incident response, digital forensics process and digital forensic readiness and presents the proposed digital forensic readiness framework for smart circular cities, the DFRP and the generation and transmission of NFT tokens that assure the integrity of Chain of Custody.

The proposed framework, presented in Chapter 8, is informed by the the risk assessment process, presented in the Chapter 6 that designates potential attack vectors that may affect a particular sector and service of a city and the vulnerability management, presented in the Chapter 7, which defined the vulnerability exposure of a city against several dimensions of it. It should be mentioned that the risk assessment remains a critical process and one of the fundamental parts of the proposed DFRP.

The DFRF presented in this research employs Distributed Ledger Technologies in order for the integrity of digital evidence objects to be preserved. In particular, the proposed framework employs Blockchain, smart contracts and NFT technological enablers for preserving the transparency of the digital throughout the digital forensic readiness processes, the possession of digital evidence objects by data owners and custodians, during the pre-incident and the post incident phases, as well as the integrity of the Chain of Custody, ensuring that the available digital evidence will not be altered at any stage of the process. In particular, for the needs of this research, a private, permissioned Blockchain network is employed. All the participants of the DFRP are nodes of this Blockchain network and are assigned with a pair of keys in order to be able to verify transaction within the network. In addition, all the details related to a digital evidence object, such as the assigned NFT value and a timestamp, are preserved on the Blockchain as records, which are updated at every phase of the of the process. The NFT values are generated and assigned to every digital evidence object, from its creation stage until its final deletion by the custodian, after the completion of a digital forensic investigation. The NFT values are generated by the execution of smart contacts and facilitate the ownership of digital evidence objects, keeping records of all the changes of ownership among data owners and custodians, after the beginning of a digital forensic investigation. Furthermore, for the needs of this research, a distributed NFT scheme has been adopted, and its main goal focuses on the distribution of the ownership of a particular digital evidence object to more than one custodian, when it is necessary. As such, percentages of the NFT value can be assigned to more than one custodian, who conduct a particular digital forensic investigation. Finally, the conclusions, limitation, and proposals for further study based on this research are presented in Chapter 8.

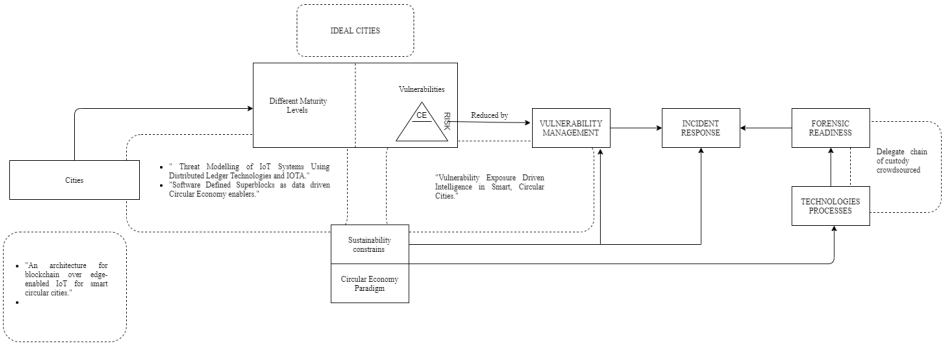

FIGURE 1.1: PhD Overview

1.5 Related Publications

This section presents material in Chapters 3 to 6 that have been published in peer reviewed conference proceedings and workshops.

- Damianou, A., Angelopoulos, C.M. and Katos, V., 2019, May. An architecture for blockchain over edge-enabled IoT for smart circular cities. In 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 465-472). IEEE.
- A. Damianou, M. A. Khan, C. Marios Angelopoulos and V. Katos, "Threat Modelling of IoT Systems Using Distributed Ledger Technologies and IOTA," 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2021, pp. 404-413, doi: 10.1109/DCOSS52077.2021.00070.
- Jarvis, P.D., Damianou, A., Ciobanu, C. and Katos, V., 2021. Vulnerability Exposure Driven Intelligence in Smart, Circular Cities. Digital threats: research and practice. ACM Journals.

Further publications

- Angelopoulos, C.M., Damianou, A. and Katos, V., 2020. DHP Framework: Digital Health Passports Using Blockchain–Use case on international tourism during the COVID-19 pandemic. arXiv preprint arXiv:2005.08922.
- Bada, A.O., Damianou, A., Angelopoulos, C.M. and Katos, V., 2021, July. Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption. In 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 503-511). IEEE.

Chapter 2

Methodology

2.1 Introduction

In this Chapter the research approaches that support this thesis from a philosophical and methodological perspective are presented and discussed, as well as the decision making behind the methodological approaches that have been employed.

This Chapter presents the research methodology that has been adopted, starting with the aims of it and all the approaches that have been employed in order to be addressed. The two methodology approaches, quantitative and qualitative, have been described in accordance to each presented Chapter of this thesis. Also, the decision making behind each standard and scheme is presented as well.

In addition, the review of the literature provides all the necessary knowledge related to this research. First of all, the term Circular Economy is defined and analysed, as well as its contribution to the realm of smart cities and the establishment of a maturity model. Also, light has been shed on the establishment and evolution of smart cities and their major technological enablers that facilitate the improvement of the provided services to citizens, as well as the life quality of them. Furthermore, the DREAD and CVSSv3.0 standards have been employed in order for the risk assessment process related to this research to be completed. Finally, the term digital forensic readiness have been defined, analysed, and adopted for the needs of this research, as one of the fundamental contribution of it.

Moreover, the available datasets, the sources of data and how they have been proceed are presented in this Chapter. The available dataset includes data collected or generated that belong to two main and orthogonal domains, related to cyber security and to Cities in Motion research (Berrone and Ricart (2019)).

Finally, the analysis and the evaluation part of this research is presented, the statistical analysis that has been adopted for the evaluation the hypotheses, presented in Chapter 7, as well as the evaluation of the proposed Digital Forensic Readiness Framework (DFRF).

2.2 Research Methodology

This research adopts both qualitative and quantitative research. As mentioned earlier, the scope of the research is on smart cities and specifically those that aim to adopt the data-driven CE paradigm. The qualitative research aspects aim to:

- define the context through the development and presentation of representative use cases;

- evaluate and assess the appropriateness and suitability of some of the enabling technologies (such as Blockchain) and their level of alignment in the CE paradigm transition;
- perform a (qualitative) risk assessment of a representative use case (Intelligent Transportation Systems);
- evaluate the proposed Digital Forensic Readiness Playbook (DFRP) in terms of their CE potential.

The quantitative research aims to provide insights on the risks introduced by vulnerabilities and how these are perceived by cities placed on the various maturity levels. The outcome of the quantitative research would in turn justify the need for incident response plans adjusted by the respective maturity level.

In particular, the methodology that has been adopted for this research is a combination of quantitative and qualitative research.

Starting with the qualitative research, the context of this research through the presentation of four use cases related to some critical sectors of smart cities, such as healthcare, transportation and energy that concern different maturity levels that a city may achieve, has been defined. In addition, through the presentation of attack scenarios, the different manifestations of risks across the maturity levels, and the impact of vulnerabilities are presented. The presentation of the four use cases indicate the impact of an attack exploitation among different maturity levels that the four cities has achieved, and how this exploitation affects not only the compromised systems and services, but the digital infrastructures in general. This is the first approach of identifying the exposure profile of a city taking into consideration the maturity level that it has achieved and the different mechanisms that it is necessary to be adopted in order for both cyber physical and socio technical systems to be protected enough. Furthermore, the different exposure profiles indicate the different approaches that has to be adopted regarding the deployment and implementation of the proposed Digital Forensic Readiness Framework.

Furthermore, the appropriateness and suitability of some enabling technologies, such as Edge Computing and Blockchain, facilitating their coexistence within the same urban ecosystem are evaluated. In addition, a smart cities architecture for facilitating CE and IoT paradigm and we critically assessed it against existing Blockchain architectures under a broader context of emerging ICTs and their implication has been designed. The Blockchain may be considered as a novel and innovative technological enabler that is broadly adopted for facilitating various purposes, such as decentralisation, transparency and immutability. In addition, the Blockchain uses strong cryptographic techniques and provides enhanced security and privacy where it is applied. Due to these characteristics, the Blockchain is adopted by this research in the context of smart cities.

Moreover, the research focuses on the Intelligent Transportation Systems sector and a (qualitative) risk assessment over the attack vectors that we identified, employing the DREAD threat modelling is performed. For the needs of this research, only the DREAD threat model has been employed over OCTAVE and STRIDE for several reasons. First of all, the DREAD model is considered as easier and more understandable by people, who may not be involved in cybersecurity. In addition, the DREAD threat model takes into consideration the affected users by the exploitation of a vulnerability or a risk, which is considered as important factor within the realm of smart cities. Furthermore, the DREAD threat model may be considered as compatible with the CVSSv3.0 scoring system, that has been adopted in Chapter

7. The CVSSv3.0 scoring system has been adopted over other vulnerability scoring systems, such as OWASP Application Security Verification Standard (ASVS) and Tenable Vulnerability Priority Rating (VPR). The OWASP ASVS Project is used for testing web application technical security controls and provides developers with a list of requirements for secure web applications development (Manico (2015)).

On the other hand, the Tenable VPR facilitates organisations to improve their remediation efficiency and effectiveness, by assessing the identified vulnerabilities taking into consideration two components, the technical impact and the threat. The identified vulnerabilities are rated as Critical, High, Medium and Low. The technological impact measures the impact on confidentiality, integrity and availability after a vulnerability exploitation. The technological impact is equivalent to the CVSSv3.0 impact subscore. The second component, the threat, reflects both current and future threat activity against an identified vulnerability.

Comparing all the standards that have been presented above, the OWASP ASVS may not be considered compatible with the smart cities case, since it focuses on web applications and the assessment of fundamental identified vulnerabilities assessment during their development.

On the other hand, the Tenable VPR standard may be considered as more compatible to smart cities concepts and to CVSSv3.0. In addition, according to (Nessus (2022)), the VPR is more efficient than CVSSv3.0, since it takes into consideration the age of a vulnerability and prioritises each identified vulnerability taking into account both technical characteristics and threat intelligence.

Also, it should be mentioned that both standards are considered as equivalent. In this case however, the CVSSv3.0 is adopted and established more in order to be considered as more trustworthy.

Both schemes, the DREAD and CVSSv3.0, complete the risk assessment process of this research.

In terms of the quantitative research, a statistical analysis taking into consideration various datasets, related and not related to cybersecurity has been performed. The vulnerability exposure of a city, expressing it as the sum of the quantity v, standing for every identified vulnerability, multiplied with b_v, standing for the respective CVSSv3.0 base score is defined. We ran some hypotheses testing based on the literature having various details regarding the vulnerability profile of a city and on a country level as well, from business studies, such as Cities in Motions (Berrone and Ricart (2019)) study. As such, several hypotheses, like *"The severity of vulnerabilities in countries decreases with GDP per capital"*, which has been rejected, *"The city type moderates the vulnerability exposure, so the smarter cities have a larger vulnerability exposure than plainer cities"*, *"The population of cities increase the vulnerability exposure"*, and *"The level of technological integration decreases the cities vulnerability exposure"* are defined.

Also, a hierarchical clustering takes place. It has been found the profile of every city, what vulnerabilities every city suffers from and then we did a simple clustering taking into consideration only the smart cities that obtain a CE agenda, having achieved the highest maturity level, the Responsive. The outcome of this part of the research justifies the needs for an incident response and a digital forensic readiness plan adjusted by the respective maturity level.

Finally, a cross methodology evaluation approach from the macroeconomic domain has been employed to assess whether the proposed playbook would support the CE paradigm and how a crowdsourced approach would affect the maturity level, incident response and the overall equilibrium between them, increasing both.

Figure 2.1 presents both, the qualitative and the quantitative methodologies approaches, adopted for the needs of this research.

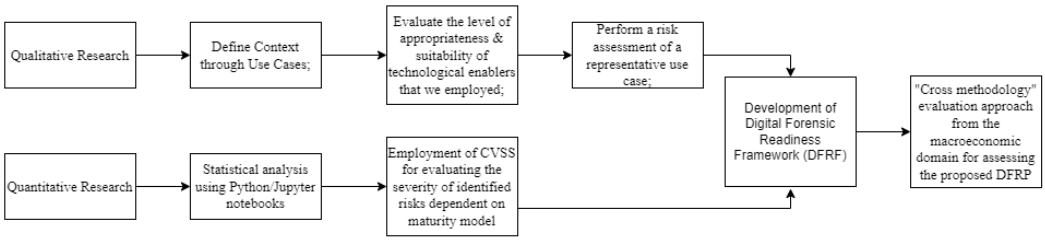

FIGURE 2.1: Methodology Overview

2.2.1 Literature review

The research was informed by the following areas of the existing literature and state of the art:

- Circular economy is considered as a relatively novel production and consumption model and it is considered to be a sustainable solution along with the adoption of novel technologies. Its contribution to this research is on defining the maturity model and differentiating upon the levels of impact of a software vulnerability.
- Research on smart cities remains a hot topic during the last decades, providing evolving ideas for the improvement of cities around the globe and provided services to citizens. The research over smart city topic reveals all the advantages and limitations of existing smart cities concepts and the opportunities that are provided by the employment of technological enablers and other techniques that may contribute to the provided citizens services.
- For the needs of this research, elements of risk assessment should be taken into consideration. In particular, the industry-standard DREAD rating system has been adopted (Huq, Vosseler, and Swimmer (2017)). The DREAD threat model provides a rating system and three categories of severity, low, medium, and high. The assessment of the identified attack vectors is performed against Damage, Exploitability, Affected Users, and Discoverability.
- Vulnerability management facilitated this research and allowed the identification of vulnerabilities and risks that may affect a smart city ecosystem. In order for the identified vulnerabilities to be assessed, the CVSS scoring system has been adopted. Common Vulnerability Scoring System evaluates vulnerabilities related to software, hardware, and firmware by offering a base score calculation. The CVSS score enables the quantitative research aspects of this work, as it ranges between 0 and 10, mapping also the severity of a vulnerability from low to critical.
- According to NIST, "*Incident response is an approach that addresses and manages the next phase of a security breach or a cyberattack. It is also known as IT incident, computer incident or security incident. Goals of incident response include the handle of a situation in a way that limits the damage and reduces the recovery time and cost after an incident"* (Cichonski et al. (2012)). In addition, the relevant aspect of incident response that this work focuses on is digital forensic readiness, referring to the processes that should be followed before an incident, in order to optimise the collection of digital evidence and minimising both the time and costs of a digital forensic investigation.

2.2.2 Datasets

For the purpose of the quantitative research, both primary and secondary data were collected. The datasets collected or generated belong to two main and orthogonal domains. The first domain involves "smartness" metrics and factors conducted by business type of research groups, such as the Cities in Motion research (Berrone and Ricart (2019)). The second domain refers to cybersecurity research. More specifically, this research adopted the ENISA vulnerabilities 2018-2019 dataset (Rostami (2020), ENISA (2019)), which includes contextualised vulnerability data from various open sources. This dataset was extended and enriched with geolocation (on a country and city level) data, as well as device exposure data from Shodan's database. In addition, the Global Cybersecurity Index was also included in order to allow the execution of hypothesis testing on a country level (Bruggemann et al. (2021)).

2.2.3 Analysis and evaluation

The quantitative research includes statistical analysis using Python / Jupyter notebooks. The analysis tested a number of statistical hypotheses to illustrate the potential risks that may affect a city against a number of factors contained in cities in motion research (Berrone and Ricart (2019)), taking into consideration the maturity level that a city has achieved. Exploits and risks that may be indicated as high and/or critical and may affect severely a particular city at a certain maturity level, indicate the need for the deployment and implementation of a digital forensic readiness framework. In addition, the CVSS scoring system was adopted for evaluating the severity of an identified risk within a city, taking into consideration its severity based on the maturity level.

The proposed digital forensics readiness framework is evaluated on the basis of its agreement with the CE paradigm. Specifically, the introduction of Blockchain in the incident response and the digital forensics process in particular proposed in this thesis considers a crowdsourced approach to preserving the evidence. The "*cross methodology*" evaluation approach has been adopted from the domain of Macroeconomics to assess whether the proposed playbook would support the CE paradigm. This is achieved by showing that the additional incident response processes will not necessarily have a disproportionate impact on the resources and ICT investment of the city in its journey to attaining a higher maturity level.

2.3 Concluding Summary

In this Chapter, the methodological approaches that have been adopted for the needs of this research. Also, the decision making behind the methods and standards that have been employed is introduced along with details related to them. In addition, the literature review approach, the dataset process and the analysis and evaluation of the main contribution of this research are presented in this Chapter.

Chapter 3

Data-driven Circular Economy in Smart Cities

3.1 Introduction

This Chapter focuses on the presentation of the literature review related to smart cities and the Circular Economy paradigm. The Chapter includes the definition of the Circular Economy (CE), its business models, the definition of Smart City concept, the technological integration and the key technological enablers that are employed in order to facilitate the technological advancement, performance, and improvement of provided city services and quality of life of citizens. In addition, the term Data-driven Circular Economy is described and presents the advantages of this approach in terms of an urban environment. Furthermore, the term circular cities is introduced.

Finally, various technological enablers within the realm of smart city ecosystem and some real smart cities use cases are presented as well.

3.2 Circular Economy

Circular Economy has been introduced as a novel production and consumption model that is promoted by several national governments, like France, China, Japan, the UK and Canada, and by several businesses around the world (Morlet et al. (2016a)). It is estimated that this type of economy can create 600 billion euros in annual economic gains in the European Union. The current linear *take, make, dispose* economic model that enables the extraction, exploit, use and dispose materials at high rates, has been recognised as unsustainable. This model relies on easily accessible resources and energy that are consumed. The reduction of consuming those resources and energy is not the solution to the problem. The flow of the current and traditional linear model seems to be harmful, especially for the environment, as the recycling of these materials is not efficient enough to reduce the amount of wasted products (Morlet et al. (2016a)).

Even though several efforts have been made in order to improve recycling processes, both from technical and business perspective, the core problem has not been addressed yet. The Circular Economy concept is the fundamental change that the linear, old economy model needs. Adopting natural "*techniques*" that recycle and reuse waste, the Circular Economy facilitates the claim that materials may be reused and remain functional, since they have the opportunity to be generated and restored. The main advantages of the Circular Economy involve reduced exposure to price volatility, substantial net material savings, increased economic development,

increased innovation and job creation potential and increased resilience in living systems and in the economy (Morlet et al. (2016a)). According to researchers around the world, in order for circularity and sustainability to be achieved, the two key factors are technology and people (MacArthur et al. (2013)).

The Circular Economy's main aim includes the preservation of products, materials and components at their highest utility and value during their whole life cycle.

It distinguishes between biological and technical cycles as an attempt to minimise leakage and wastage. Circular Economy is built on the premise that every asset can be used more than once for facilitating more than one purpose. Figure 3.1 captures the concept of CE *butterfly* system diagram, presenting the relationship between biological and technical cycles.

3.3 Data-driven Circular Economy

The term Data-driven Circular Economy refers to the usage of reactive, adaptive, autonomous or collaborative objects and systems for creating of economic and environmental value by closing material and energy loops, reducing natural resources depletion, and restoring natural balances (Langley et al. (2021a)). The Circular Economy model contrasts with the established linear economic model, where resources turn to assets that are disposed of after they have fulfilled their usage purpose.

Circular Economy was first presented in the late 1970s and evolved over the years until the present, enabling the transition from the linear *take-make- dispose* model to the *make, use, remake* model. Circular Economy includes the design and development of innovative materials that are more *eco-friendly* and highly recycling friendly. On the other hand, the rise of consumerism did not truly allow the adoption of the Circular Economy model, but rather the introduction of the recycling process towards the end of the produce-consume-dispose line. The concept of the Circular Economy has been revisited in recent years in the light of recent technological advances. Rise of technology, especially of the ICTs, allows the generation and collection of data of high granularity and fidelity. The value of this data is high, since multi-dimensional information for facilitating the fine-turning of processes, as well as decision making.

Internet of Things paradigm allows the generation and the transmission of data among Internet enabled devices. The Internet of Things (IoT) paradigm includes a variety of devices and technologies, like sensors and actuators, embedded microprocessors and microcontrollers, low power wireless networks and light-weight communication and application protocols, which underpin the seamless and massive integration of everyday objects to the Internet. The scope of this integration enables not only remote control and automation, but the communication of devices with each other and the adjust of their operation depending on received data and information from various systems and machines. Another important aspect of the Internet of Things paradigm is the gap bridging between the cyber plain and the physical plain, thus paving the way towards cyber-physical systems.

While sensors allow digital systems the data collection from their environment and the monitoring of physical processes, actuators allow digital systems the action upon their environment. The IoT paradigm is a representative example enabled by the recent technological advancements that have transformed the understanding and interaction with *computers*. Other theologies of the same category include Distributed Ledger Technologies and Next Generation Wireless Communications, such as Multi-access Edge Computing and 5G, Artificial Intelligence, machine learning,

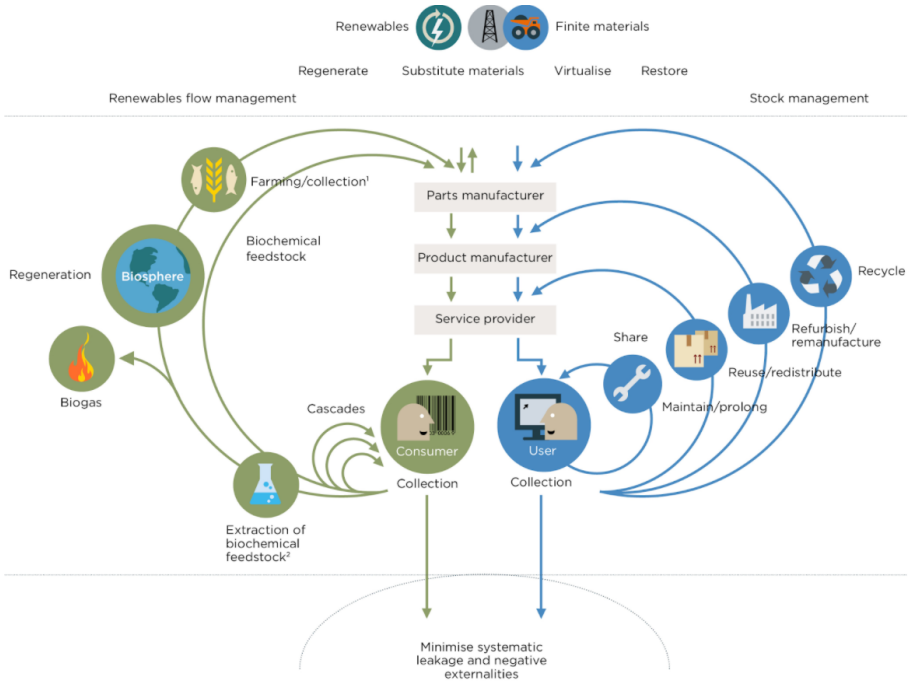

FIGURE 3.1: CE system diagram (Ellen-MacArthur-Fundation (*Introdution to Circular Economy*))

and Robotics. All these technologies coordinate, creating a novel technology-led environment that supports the socio-economic paradigm, like the Circular Economy.

The employment of the aforementioned technologies enables the identification of smart assets, the collection of dense spatiotemporal data related to assets and the automatisation of assets behavior and their reaction. In addition, this employment enables the reconsideration of the Circular Economy model under a Data-driven methodological approach perspective. This approach improves the digitisation and decision-making process, facilitates interoperability between heterogeneous systems, and facilitates the development of comprehensive use cases.

3.4 Business Models of Circular Economy

As mentioned above, the Circular Economy's aim is the contribution to the optimisation of resources utilisation and the extension of their lifecycle. The Circular Economy focuses on the utilisation of existing resources, the deployment of products with extended lifecycle and their re-usage by converting back into new sources for a different purpose (Esposito, Tse, and Soufani (2018)). One of the achievements of the Circular Economy model may be the replacement of the end-of-life concept with restoration, by promoting the transition to the use of renewable energy and the elimination of waste by creating new materials, products and systems with extended lifecycle that facilitate various purposes (MacArthur et al. (2013)).

Also, the Circular Economy may play a key role to the deceleration of climate change and the protection of environment by:

- renewable resources usage for equilibrating the demand for non-renewable resources;

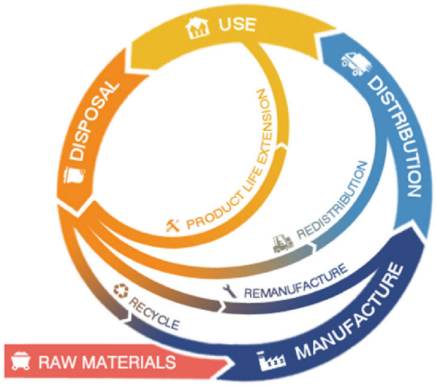

FIGURE 3.2: The CE Cycle (Ideal-Cities (2018))

- decreasing waste by reusing existing resources and designing products in a smart way for increasing their productivity during their whole lifecycle;
- using eco-friendly components in the manufacturing process that can return to the environment without harming it.

The principles above create a fertile ground for the establishment of four sources of value creation to implement instead of Linear Economy model (MacArthur et al. (2013)):

- Inner circular power is related to product shelf life and reduced replacements, refurbishment and re-manufacturing need. The increase of the power of inner circle reduces the labour, energy and resources consumption embedded in the product.
- The circling longer power refers to the maximisation of the number of consecutive cycles- reuse, re-manufacturing or recycling, and the time in each period.
- Cascade use power is related to the diversification of the reuse in all phases of the value chain.
- The pure circles power stems from the fact that using uncontaminated materials in production enhances the efficiency of collection and redistribution while preserving quality.

The Circular Economy model attempts to change the traditional concept of new resources consumption to a more resilient behaviour where products are not wasted after the end of their lifecycle, but adapt for facilitating a different purpose.

3.4.1 Business Models

Business models of Circular Economy aim to the maximisation of the usage of existing resources avoiding the consumption and extraction of new ones. Business models of Circular Economy recommend actions in all phases of the value chain for improving resources usage. Research by Lacy and Rutqvist, Lacy and Rutqvist (2015) distinguish 5 types according to a business-oriented perspective (Ideal-Cities (2018)):

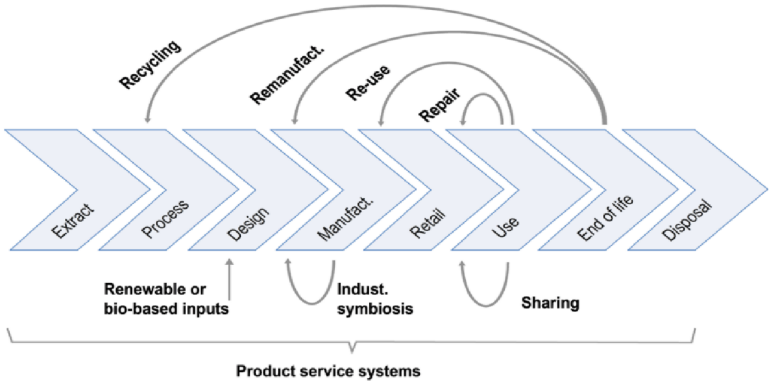

FIGURE 3.3: Circular economy business model impact in the linear economy (OECD (2019))

- Circular supply chain: Right from the start;
- Recovering and recycling: making a history of waste;
- The product life-extension Business Model: Products that are built to last;
- The sharing platform business model: Sweating Idle Assets;
- The product as a service business model;

3.4.2 Circular Supply Chain

The circular supply chain promotes the transitional materials replacement with bio-based materials, in order for companies to reduce the impact to the environment by producing materials that will end up to waste. This process is challenging, since the demand of market for new eco-friendly products must be ensured because higher prices may be applied and traditional material must to be replaced with new products that satisfy or surpass their quality. Finally, the cost for the new products production must be affordable for companies. In any other case, companies may not be amenable to adopt models that will increase the production cost (MacArthur et al. (2013)).

3.4.3 Recovering and Recycling

Since market is competitive and the materials prices have increased, companies turn their attention to reuse by-products. This model encourages the reuse of material and the value of product return flow maximisation. The major challenge for adopting this model is related to the preservation of the unit cost of a product to low levels, compared to the traditional materials production. The by-product must meet quality standards, which might be challenging to meet at times. The by-products availability will also obtain a key role in ensuring material supply, especially in locations, with lower population and demand. Finally, the cost of transportation can have an

impact on the implementation, depending on the nature and quantity of material (OECD (2019)).

3.4.4 Product life-extension

Companies and organisations rely on the model that focuses on production of volume that encourages costumers to replace a product frequently. This model proposes the creation of products with limited lifecycle that are wasted after the first usage, causing a significant amount of waste. This business model aims to the improvement of products life span proposing innovative ways for product up-gradation without change it every time that a new feature is released. Model suggests various ways of putting a product back to the market without discarding it. The main challenge for this model is to provide a product that can be easily upgraded or disassembled to restore various parts (OECD (2019)).

3.4.5 Sharing Model

Sharing model refers to the sharing economy and involves virtual platforms in order for owners to connect with costumers or organisations, who can use their services. Platforms will not accept product idleness, but will increase their productivity by allowing co-access or co-ownership (MacArthur et al. (2013)). This business model is the product of modern technology such as the Internet and mobile phone applications, promoting communication means among people. For owners of underutilised assets, the use of the platform provides an opportunity for income increase (Nicholls et al. (*& Muir-Wood, R.(2008). Ranking port cities with high exposure and vulnerability to climate extremes*)). The challenges that this model includes refer to criticism of the broader economic impact and the need to pass new legislation to avoid misunderstandings with the hotel industry .

3.4.6 Product as a service

This business model introduces a scheme where the ownership of a product is retained by the company and the product itself is less important than the performance. The services offered from a company include the maintenance through design, use, reuse, re-manufacture and recycling (Tukker (2004)). In essence, costumer of a product becomes a user of a service instead of the product owner. There are four types of monetisation including the pay for the usage of a product or service based on metrics, the rent of a product or service for a limited time period and finally, payment after a performance agreement, where an involved service has to achieve specific results. The market expansion and the full service digitalisation are some of the main challenges of this model. Physical services may be limited in terms of costumers who are able to access it. On the other hand, a fully digital service may become unavailable to costumers (Tukker (2004)).

3.5 Smart Cities

Urbanisation has been consistently increasing over the last decades, where a vast number of people relocate to big cities around the world to settle, work and live. Consequently, the concentration of people within urban environments comes along with concerns regarding the living conditions, traffic air and noise pollution, and the increased generation and accumulation of rubbish. Efficient solutions for addressing

sustainability issues that urbanisation raises are essential with the Information and Communication Technologies (ICTs) to play a significant role in addressing these challenges.

During the last years, the transition from a traditional to a smart city has come to the spotlight, although this concept is not a new one. The International Telecommunication Union (ITU) has captured more than 100 definitions for describing a smart city concept (International-Telecommunication-Union (2014)).

In addition, the term smart is not the only one used to describe urban environments that employ technological enablers. These terms include *wired city, connected city, intelligent city,* and *digital city* (Mohanty, Choppali, and Kougianos (2016)).

Some smart city term definitions are presented below:

- **2000** *A city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports, communications, water, power, even major building, can better optimise its resources, plan its preventive maintenance activities, and monitor security aspects while maximising services to its citizens* (Hall et al. (2000)).

- **2006,2008** *Territories with a high capacity for learning and innovation, which is built in to the creativity of their population, their institutions of knowledge production, and their digital infrastructures for communication* (Hollands (2008a)).

- **2007** *A Smart City is a city well performing in a forward-looking way in these six characteristics (economy, mobility, environment, people, living, governance) built on the "smart" combination of endowments and activities of self-decisive, independent and aware citizens* (Giffinger et al. (2007)).

- **2012** *Smart cities a high productivity as they have a relatively high share of highly educated people, knowledge-intensive jobs, output oriented planning system, creative activities and sustainability oriented initiatives* (Kourtit, Nijkamp, and Arribas (2012)).

- **2013** *The term "smart city" is understood as a certain intellectual ability that addresses several innovative socio-technical and socio-economic aspects of growth. These aspects lead to smart city conceptions as "green" referring urban infrastructure for environment protection and reduction of CO_2 emission "interconnected" related to revolution of broadband economy, "intelligent" declaring the capacity to produce added value information from the processing of city's real-time data from sensors and activators, whereas the terms "innovating", "knowledge" cities interchangeably refer to the city's ability to raise innovation based on knowledge and creative human capital* (Zygiaris (2013)).

- **2014** *A smart city is defined with the meaning of smartness penetrating the urban context, the role of technologies in making a city smarter, and focal domains (infrastructures and services) that need to be smarter* (Nam and Pardo (2014)).

- **2015** *A smart city as a place characterised by the "use of advanced, integrated materials, sensors, electronics, and networks which are interfaced with computerised systems comprised of databases, tracking, and decision-making algorithms"*(Teli et al. (2015)).

- **2017** *A city is designated as smart if it balances economic, social, and environmental development, and if it links up to democratic processes through a participatory government. SC involves the implementation and deployment of information and communication technology (ICT) infrastructures to support social and urban*

growth through improving the economy, citizens' involvement and government efficiency (Yeh (2017)).

- **2018** *Smart cities can be defined as a technologically advanced and modernised territory with a certain intellectual ability that deals with various social, technical, economic aspects of growth based on smart computing techniques to develop superior infrastructure constituents and services* (Rana et al. (2019)).

Although these definitions revolve around technological integration and sustainable development, another aspect of a smart city that emerges during the last years is the human factor, in particular citizens' participation. Despite the ambiguity of smart city term, the core notion of the term lies in the usage of modern and state of the art ICTs. The goal of modern ICTs integration includes the improvement of management processes and services of a city and the quality of citizens life.

On the other hand, these unilateral and concise definitions do not reflect the complexity, the needs and the facets that compose a smart city ecosystem. In many cases, cities are considered as organisms or environments, where many parts interact with each other to facilitate various purposes, services and functions. These interaction indicate certain behaviours on both macro and micro level. Thus, research community attempts to define smart cities by including a set of dimensions (see Hall et al. (2000), Hollands (2008b); Eger (2009); Mahizhnan (1999); Barrionuevo, Berrone, and Ricart (2012)).

Defining different dimensions of a smart city enables the research based on particular aspect, but at the same time acknowledges the interdisciplinary nature of the problem domain. One of the most comprehensive dimensions definition of a smart city approaches is the one by Chourabi et al. (2012) and it is summarised in Table 3.1.

"Analysing the potential for wide scale roll out of integrated Smart Cities and Communities solutions" report of the European Commission presents the results of a 300 examples of Smart Cities initiatives across Europe study. The analysis identifies the similarities of the corresponding Smart Cities and classifies them according to the sector they refer to (Ideal-Cities (2018)):

- Users information in real-time.
- Enhancements of public transport.
- Traffic monitoring and management.
- Built environment smart technologies.
- Sustainable districts.
- Place making.
- Smart city platforms.
- Intelligent city services.
- Smart grids.

The classification above indicates that the initial efforts for the development of a smart city are focused on transportation, building and space management and energy verticals. Although these vertical have been identified as important for the improvement of city's functions, citizens and visitors needs are not addressed. Actually, the same European Commission report presents common reasons of Smart Cities failing across Europe, identifying the lack of attention to users needs that is excluded from the technological deployment of popular solutions.

TABLE 3.1: Dimensions of a smart city (Chourabi et al. (2012))

Dimension	Description
Management & Organisation	Managerial and organisational factors, such as project size, attitudes and behaviors of manager, and organisational diversity may influence a project.
Technology	Smart city relies on applied technologies that enhance critical infrastructure components and services and contribute to the improvement of citizens' life quality.
Governance	Processes, norms, and practices that guide information sharing across diverse stakeholders, as well as their leadership, cooperation, communication, data exchange, partnership and service integration.
Policy Context	The environment's political and institutional components are included.
People & Communities	Individuals and communities that influence and affect the implementation of smart city initiatives include participation and partnership, accessibility, quality of life and education.
Economy	The economic contributions and outcomes of smart city initiatives involve innovation, productivity and flexibility.
Built Infrastructure	Wireless infrastructure and service-oriented information systems contribute to the availability and quality of technological infrastructure.
Natural Environment	Sustainability and effective natural resource management are included.

3.5.1 Cyber-Physical Systems and Socio-Technical Systems

From a system perspective, a city may be considered as a system of high complexity that continuously evolves, with all its components being organised, interconnected and employed to facilitate particular functions or purposes. For the needs of this research, a city can be viewed as a system of systems (Ki-Aries et al. (2018)) comprised of a Socio-Technical System (STS) (Baxter and Sommerville (2011)) and a Cyber-Physical System (CPS) (Rajkumar et al. (2010)).

Representing these two systems in a Venn diagram, the overlapping area would include the pure ICT/cyber elements. STS is defined as the system that includes the users and/or the human assets, who interact with the digital infrastructures of a city to receive a service or to contribute to a city's function. Interactions among users/humans are related to the exchange of information between both the physical and cyber plains.

A Cyber-Physical System involves components, such as intelligent assets, digital infrastructures and physical assets that obtain both physical and cyber dimension.

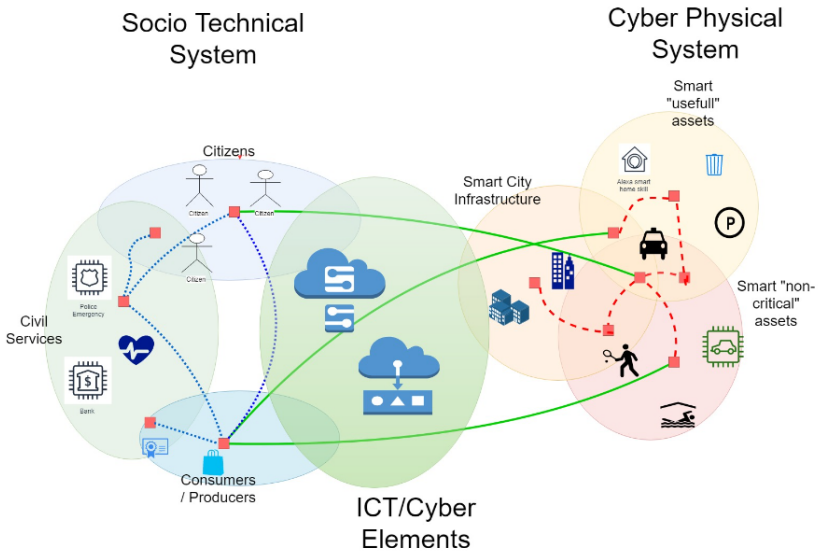

FIGURE 3.4: Coexistence of Cyber-physical and Socio-technical Systems within a smart city environment (Ideal-Cities (2018))

Intelligent assets obtain various levels of *importance* in Cyber-Physical System, taking into consideration the purpose of employment of each asset and the level of criticality of the service that every asset facilitates. The CPSs facilitate industrial control systems and critical infrastructures, having been employed for facilitating other domains, smart cities included. The Cyber-Physical Systems are applied and perform their services in a way to ensure the preservation of the sustainability, safety and security.

One of the milestones of massive CPS deployment is the establishment of the IoT paradigm. The IoT paradigm is rooted back in 2008 and introduces technologies, like embedded systems and wireless sensor networks. Basically, smart devices, sensors and actuators are employed as means of production, collection and exchange of information using wireless networks. Alongside smart devices, machine learning approaches have been introduced and adopted Anthopoulos (2017) for added values to be created from the produced data. Both types of assets, human and Internet connection enabled devices, such as IoTs, interact through the information exchange. Human assets are the producers and consumers of data and information.

Through crowdsensing and crowdsourcing methods, the granularity and accuracy of produced information is high, enabling a fine-grained decision making in real-time, which can be supported by AI solutions. For instance, a smart building environment control system is able to monitor certain environmental parameters, such as temperature, humidity and occupancy of building areas in order to adjust the conditions in the building based on the current circumstances.

3.5.2 Data-driven Circular Economy in an Urban Ecosystem- Circular Cities

A smart city should be considered as the epitome of sustainability since any deviation from this would entertain scenarios of dystopic futures. Since sustainability is one of the main characteristics of smart cities, it should be achieved in some way. A Circular Economy agenda may be the solution to this issue and the means may be provided through ICT integration. In other words, the goal of a city includes not

only to become *smart*, but, to reach a state where sustainable and equitable growth is achieved (Ideal-Cities (2018)).

The main goal of the Circular Economy model is to maintain assets utility without wasting new sources before the end of their life cycle by smartly designing them so as to be used again and again for various purposes, instead of creating new products (Ideal-Cities (2018)).

The coexistence of ICT and Circular Economy can facilitate the extended usage of assets within an environment, providing valuable information regarding their location, condition and performance in real and over time. According to the Ellen MacArthur Foundation, *"A Circular Economy is restorative and regenerative by design, and which aims to keep products, components and materials at their highest utility and value at all time. It distinguished between technical and biological cycles as an attempt to minimise leakage and wastage"* (Morlet et al. (2016a)).

Circular Economy is based on the premise that any material can be reused in this way to be functional again since it will have the opportunity to be regenerated and restored, employing nature-inspired *techniques* on waste recycling/upcycling and reuse. For the aforementioned highest utility and value to be achieved, information flows must be enabled and maintained, for decision-making processes to be placed. As such, a Circular Economy model needs to be a data-driven one for achieving its goals:

Definition 1. *Smart, or data-driven Circular Economy is the utilisation of reactive, adaptive, autonomous or collaborative objects and systems for economic and environmental value creation (Langley et al. (2021b)).*

The management of finite resources and assets within a data-driven CE ecosystem is coordinated by data flows. Since data is considered as an asset of high value and regarding Clive Humby, who back in 2006 claimed that "*data is the new oil*" Olowononi, Rawat, and Liu (2020) to emphasise how valuable data is (Kershner (2021)), it can be seen that CE would need to be data-enabled or data-driven, to be able to deliver what is evangelises. The interaction of the CE with intelligent assets and IoT paradigm creates data structures and patterns for a "*circular-by-design*" approach to be adopted.

Currently, an asset management prevailing pattern includes `Location`,`Condition`, `Availability`. `Location` and `Availability` properties refer to the geolocation and the state of an asset. It turns out that these two attributes are sufficient to take advantage of highly profitable data-driven CE business models, such as Uber and Airbnb. The `Condition` property is more esoteric to the CE itself as it is used to describe the state the respective asset is in terms of its lifecycle. An example definition of this property is `{Condition::good|require_repair|recycle}`. A complete treatment of this concept is presented in Miaoudakis et al. (2020).

The adoption of a maturity model facilitates the structuring and streamlining of the "*CE readiness*" of a city against a set of dimensions. Maturity models are widely used in business performance to identify the strengths and weaknesses of a business and provide benchmarking information. Some of the popular maturity models include OPM3, CMMI, P3M3, PRINCE, BPMM, and Kerzner's Project Management Maturity Model (Khoshgoftar and Osman (2009)). There are differences among these maturity models in terms of factors, number of levels as well as application domains(Khoshgoftar and Osman (2009)).

For this research to be facilitated, the maturity model for smart circular cities as described in *IDEAL CITIES* project (Ideal-Cities (2018)) has been employed. The adopted maturity model illustrates the technological roadmap for a city adopting a CE agenda. In Figure 3.5, the maturity model is outlined (Ideal-Cities (2018)).

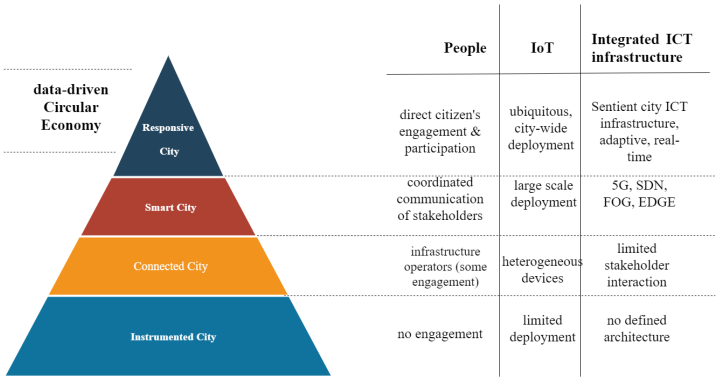

FIGURE 3.5: A maturity model for a smart, circular city (adapted from Ideal-Cities (2018))

- **The Instrumented City** refers to the initial transition stage. City embeds sensors and devices constellations on the physical infrastructures (e.g. street lights, bridges, gas pipes, the grid). On this maturity level, the employed devices conduct *constrained* tasks for facilitating specific purposes. The employed, equipped with sensors devices perform constrained tasks in order to facilitate narrow and specific purposes An example is the smart meters installed for electricity metering purposes in households. At this stage, there is no data exchange between stakeholders and the usage of this data is constrained.

- **The Connected City** is the second stage of transition. Connectors among different constellations have been placed. Even connectors are in place, there is no actual exploitation of the available data. Stakeholders at this stage are still constrained, making use of data for specified services within particular sectors or domains, despite the increased data heterogeneity.

- **The Smart City** is the third stage of transition. All city assets are fully interconnected and data is available to all city members, who can obtain high levels of situational awareness. Operators of infrastructures, utility and service providers can conduct intelligent processing and the local government stakeholders can perform global processing and maintain an overview of the city's operation. The activities of a smart city environment take place as "back office" operations. A smart city can be considered an heterogeneous environment, since it includes different purpose devices and technologies that provided enhanced services to stakeholders, citizens and visitors, though their personal devices, such as smart phones, wearables and tablets. Taking into consideration the inter-connectivity and heterogeneity of a smart city, the volume of data that is produced can be considered as vast and facilitates different aspects and services of a city.

- **The Responsive City** is the last and highest stage. It can be considered as the city's *self actualisation* level, in resemblance to Maslow's hierarchy of needs. At this stage of the transition, every part of a city is in a complete sync with its counterparts. In this terms, every part of city, humans, intelligent assets and infrastructures, stakeholders and authorities have access to information, in an

appropriate and accessible format, in real time. Thus, the whole city, its infrastructures and services can be dynamically reconfigured when it is necessary in order to be prepared to address citizens and visitors needs, by balancing supply and demand. This means that a city at this level is able to adjust itself in relation to circumstances, whenever it is necessary.

A representative case study is the gatherings of people, such as social events or incidents, where the safety of citizens and visitors is the first priority. In addition, the needs of citizens and visitors may be addressed before they are expressed by the city itself, avoiding difficulties and responding before they take place. Offering capabilities to the city's assets to participate in real-time decision making by re-configuring its resources in order to meet the needs of the stakeholders and beneficiaries, defines in essence the *sentient city*.

3.6 Smart Cities Use Cases

Currently, there are over 200 smart city initiatives with at least 40 of them globally have adopted circular economy principles. Cities that have already adopted a circular economy agenda are not necessarily defined as smart as the have not adopted and implemented smart city infrastructure components. As such, circular cities without smart city agenda may have lack of data availability (Ideal-Cities (2018)).

Some smart cities use cases include Amsterdam, Copenhagen, and Barcelona. Their roadmap for achieving a level of smartness is presented below:

3.6.1 Amsterdam

Amsterdam was one of the first European cities that adopted both smart city and circular economy agendas. The transformation of Amsterdam into a smart city began in 2009. The first step of the transition was to keep detailed records of 12K records in 32 sectors in the city. This is a task that has been successful in a short period of time.

Amsterdam was certified with the International Standard (ISO 37120) on Sustainable Development of Communities- Indicators for City Services and Quality of Life, in 2014, along with 20 other cities by the World Council of City Data (WCCD) (WCCD (2018)). The ISO 37120 is a set of 100 indicators, categorised under 17 Sustainable Development Goals (SDGs), developed using the Global City Indicators Facility (GCIF) framework.

Amsterdam is involved in more than 80 pilot projects that address the needs of citizens and visitors since 2014. The main processes for facilitating these projects were related to integration of necessary infrastructures and technologies and the implementation of related applications. Stakeholders of these projects are members of private and public sectors of the city and the aim of these projects focuses on the management of waste, energy, parking and the creation of tailored application for addressing specified challenges within Amsterdam.

In addition, Amsterdam was one of the first European cities that adopted the Circular Economy model in 2015, being the first city globally that used the big number of sensors and generally the high-level ICT infrastructures to promote innovative data driven projects around the premises of a city. Some of these projects include street lights that switch on only when they detect movement and office lights that turn on detecting employees' smartphones. Due to this high-level data driven infrastructure, the flow of data for the needs of the city is pretty easy among individual projects. One of the most representative examples of circularity application is the

office building the *Edge*. The *Edge* building houses the headquarters of Delloite in Amsterdam that is considered as the most intelligent office building in the world (Vayona and Demetriou (2020)), since it obtains more that 28K sensors and state of the art data centre, which constantly monitor and control the building internal environment.

3.6.2 Copenhagen

Copenhagen is another representative example of smart city and Circular Economy agendas adoption in Europe. Copenhagen is one of the leaders that has adopted the smart city paradigm, receiving many awards and recognition. One of the biggest achievements was the reduction of carbon emissions, making the city the first carbon-neutral city in the world by 2025.

The main goals of Copenhagen transition to smart city is the increase of quality of life and the growth of a greener city (Niras (2018)), focusing also on the health, smart citizens and smart learning. Currently, Copenhagen provides core services that can be categorised in four sections. These sections include Big Data city flow, asset tracking, sensor platform, and cost efficient data connection (Digital (2018)).

The CE has recently been on the agenda of the city and the Danish government, using platforms such as Gate21 that provide information about the city's life lab. In addition, the CE Agenda is incorporated into primary and secondary school programs, as well as re-education and vocational training, to emphasise its importance as an important part of citizens' lives (Ideal-Cities (2018)).

3.6.3 Barcelona

Barcelona is considered as smart city since 2014, when it was recognised by the European Commission. The story of transition of Barcelona to a smart city goes back to 1990s, when authorities of the city and organisations were planing and investing on relating projects. Information and Communication Technologies, such as integrated sensor networks and WiFi networks is a key factor in developing sustainable, green cities that facilitate innovation, access to information and collaboration among citizens, governments, and academic institutions, for improving the efficiency and quality of public services and life.

The team Smart City Barcelona that facilitated the development of smart city plan was created by Xavier Trias, after his election as major of Barcelona in 2011. 12 use cases have been identified by Smart City Barcelona for intervention, which include environment, ICT, water, energy, matter, mobility, nature, built domain (public and private), economy and Laws, information flow, open government, and public and social services. Based on these areas, 22 programs have been launched in 200 projects (Gascó-Hernandez (2018)).

3.7 Technological Enablers

Technological enablers refer to all the technologies and paradigms that are employed in order for the aims and the challenges of a smart city ecosystem to be addressed. The technological enablers involve ICT infrastructures and paradigms that are able to automate various processes and facilitate various services within the realm of a smart city ecosystem. The technological enablers may include novel and innovative technological paradigms, such as IoT paradigm, Cloud and Edge Computing, and DLTs.

On the other hand, due to the novelty of these paradigms, the expansion of the threat landscape and the challenges that the adoption of these technologies may rise should be taken into consideration.

3.7.1 IoT

IoT paradigm is related to networks of physical devices, equipped with sensors, actuators and processors that obtain unique identifiers and can be connected to the Internet and exchange data between each other seamlessly, without requiring the human factor. The connected devices number increases rapidly and is anticipated to grow to 26 billion by 2020. It is 30 times the estimated number of devices used in 2009, far exceeding the 7.3 billion smartphones, tablets and PCs expected to be used by 2020 (Lei et al. (2017)).

The IoT systems architecture includes three layers, the Perception Layer that involves employed devices which are Internet enabled and generate and exchange data through the established Internet communication networks, the Network Layer that includes combinations of short-range communication network technologies, such as ZigBee and Bluetooth, and Internet technologies, such as Wi-Fi and 5G for longer distances, in order to transmit data to a nearby gateway and the Application Layer that includes all the services that IoT paradigm may facilitate, such as smart homes, smart vehicles, and smart cities, where data is received and processed (Talari et al. (2017); Lei et al. (2017); Mahmoud et al. (2015)).

As Internet of Things networks gain popularity, vulnerabilities and attacks take advantage, providing extensive threat landscape. As such, protection of IoT devices and networks from sophisticated cyber security methods is critical and essential.

IoT Security and Privacy Challenges

In the last two decades, computing and communications technologies have gained ground bringing a plethora of new appliances along. The IoT paradigm includes everyday objects, such as home devices, cameras and wearables that can be controlled through mobile devices, such as smart phones, laptops and tablets. All these devices are interconnected, they communicate with each other, they generate and exchange data, facilitating specific purposes (Mahmoud et al. (2015)).

Due to the interconnected nature of the IoT paradigm, the related applications come along with new security and privacy challenges. With IoT gaining more and more ground, connecting different, heterogeneous sectors, the threat landscape is evolving rapidly. New vulnerabilities and exploitation techniques have made their appearance affecting even critical infrastructures and causing significance damages. Attacks that target to the constrained nature of IoT devices have been evolved and multiplied over the last years threatening even human lives, especially in cases of compromising medical devices.

Understanding, preventing, and protecting this highly networked cyber-physical world requires a comprehensive survey of known threats and vulnerabilities in the IoT paradigm. Some of the threat landscape of IoT are presented below:

- **Interoperability:** Interoperability challenges rise due to the variety of networks operating systems and programming languages that coexist within the same environment (Alur et al. (2016));
- **Openness:** For an IoT system sustainability to be achieved, system openness is critical in order to be able to be extended and re-implemented in new ways.

Openness of IoT systems facilitates the access to functionality, human interaction, security and privacy (Alur et al. (2016));

- **Security & Trust:** Data acquisition, processing, at rest and in transit related challenges are posed in IoT systems and Wireless Sensors Networks (WSNs). Especially, in terms of a smart city ecosystem, where vast amount of data is generated from employed smart devices and network data flows, attention should be given to both cyber and physical risks, due to the interdependency between the two plains(Borgia (2014));

- **Scalability:** Scalability of IoT systems increases by the deployment of more smart devices, the upgrade of network with middleware and the enhance of application layer by using more brokers and APIs, adopting more sophisticated methods, regarding security and privacy, while minimising interoperability issues. Network scalability and data scalability indicate the two levels of scalability (Borgia (2014)).

In addition, apart from the security and privacy issues, the constrained and ephemeral nature of the IoT paradigm may be considered as a challenge. Especially, within the realm of smart cities ecosystem, the vast generation of data increases the concerns related to the handle of it from the technological enablers. Due to the constrained computational and communication capabilities, the IoT paradigm may increase issues related to the maintenance of potential digital evidence for facilitating potential investigations after an incident.

3.7.2 Crowdsourcing and Crowdsensing

Crowdsourcing model refers to the source model of faster problem solving by the contribution of humans and companies through the Internet. Some of the most representative examples of crowdsourcing model application include Linux and Wikipedia. The contribution of this model may be considered as valuable. It primarily separates and assigns tasks of the same work to different users in order to get a rapid solution to an issue. During the crowdsourcing process, various ideas are gathered, filtered and combined to provide the final solution to each issue (Schuurman et al. (2012)).

The advantages of crowdsourcing model includes low cost, quality, flexibility and scalability (Doan, Ramakrishnan, and Halevy (2011)). Furthermore, crowdsourcing process is typically a man-to-machine process.

Crowdsensing, also known as mobile crowdsensing, refers to techniques, where a large group of people obtaining personal and smart devices, equipped with sensors, collect and exchange data with the intent of extracting information to measure, map, analyse, estimate, or predict processes of common interest. Crowdsensing refers to the extraction of data for helping public. Crowdsensing techniques are part of the crowdsourcing model and replaces the old techniques for gathering information. In addition, it is an alternative way for gathering information without the cost of obtaining and maintaining special equipment, such as sensors. A project called Air-Cloud, which is a system for monitoring the concentration of PM2.5 in China, is an example of crowdsensing employment. The crowdsensing technique consists of two components, a mobile component for data collection and a central server for data storage and analysis (Alvear et al. (2018)).

3.7.3 Cloud Computing

The Cloud Computing is the on-demand computer system resources availability, especially data storage and computing power, without the user direct data active management. In general, the term Cloud Computing describes the centres of data that are located around the Internet, available to users. The basic Cloud Computing features are presented below (Mell, Grance, et al. (2011)):

- On-demand self-service refers to provided services by Cloud and includes computing capabilities without human interaction requirements with service provider;
- Broad network access is related to the services that are available through network, Internet accessed by using devices, which support various client platforms, such as laptops and workstations;
- Resource pooling refers to the ability of Cloud Computing platforms to serve more than one customer by assigning dynamically physical and virtual resources to users based on their needs;
- Rapid elasticity refers to the services provided by Cloud Computing platforms that can be elastically provisioned and released dynamically to meet the needs of consumers;
- Measured service is related to services that are automatically regulated and readopted as needed by utilising a metering capability at a level of abstraction appropriate for the kind of service. The use of Cloud Computing resources can be monitored and managed in order to maintain transparency for both the supplier and the user of the service.

The Cloud Computing includes various service models. The main service models are the Software as a Service (SaaS), the Platform as a Service (PaaS) and the Infrastructure as a Service (IaaS). Software as a Service (SaaS) model refers to the provided Cloud services in an application form. Applications are available to users through the Internet Interface via a web browser or though a program interface. The term Platform as a Service describes the services solutions, created based on customers demands. Costumers cannot manage or configure Cloud infrastructures, but the can change the setting of application.

Finally, the Infrastructure-as-a-Service model refers to the use of Cloud Computing as an infrastructure that allows customers to deploy, run and use software, including operating systems and applications. This service model does not allow clients to manage and control the underlying Cloud infrastructure, but it does allow them to control the operating system and the applications over it (Mell, Grance, et al. (2011)).

Cloud Security and Privacy Challenges

The Cloud Computing provides promising facilities and benefits to various organisations, companies and individuals that seek for alternatives, regarding their data storage and management, their services and their relationship with others. On the other hand, although Cloud Computing is considered as an evolved enough technology there are still some barriers that affect its performance. Security and privacy vulnerabilities and threats are included to these barriers, since many Cloud Computing services suffer from various cyber attacks, some of them common and some of

them more sophisticated and tailored. Furthermore, the heterogeneity of providers and services deteriorates the vulnerable Cloud Computing. Many researchers have discussed the privacy challenges in Cloud Computing and summarise them, as it is essential since various types of data are stored on Cloud Computing. Cloud Computing challenges include risks against confidentiality, integrity and availability as well. In addition, potential attacks that can compromise Cloud based systems involve SQL injection, Indirect Denial of Service, cross scripting and metadata spoofing attacks (Basu et al. (2018)) .

3.7.4 Edge Computing

The term Edge Computing describes the technologies that enable computations at the edge of the network. Edge of the network term is used for defining all the computing and network resources located among data sources and Cloud Computing services. Edge Computing uses Radio Access Network and aims to enhance the performance of network, by reducing latency, increasing its efficiency and providing satisfactory services to end users. Edge Computing main characteristics include low latency, proximity, high bandwidth and real-time insight into radio network information and location awareness, as data is collected and processed closer to clients. Edge Computing applications demand high bandwidth and low latency settings. As a result, service providers for dispersed data centres are positioned at the Edge Computing. Edge Computing may be accessed through a variety of methods, including wireline. Edge Computing is the development of mobile base stations and one of the key technologies underlying 5G networks, along with Network Functions Virtualisation (NFV) and Software-Defined Networking (SDN).

This contributes to the demanding requirements related to 5G throughput, latency scalability and automation, helping to transform mobile broadband network into a programmable world (Hu et al. (2015)).

Edge Computing Security and Privacy Challenges

The Edge Computing enables the storage and processing of data, such as Cloud Computing, adopting a decentralised way. As such, Edge Computing is considered as a promising technology in recent years, since it is key enabler for other technologies, such as the IoT paradigm.

Some of the features of Edge Computing, like content perception, real-time computing and parallel processing bring new challenges that affect stored data security and privacy, which are not addressed even in other preserving computing paradigms, such as Cloud and Fog Computing. These challenges should be identified and addressed, since Edge Computing is part of several sectors infrastructures, in Responsive and Smart cities technological enablers, as well. The fact that security and privacy vulnerabilities can be compromised, brings significant concerns regarding the adoption of Edge Computing solutions, although it comes along with various opportunities.

Furthermore, since some of the main features of the Cloud and Edge Computing are the interconnectivity, and heterogeneity. The employment of the Cloud and Edge Computing by various service providers and sectors' infrastructures. In addition, the employment of different Cloud and Edge providers may be a challenge related to the maintenance of data stored in different locations, making the identification of data sources and storage location, as well as the retrieval of data during or after the occurrence of an incident and the beginning of a digital forensic investigation. From

a digital forensic perspective, the interconnectivity and heterogeneity of the Cloud and Edge Computing paradigms might be a nightmare, especially within the realm of technologically advanced ecosystems. The rapid identification of data sources and the retrieval of data that can be used as digital evidence during the incident response are two critical steps for the beginning of an investigation that will answer to questions, such as who, when, why, how and where. Thus, the identification of data sources, collection and preservation of data as digital evidence before an incident takes place is important in order for the time and cost of an investigation to be reduced.

3.7.5 5G

The evolution of wireless communication is critical, based on the increase of demands regarding wireless communication. The wireless communication has changed completely the way society exchanges data. The data rate, mobility, coverage and spectral efficiency increase based on the evolution of wireless technologies. 5G networks are the later version of mobile Internet connectivity and its main advantages include faster speeds and more reliable connections on smartphones and other devices. The frequency band where 5G networks operate range between 28GHz and 60GHz. This range is known as millimetre wave spectrum.

The main goal of the fifth generation of mobile communications is the increase of capacity, comparing with the current 4G, providing higher mobile broadband users density and enabling device-to-device and machine communications. 5G evolution target involves the addressing of the needs of the IoT paradigm, industrial and cyber-physical employment, as well as the Internet of Everything (Belmonte Martin et al. (2015)).

In 2016, 5G action plan of the European Commission was introduced, which included the certitude of commercial 5G deployment at a EU level by the end of 2020, as well as the 5G deployment for all the European urban areas and important transportation paths by 2025 (European-Commission (2016)). In 2019, various European contractors, such as Vodafone, Orange and EE started the deployment phase of 5G. 5G facilities, such as base stations and antennas have already been settled in Finland, Estonia and Austria.

In order for 5G commercial services to become available to public, operators must take into consideration various processes, including 5G roadmaps, spectrum and early deployment trials (Pujol, Manero, and Jaffal (2018)). The evolution of 5G may facilitate the IoT paradigm and wireless networks. By reducing communications delay and increasing capacity, 5G enables the interconnectivity of millions of devices within a city environment, expanding the IoT paradigm and making gain popularity. On the other hand, the evolution of 5G technology and the deployment of a plethora of wireless protocols and heterogeneous networks, which collaborate between each other may arise security and privacy challenges. The European Commission has already released cybersecurity of the 5G related recommendations and guidelines regarding the performance of resources management and risk analysis at a national level, collaborating with ENISA (European-Commission (2019)).

5G involves five significant elements that are listed below (Wei et al. (2016); Rappaport et al. (2013)):

Millimetre Waves

As millions of smart devices work on the same radio frequencies, the latter get packed by under 60GHz working devices. Millimetre waves occupy the space between the 30GHz to 300 GHz spectrum, releasing the space for facilitating the connected devices. Although millimetre waves proposal is promising, including advantages, such as bigger bandwidth rates and always-on availability through service providers, it includes some drawbacks as well, related to their performance disturbing by building, walls and environmental phenomena, such as rain and clouds (Wei et al. (2016); Rappaport et al. (2013)).

Small Cell

The implementation of millimetre waves rises challenges related to the efficiency of traditional cell towers, as they get disrupted by the big number of obstacles, forcing them in losing signal among towers. The solution to this issue is the deployment of multiple low-power, mini base stations in a short range between obstacles, assigning devices to particular base stations while they are on the move and enabling them to preserve their connection active (Wei et al. (2016); Rappaport et al. (2013)).

Massive MIMO

Massive Multiple input multiple output (MIMO) base stations can accommodate up to 8 times the number of ports utilised for antennas of cellular connections. As consequence, the networks capacity increases, as well as multiple signals that cause serious interference, causing risks addressed by an adversary (Wei et al. (2016); Rappaport et al. (2013)).

Beamforming

Beamforming is in charge of the proper transmission of stream data delivered to specified users. MIMO base stations can triangulate each signal and sort the destination of each packet using signal processing techniques, allowing them to transmit data streams to the proper receiver (Wei et al. (2016); Rappaport et al. (2013)).

Full Duplex

The Full Duplex has been introduced for eliminating interference when sending and receiving data on one and the same frequency. This scheme works as a signal system that acts as a traffic light between streams that use the same frequency for avoiding interference (Wei et al. (2016); Rappaport et al. (2013)).

5G Security and Privacy Challenges

Since the 5G is key enabler, not only for Smart and Responsive cities, but for several city's sectors, its cybersecurity resilience is essential and various vulnerabilities and threats must be addressed. Recent research works reveal potential security and privacy challenges that affect 5G services, infrastructures and users (Sicari, Rizzardi, and Coen-Porisini (2020); Lai et al. (2020); Ahmad et al. (2018)). Vast amount of data is exchanged through a 5G network among various devices that are connected over this network. In some cases, these devices may be vulnerable towards several kind of attacks, such as eavesdropping, impersonation, man-in-the-middle and Denial-of-Service (DoS).

3.7.6 Blockchain

The term Blockchain refers to a Distributed Ledger Technology (DLT) and describes a sequence of blocks that consist of groups of verified transactions list, which is called the ledger that are kept by the network as records without being possible to be altered. A copy of the ledger is obtained and stored by all the participants of a Blockchain network, the nodes. Each block obtains two parts, the block header and the main part of it that includes a transaction counter and transactions. The block header part contains the header of the previous block in order for the sequence of the chain to be achieved.

Each node of a Blockchain network owns one pair of asymmetric encryption keys, a public and a private, which are used for signing and verifying transactions that are exchanged among nodes. Sender signs a new transaction with the private key and receiver can verify this new transaction by using the public key of sender. As such, data integrity may be checked. There are three types of Blockchain that include public, private and consortium Blockchain.

The Blockchain technology is decentralised, thus there is no need for a centralised authority to manage a Blockchain network. In order for the consensus to be achieved within a network and reliability and consistency of transactions to be ensured, consensus mechanisms are used. Some of the most popular consensus mechanisms of Blockchain include the Proof of Work (PoW), the Proof of Elapsed Time (PoET), the Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof of Stake (DPoS). Each consensus mechanism has various strengths and weaknesses in terms of node identity management, energy savings, adversary tolerance and the requirements of each Blockchain application.

Also, as throughput is defined the number of transactions that are stored in the ledger per second. The throughput of convectional Blockchain, such as is constrained, as in Bitcoin. The throughput of Bitcoin is limited to seven transactions per second, due to the complexity of the PoW consensus mechanism that is used (Zheng et al. (2017)). The Blockchain work flow is presented in Figure 3.6

The creation of a transaction is the first step in the Blockchain network, in a request form. The requested transaction is broadcasted into a Peer-to-Peer (P2P) network. Other nodes can validate the status of nodes and transactions. Once a transaction is verified, it is combined with other transactions and stored in new block that will be added to the chain as a record. Once the new block is generated and added to the chain, all the copies of the ledger are updated. The sequence of blocks is presented in Figure 3.6.

The Blockchain technology obtains various features related to security and privacy, such as strong cryptographic techniques, immutability, transparency and resilience. The distributed dimension of Blockchain increases the resilience of it (GSMA (2018)). Due to the decentralised and distributed features of the Blockchain, the ledger can be stored across different systems, devices and locations of the network (Kosba et al. (2016)).

The security and privacy of the network are achieved by using strong cryptographic techniques that are applied over the ledger and the network in general. Some of these techniques include hash functions, asymmetric cryptography, public and private key scheme and digital signatures (Fernández-Caramés and Fraga-Lamas (2018)).

The Blockchain technology has become popular as part of the most famous cryptocurrency, the Bitcoin (Nakamoto and Bitcoin (2008)). Even though, its capabilities can be applied over many other existing technologies and fields in order to get

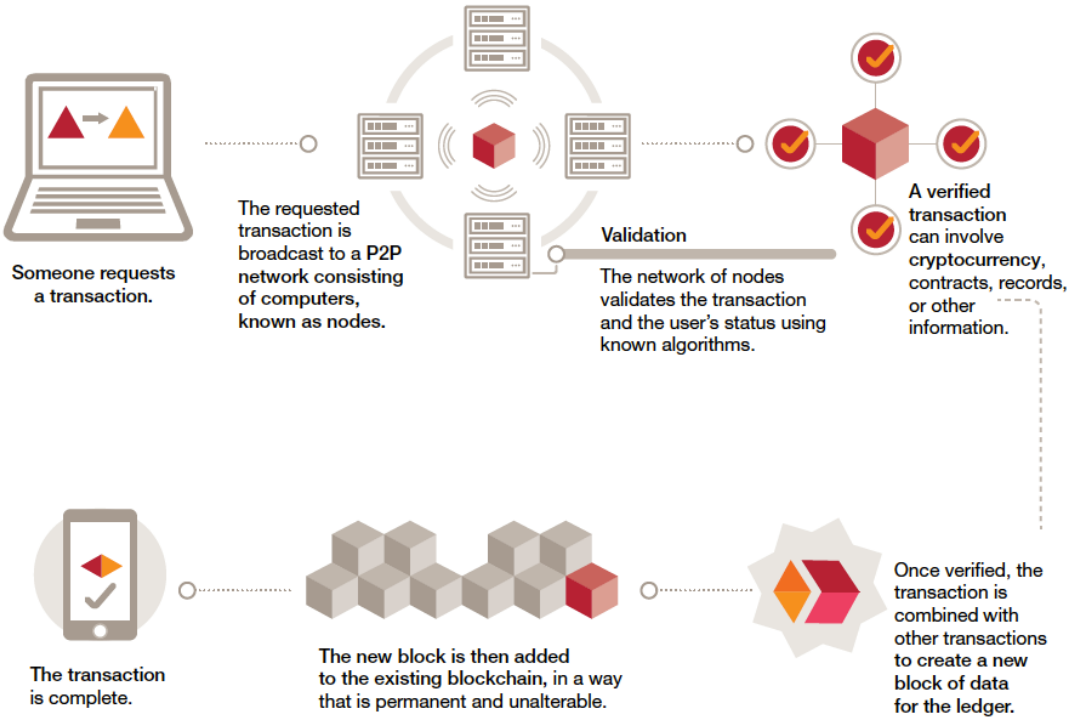

FIGURE 3.6: How Blockchain Works (Baru (2018))

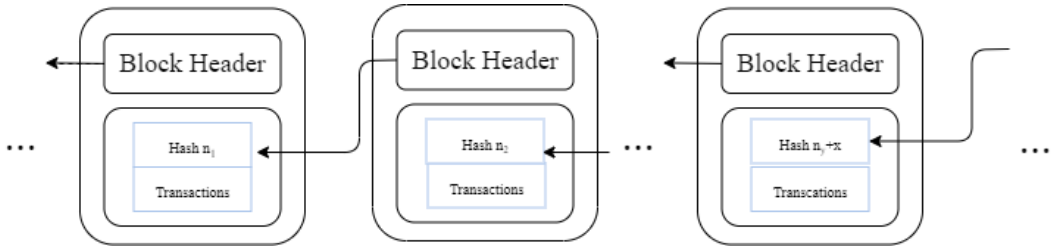

FIGURE 3.7: Block sequence in the chain

improved. It had been already applied over financial market, mainly due to its involvement into cryptocurrencies schemes, IoT, supply chain, e-voting, healthcare and storage.

Furthermore, it provides security where it is applied due to the strong cryptographic techniques that it uses and resilience due to its distributed nature.

3.7.7 Blockchain Features

Some of the fundamental features of the Blockchain include:

- **Transparency**: Every participant of the Blockchain network can have access to the records of the distributed ledger and check the data that is stored there. The participants can check the digital signatures over the data, so they can check the integrity of it. Moreover, all of them have access to the same data on the distributed ledger (GSMA (2018)).
- **Immutability**: Once a participant-node of the peer-to-peer network verifies a transaction, this is recorded, stored on the distributed ledger and becomes part of the transaction history of the network. It is extremely difficult for a node to change the history of the distributed ledger (GSMA (2018), Xie et al. (2019)).

- **Security**: Strong cryptographic techniques are applied over distributed ledger technology in order to secure the records of it. Furthermore, the fact that every node in the network keeps a copy of the ledger records, makes the technology more secure (GSMA (2018), Xie et al. (2019)).
- **Decentralisation**: It is the main feature of the Blockchain technology. The distributed ledger technology does not rely on a central authority, who checks the network, the performance of it and approves transactions. Blockchain transactions have their own proof of validity and authorisation to enforce the constrains. Since the Blockchain uses consensus mechanisms in order for the nodes to work *properly*, the transactions can be verified and processed very fast (GSMA (2018); Xie et al. (2019)).
- **Non-repudiation**: All transactions of Blockchain-based systems are digitally signed and stored in blocks, which are linked and secured using hash functions (see Figure 3.7). As such, all the modifications can be detected making the ledger immutable (Xie et al. (2019)). Every participant may be considered as *"unable"* to make changes to the ledger and to refuse their involvement to the network.

Blockchain Security and Privacy Challenges

Blockchain has attracted a great interest and it is considered as an innovative technology that has been adopted for various purposes, since it facilitates different kinds of services and provides a wide range of opportunities. Thus, many companies and organisations have invested vast amount of money on the Blockchain. This explosion of Blockchain applications has changed a lot the way in which systems are designed, enabling new ways of keeping records of all the actions that have been taken place inside a network, and the way in which distributed untrusted entities communicate between each other.

On the other hand, despite the opportunities and the innovation of this technology, the Blockchain may be exposed to vulnerabilities and comes along with new risks that may not be discovered yet. These risks can affect the organisations' and companies' infrastructures and damage their operation.

In addition, another challenge related to the Blockchain is the number of generated blocks, and the increase of the ledger size. In particular, in the case of the employment of both, the Blockchain and the IoT paradigm may raise challenges related to the performance of the last mentioned, due to the devices limited capacity. The increase of the ledger size in accordance with the constrained memory capacity and capability of the IoT paradigm may rise challenges related to the preservation of data.

3.7.8 Blockchain Vulnerabilities

51% Vulnerability

This vulnerability is related to the Proof of Work consensus mechanism, which demands a lot of computational power for the miners and the cost for producing a PoW value is very high. For reducing the mining process cost miners may be gathered into *mining pools* for calculating PoW values together.

The 51% vulnerability is enabled in case of the hashing power of a mining pool or of a single miner is more than 50% of the whole network. It has to be mentioned

that obtaining more than 50% of the hashing power of the whole network is not an easy achievement.

Attackers can exploit this vulnerability of Blockchain networks in order to take the control over the whole network. As such, controller is able to change or delete transactions that are stored in the ledger, reverse transactions and initiate double spending attacks, change the order of transactions for validation, make unable other miners to conduct mining process and obstruct the validation process of transactions in the waiting list.

Furthermore, the 51% vulnerability can take place when a single miner or a pool of miners obtain more than the 50% of the total number of cryptocurrencies of a network (Li et al. (2020)).

Transaction Privacy Leakage

Traceability is fundamental feature of the Blockchain for avoiding inappropriate behavior of users and ensuring protection of the network.

On the other hand, taking measures for protecting privacy of users is essential. In order to protect the privacy of its users, Bitcoin and Zcash networks provide one-time accounts in order to store the cryptocurrencies that users receive. Furthermore, the existence of the private key prevents attackers from revealing the identities of involved users of every transaction.

In the case of the Monero cryptocurrency, users can involve some chaff coins in the new transaction in order for attackers to not be able to know the number of coins that it has spent. The name of this process is mixing. Blockchain technology does not provide strong privacy in general. According to Möser et al. (2017), empirically evaluated two linkability related weaknesses of mixing strategy on the Monero. The research revealed that 66,09% of transactions in this system do not include chaff coins. This fact can lead to the conception that the privacy leakage of the senders of these transactions is feasible (Li et al. (2020)).

Smart Contracts

The smart contracts term refers to computer programs and/or transaction protocols that are executed automatically, triggered by a new transaction within a Blockchain network (Christidis and Devetsikiotis (2016)). Smart contracts may include major vulnerabilities to their operation and some attackers create criminal smart contracts in order to gain access to confidential information, to steal cryptographic keys and modify stored data.

Some of the major vulnerabilities of smart contracts will be presented below (Li et al. (2020)) :

- **Transaction ordering dependence**: This vulnerability is triggered when a miner validates a block, which includes two transactions that use the same smart contract. The order in which the transactions will be committed is very important. As such, if the order changed, the state will be different and the vulnerability is triggered. This fact affects the final state of the Blockchain. For instance, if the state is a, it can change to a', it depends on the miner.

- **Timestamp dependence**: Some contracts are based on timestamps. Some of them are triggered due to the timestamp that a miner has applied on the block regarding their local system. If an attacker can achieve the change of the timestamp over a block, these smart contracts are vulnerable.

- **Mishandled exceptions**: This category of vulnerabilities is triggered when a smart contract calls another one. If one of them does not work properly and the first is not able to detect the issue, the latter may be vulnerable.
- **Re-entrancy vulnerability**: The state of a contract account changes after the complement of the smart contract invocation. This vulnerability is triggered when an attacker uses the intermediate state in order to make calls to the smart contract. In the case that the smart contract involves transaction with Ether, the latter may be stolen.

3.7.9 Big Data

Big Data may be considered as technological enabler of a smart city. The usage of the IoT paradigm enables the generation, exchange and collection of data. This fact may enable the concentration of vast amount of data that can be stored and analyses in order to facilitate various services, sectors and applications of a smart city, producing essential patterns and enhancing decision making processes. Use cases related to Big Data analytics application include public healthcare sector, transportation, public safety, energy and water management.

The employment of Big Data plays a key role for enhancing provided services of a smart city environment through the usage of the right tools and methods for an effective data analysis. This data analysis will improve and contribute to the communication and the development of new services that will benefit citizens, improve the urban environment and give a better customer experience. Data generated by the interaction of employed technological enablers and citizens with the smart city infrastructures should stored and proceed for analysing purposes to address current demands of the city environment.

Although the analysis processes of Big Data within a smart city environment may be considered as essential and helpful, there are related challenges that must be addressed. The first challenge is related to the cost of analysing vast amount of data. Another challenge is related to the low degree of automation in quick queries and the retrieval of Big Data. During an emergency situation, where data retrieval is critical, the process must be fast. The automation of these systems in terms of data retrieval and rapid query response should be considered. Using these automatic procedures, it will be feasible, for instance, to retrieve data while conducting prior warning and successfully preventing illegal acts. Automation will enable preventive interventions, emergency situations requiring rapid insertion and post-event measurements (Pan et al. (2016)).

Big Data technology is critical for smart cities. Yet, since it is constrained by the availability of other technological enablers and tools, such as the IoT paradigm and Cloud Computing, its flow must be maintained. The generation, analysis and storage of Big Data are all dependent on other tools and technologies, as well as their availability (Hashem et al. (2016)).

Finally, mining large data for knowledge purposes is challenging. Mining large amount of data should be a meticulous procedure in order to acquire valuable information when it is required. The primary features of Big Data, however, make mining challenging. Data mining from datasets containing geographical information, for example, is a difficult process (Pan et al. (2016)).

3.7.10 Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to a part of computer science and its application is involved with various topics, such as scientific research tools, games, robots control and medical tools. In addition, Artificial Intelligence can facilitate various modern services. The term Artificial Intelligence describes the idea that *intelligent* assets perceive their environment, interacting with it in order to take actions and enhance it (Russell and Norvig (2002); Mitrou (2018)). Artificial Intelligence relies on the ability of intelligent assets to receive training and to predict and anticipate potential events that may take place in the future, based on data analysis. The deployment and the implementation of AI mechanisms enhance the decision making, problem solving, pattern recognition and learning processes (Mitrou (2018)).

The employment of modern technologies and tools for addressing challenges of an urban environment is essential. Furthermore, the employment of devices that facilitate the data flow within a smart city ecosystem provides the necessary feedback for the education of AI-based systems for improving their performance and providing effective services, such as decision making processes. Also, users behaviour can be used as feedback for the education of AI-based systems within a smart city. Useful patterns may be created from this process, easily detected by a system, enabling it to perform autonomously, when it is necessary (Mahdavinejad et al. (2018)).

Artificial Intelligence Security and Privacy Challenges

The evolution of AI and the new paradigms that are deployed based on AI introduce a threat landscape where novel criminal techniques are emerged. Various research works introduce the AI based threat landscape and the malicious usage of artificial intelligent technologies (Brundage et al. (2018); Kaloudi and Li (2020)). The field of Artificial Intelligence consists of two domains, the rule-based and the machine learning based that provide to computer systems to be trained by large datasets. The AI technologies learning approaches provide the opportunities to malicious parties to take advantage of them and perform automated attack processes. The development of novel AI technologies and the evolution of learning capability such as deep learning, reinforcement learning, genetic algorithms and support vector machines may provide to criminals the means for more sophisticated, automated and efficient attacks (Goodfellow, Bengio, and Courville (2016); Kaelbling, Littman, and Moore (1996); De Jong (1988); Pradhan (2012); Kaloudi and Li (2020)).

3.7.11 Machine Learning

Machine learning may be considered as a domain of Artificial Intelligence and provides the ability to machines and systems to be trained without explicit programming to be essential (Mahdavinejad et al. (2018)). Machine learning makes use of sets of information samples, which are called training sets, as inputs to learning algorithms for their training process. Machine learning includes three main categories of learning (Mohammadi and Al-Fuqaha (2018)):

- The supervised learning describes the learning category in which the training set includes the input vectors samples and labels that are the matching suitable targets vectors;
- The unsupervised learning refers to the learning category that includes only the input vectors samples;

- The category of reinforcement learning is concerned with the issue of determining the best action or series of actions to perform in a given circumstance in order to maximise reward.

Since the amount of generated data in a smart city is vast, recycling processes for data handling are required. Machine learning algorithms that can extract knowledge and useful information from data should be utilised to decrease the quantity of digital waste.

As the IoT paradigm may be considered as constrained, machine learning techniques are employed over IoT devices to acquire the required data in order to preserve only the information that is important for the system. Moreover, there are use cases of machine learning techniques being used to minimise water and energy use. California employed Big Data analytics back in 2017 to secure water during drought conditions. It was accomplished through the use of smart water metres and an intelligent Deep Reinforcement Learning (DRL) based system. The results aided in reducing water usage throughout the summer period and which hours of the day (Mohammadi and Al-Fuqaha (2018)).

3.7.12 Robotics

Smart cities ecosystems provide a fertile ground for employing and testing robots in order for urban services to be improved. Robotics and autonomous systems (RAS) may be considered as an additional technological enabler that may facilitate the initial smart cities services and applications considerably. Various cities cases, such as Tokyo, Singapore and Dubai, have already adopted (Fourtané (2018)). AI and machine learning are employed for facilitating RAS technologies for making decisions and addressing processes without the direct contribution of human (Macrorie, Marvin, and While (2021)).

Various use cases indicate the application of robotics on smart urban environments. One of these use cases includes the adoption of robotics solutions by Olympic Games of 2020 in Tokyo, Japan, where people would be served by smart robots in 20 different foreign languages. In addition, various smart cities projects in Dubai include robotics that address and provide public services, as in Rotterdam, Netherlands, as well (Fourtané (2018)). Furthermore, Singapore introduces robots as physical extension for management and city control of existing systems and their adoption for providing services to hotel clients (Fourtané (2018)).

Potentials applications in security, transportation, sustainability, construction, energy and water management sectors have been identified by Nikitas et al. (2017) research.

For instance, in the transportation sector, there is a number of cases that indicate the adoption of robotics as a solution in smart cities environments, such as the hyperloop and autonomous and connected vehicles, subway trains, buses and boats, which enable the machines driving without the human factor contribution (Dia (2016)).

In addition, the National Science and Technology Council identified new opportunities regarding the adoption of AI and robotics in other sectors, such as healthcare, education and environment management (Felten (2016)) and new AI solutions that include IT infrastructures for smart energy generation and distribution, management of intelligent traffic systems, smart waste management systems, and so on (Tripathi (2016); Golubchikov and Thornbush (2020)).

3.7.13 SDN & NFV

Software Defined Networks (SDN) and Network Functions Virtualisation (NFV) are critical infrastructure technologies for efficiently managing resources, applications and data at prescribed and necessary service levels. SDN provides dynamically configure network typologies capabilities.

SDN is considered as one of the innovation pillars of network infrastructures, allowing the separation of the control and data plains via an open and standard interface that enables network programmability. Examples of SDN technologies include OpenFLow, ForCES and I2RS. SDN along with 5G technologies enable the efficient data forward for meeting all the underlying demands of a smart city environment (Matias et al. (2015)).

NFV refers to an innovative network architecture related to service delivery. NFV leverages IT virtualisation technologies for virtualising entire classes of network node functions into building blocks that may be connected or chained together in order to develop communication services (Matias et al. (2015)). The network may be elastically scaled up or down using SDN and NFV, allowing a city to adapt to changing demands and plan for the unexpected.

For instance, comparable to designating special lanes for emergency vehicles to deal with accidents or life-threatening situations, the network connections will be adjusted to provide capacity for emergency services while reducing throughput allocated to regular *crowd* users while enabling them to merely transmit brief messages rather than video streams that use bandwidth.

3.7.14 Machine To Machine (M2M) Communication

Machine-to-Machine (M2M) communication refers to the direct communication among devices through a wired or wireless communication channel. The M2M communication supports direct data exchange among IoT devices for facilitating smart city services.

Devices in M2M communication are either wired or wirelessly linked to the infrastructure. Wireless access methods include capillary and cellular. Although a wired connection has numerous advantages, such as high dependability, high speeds and low latency, it is not always appropriate for smart city applications due to the expensive cost and lack of scalability and mobility.

The wireless approach, on the other hand, is less costly, uses less power and is more scalable. Nevertheless, it has certain drawbacks, such as a low rate and poor security. The latter instance involves a capillary wireless solution. There is a cellular wireless solution that has addressed the difficulty of capillary M2M solutions and is better appropriate for smart city applications (Hasan, Hossain, and Niyato (2013)).

3.7.15 Human To Machine (H2M) Communication

Human-to-Machine (H2M) communication refers to the interaction between humans and devices which contributes for improving of a smart city services and facilities, since all users may facilitate a service by providing updates on real time and be updated with useful details when it is necessary, at the same time.

Some of the advantages of H2M communication include the ease and speed with which users may be alerted, the flexibility that allows to users to be informed via the system and the quick occurrence reaction to emergencies (Evince-Development (2019)).

3.8 Chapter Summary

In this Chapter the Circular Economy and Smart City concepts are presented. The Chapter starts with the introduction of the Circular Economy model and its business model, as well as its contribution as a mean of maintaining sustainability within the realm of a smart city, the presentation of the smart city concept and the evolution of its definition during the last decades. In addition, for the needs of this research, a maturity model that designates the technological roadmap for a city adopting a CE agenda is adopted and presented, which includes four levels, each of which indicate different technological integration, starting from the lowest, the Instrumented level, to the highest, the Responsive maturity level. The adopted maturity model was initially presented in Ideal-Cities (2018).

Furthermore, the technological enablers of a smart city concept are introduced, referring to all the advanced technological paradigms that facilitate the needs of a city and its citizens, providing solutions to challenges, related to the everyday life. These innovative technological paradigms include IoT paradigm, DLT technologies, Cloud and Edge Computing paradigms. These technological paradigms and their contribution to smart cities concept are defined. In addition, limitations and challenges related to these technological enablers are identified, taking into consideration the fundamental security and privacy principles. The identified technological enablers may be considered as the key data generators within a smart city ecosystem, contributing to the main digital infrastructures of the aforementioned ecosystem and facilitating the exchange of data and the needs of citizens and visitors. In addition, the generation and collection of data by the technological enablers that have been mentioned above may facilitate the identification of vulnerabilities and risks that may affect the whole smart city infrastructures and the collection of potential digital evidence that may help future digital forensics investigations, making a city *ready* to face a cyber security incident.

The aforementioned technologies may be considered as the technological enablers that a smart city ecosystem adopts for facilitating their goals for addressing related challenges and improving citizens every day life. In Chapters 6, 7 and 8, the integration of the aforementioned technological enablers, the identification of potential attack vectors, the vulnerability management within smart cities, and an incident response plan and a digital forensic readiness framework, developed taking into consideration the level of the technological enablers integration and the maturity level that a city has achieved, are presented.

Chapter 4

Use Cases

4.1 Introduction

In this Chapter, a series of use cases related to critical sectors and infrastructures that may exist in a technologically advanced city are developed and presented. The use cases form the basis of the qualitative aspects of this research. These use cases focus on transportation, healthcare, and energy, and concern different maturity levels that a city may achieve. In addition, through the presentation of attack scenarios, the different manifestations of risks across the maturity levels, and the impact of vulnerabilities are presented.

In the first use case, the concept of superblocks is introduced and extended, which was initially adopted by Barcelona city municipality for addressing different kinds of challenges surrounding transportation and traffic.

Although that the superblocks concept was introduced as an innovative and attractive solution for addressing traffic and pollution issues, in its current form and implementation it is considered to be constrained and static. In this research an enriched version of the superblocks concept was developed through the use of technological enablers, illustrating how real-time decision making would allow the superblocks to be dynamic, fluid and reflect the supply and demand at a given point in time. This use case is a representative of a data-driven circular economy approach, but at the same time shows that the high level of integration and the high complexity of interconnected systems results to higher risks from the exploitation of vulnerable devices.

Furthermore, two use cases regarding an Interconnected Healthcare System of a city are introduced and described of how malicious parties may affect various other city's sectors by compromising a part of it. In these use cases, the setup of a particular subsystem of Healthcare is described, the interactions that this subsystem has with smart devices and citizens is presented, as well as the interconnectivity of it with other sectors and infrastructures of city, such as transportation. Also, a use case related to the energy supply of a city is presented, by introducing a cyber security incident and how this may affect the energy sector, as well as others that depend on it.

Finally, the impact of an incident in all four use cases is discussed, taking into consideration the current maturity level that a city has achieved. It should be kept in mind that the impact of the exploitation of the same vulnerability or the impact of the same incident may differ between the maturity levels, and affect more some cities, than some others.

4.2 Superblocks

4.2.1 Related Work

In 2014, Barcelona municipality, trying to propose a solution for traffic and air and noise pollution reduction, and for encouraging citizens to walk and cycle more around city, instead of using cars, introduced a novel model, superblocks. Superblock refers to a new model for restructuring the road network of a city in order for urban mobility to be minimised and quality of life of citizens to be improved. The application of this model starts be choosing urban areas, around 400m by 400m each, and banding or reducing car access into them. The novel proposed Superblocks model is presented in Figure 4.1. In addition, there is a restriction regarding the speed limit within superblocks, since it is confined to 10km/h to 20km/h, giving priority to pedestrians and cyclists. The idea was considered as innovative and the motivation for introducing this concept was the traffic and pollution issues that city should to deal with. Even superblocks idea is promising, they are statically defined areas of city without being able to reconfigured depending on the city and citizens needs. The static approach of superblock may have to be reconsidered and re-evaluated regarding the current circumstances (Rueda (2019)).

Superblocks are predefined areas within a city and may be considered as static. Even though the superblocks paradigm is consider as innovative, the idea of superblocks may be more efficient in a dynamic version. Since the needs of an urban environment are not static and change frequently, we believe that superblocks must not be predefined, static areas. Furthermore, innovative technological paradigms may enable the transition from predefined superblocks, to dynamic and adaptive depending on the current situations superblocks. Superblocks models may be part of a general technological adoption for facilitating various services and operations of a smart city (*Agencia de Ecología Urbana de Barcelona* (2012)).

4.2.2 Software Defined Superblocks

We assert that the primary components of Data-driven Circular Economy model are intelligent assets (Morlet et al. (2016a)), the building blocks of which are the same ICT structures employed for the transition to a smart city. An intelligent asset in the context of a city is any resource capable of creating and consuming information in real time. In essence, this definition reflects upon the IoT devices that are enabled with sensing, actuating and communication capabilities, through which they can bridge the gap between the cyber and physical plane and objects.

The three main properties of an intelligent asset include:

- **Location** refers to the physical location of an intelligent asset and should be available for both mobile and non-mobile assets.
- **Condition** is related to a state of an asset regarding its lifecycle positioning. This information may be described further and indicate if an asset is still in a good condition, if it is close to its expiration or if it needs to be recycled.
- **Availability** includes three possible states of data, available, in-use and out-of-order.

In addition, taking into consideration the Circular Economy properties defined above, the following operational properties need to be defined:

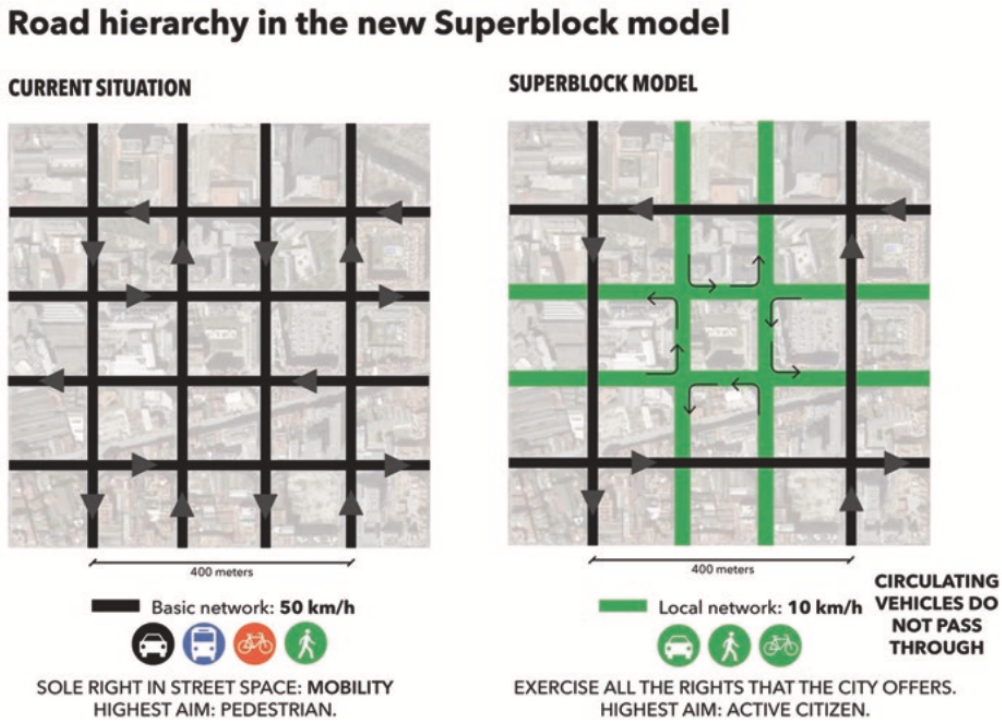

FIGURE 4.1: Networks scheme, current and future. based on superblocks. (*Agencia de Ecología Urbana de Barcelona* (2012))

- **Description** can capture all the characteristics of an assets in order to enable the circular use of the device. This is especially important for constrained and specialised devices, such as IoT sensors, where the hardware profile will be recorded. Regarding physical assets, such as a parking space, their features must be recorded as well.
- **Capability** of an asset may not be easy to be defined, since an asset can involve more than one, as it may serve various purposes. A main capability can be assigned to a particular asset indicating its main purpose and function, as well as additional capabilities. The main capability of an asset cannot change, as it defines the default use of an asset. Additional capabilities may define alternative uses of the same asset and they may change.

Based on the aforementioned, a collection of assets in the form of a UML diagram (see Figure 4.2) and state the attributes that are relevant for describing a CE use case have been identified.

4.2.3 Use Case

The deployment of superblocks model in the case of Barcelona may be considered as ideal, since the city follows a grid structure. Generally, well structured cities may befriend the deployment of a superblock model. On the other hand, as not all cities globally do not obtain a high structure level, the implementation of a superblock model may be challenging.

Bournemouth can be considered one of these cities. In addition, it should be mentioned that Bournemouth faces a major issue related to traffic management. Also, popular areas of the city, such as the beach, the Pavilion Theater and Lower Gardens

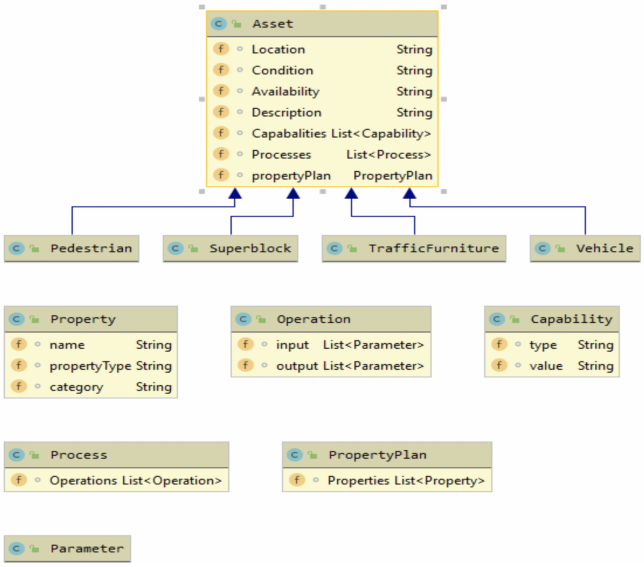

FIGURE 4.2: Software Defined Superblock Orchestration System Model

must be easily accessible. Moreover, Bournemouth becomes pole of attraction for many people, especially during summer, since various events take place in the city, such as the Bournemouth Air Festival, which is the biggest in the United Kingdom. In this case, Bournemouth city should be able to address the need for enough car park space and to provide safe access to the points of interest.

In order for these challenges to be addressed, we believe that the deployment of a data-driven superblock model may facilitate municipality and visitors of the city during a major event. In the Bournemouth city use case, superblock does not refer to a predefined area of city, but to an area that has been transformed to a superblock based on the current needs of the city. Since events may be conducted in various city areas each time, superblocks will be different, settled nearby events area.

The presented use case includes Bournemouth city, UK and various events that take place in different areas of it. Data related to past events can provide valuable information regarding the number of visitors, the needs of city and the availability of car parks.

Depending on this information and the car park slot capacity, Bournemouth city may adopt a dynamic superblock model, instead of a static version. Since the city involves more than one points of interest, superblocks must be able to be reconfigured depending on the current demands of citizens and visitors.

Therefore, decision making algorithms may be responsible for the definition of superblocks areas based on the data that may be collected for various other purposes related to an event and the needs of the city.

Superblocks must be defined based on the current event that will take place to Bournemouth city, the demand for parking slots, the capacity of various parking lots of the city, the distance between the train and bus stations and the region, where an event will take place, and the availability of car park spots of streets around the event region.

The street that has the highest number of available parking spots and connects to the parking lot, where there is more space for more vehicles, as well as the parking lot space, will be designated as a superblock and will have open access while the

rest of the streets around it do not. In this way, superblocks will be transformed from static and traditional, to dynamic and smart, enabled by technological enablers employed by the city authorities.

Furthermore, guests may utilise the locked vehicles parked on the pedestrian streets as lockers to store personal things that they do not want to carry throughout the event. We presume that guests who will utilise this service have arrived in Bournemouth through public transportation rather than their own vehicles. As a result of using this approach, there is no need for traffic controllers to deal with traffic difficulties throughout the event days, as they will be replaced by technology enablers such as Blockchain, IoT networks, Smart Contracts, and all of the technological infrastructures that will be employed.

4.2.4 Example Pattern

The described use case above may be implemented through definition of a set of patterns. A representative example is the use of a vehicle. In this case, the smartness of a vehicle is not measured in terms of its ability to be a self-driven one, as described in the literature, but its ability to increase the resource obtaining two main states, namely `parked` or `moving`. It should be emphasised that the objective of CE and sustainability is not to keep the vehicle moving, but to alter the condition to `inUse` in any of the aforementioned conditions. A vehicle in `moving` state is certainly in `inUse` state. The same can happen if a vehicle is parked. A vehicle may be considered as a storage facility. In this case, a vehicle can obtain the `locker` capability, where the location of it is specified for a period of time, as it is used as a storage space.

In this scenario, we suppose there is a citizen or visitor in need for storage space for their personal things. Assuming that the amount of storage that a citizen or a visitor needs is approximately 200 litres, which may not be able to be facilitated by storage lockers that exist in a city. As mentioned earlier assets within a city, such as smart vehicles, may be provide the necessary storage space if they are available and parked. When executed, the above narrative may be represented as a supply and demand matching exercise. Entity reusability and availability are two critical properties that must be established in a CE context. Entity reusability refers to the ability of using unused entities during a service initialisation. This pattern can be expresses as follows:

- Let $S = A_1, A_2, ..., A_n$ be a number of Assets that are needed for an initialisation of a process;
- Let $A = U_1, U_2, ..., U_n$ be a number of Assets that are unused;
- Let C^A be the Capabilities that the Asset makes available.

Then for every Asset that belongs to S, if there is an unused Asset U that $C^U \subseteq C^A$ then we use U.

In a Circularity context, availability refers to an asset ability to provide all the necessary resources for the successful execution of a process. Thus, the `cAvailability` (as opposed to the established information security domain goal) pattern is defined as:

- Let $P = C_1, C_2 \ldots C_n$ be corpus of capabilities a process needs to be available in order to be successful.

- Let $X = A_1, A_2, \ldots A_n$ be a corpus of available assets.

- Let C^A be the Capabilities that the asset A has.

The union of the capabilities of the available assets must be a subset of P, for a P to be successful.

In accordance with our language standard, the asset Vehicle is defined as follows:

`Asset(type:''Vehicle'',Condition:''Charging'', Capabilities[ Capability: {Storage:250}, Capability: {Transportation:4}], Location:{X,Y})`

In our system, the aforementioned criteria generates a smart car that can transport four people and has a storage capacity of 250 litres. For those citizens and/or visitors, who wish to use these facilities of a smart city, they can ask for storage units availability providing details regarding the needed capacity. Smart city's system may transfer particular demands to the framework `Operation(Capabilities [Capability:{Storage:200}])`.

The demand is executed by the framework via the `cAvailability` pattern, sending to the user the location X, Y of the smart vehicle that will provide the necessary storage service.

4.3 Interconnected Healthcare System

4.3.1 Use Case

Bob is a former employee of the local hospital "*Protection and Healing*", who used to work as an IT technician. His Personal Area Network (PAN) is made up of his personal devices, which include a mobile phone and a laptop. He uses free cloud services provided by two major cloud services providers. He obtains these services illegally and now makes a living through corporate espionage and blackmail. He accesses the Internet through open networks by piggybacking on them, and always away from his home. His personal devices are not registered with any Internet provider and his mobile phone receives only calls and messages.

In a smart city environment, the local hospital, "*Protection and Healing*", uses a system where all electronic devices and patient-related systems have been networked. This has been done for the increase of efficiency of these devices, the reduction of human errors and time to be achieved. This system includes "*intelligent*" medical devices that are obtained by patients and patients records. All the participants of this system are assigned with different access rights, depending on their status (doctors, patients, IT technical, admin, etc.). Through this system, doctors can interact with their patients, providing their services to those who may not have access to the hospital and provide medication prescriptions remotely.

Apart from this system, the hospital has rolled out a new system, where ambulances, which are equipped with sensors, and sensors of traffic control systems of the city can communicate in order for these vehicles to be prioritised in traffic conditions. This scheme is applied especially to streets close to the hospital. Obtaining this system and sensors, traffic operators can prioritise and facilitate ambulances to reach hospitals faster. In addition, these systems can be accessed by vehicles of patients through their navigation systems in an emergency.

Alice's Home Area Network (HAN) includes her mobile devices, such as her mobile phone and her laptop, smart home devices, the intelligent lighting and heating

system of her house, her car and a smart medicine dispenser, through which she receives her medication.

Bob was recently laid off by the hospital on claims that there was a leak of patients' data because of his fault. He believes that this claim is unfair and he tries to blame the hospital system.

4.3.2 The Incident

Bob uses his laptop to access the hospital records and to perform the following attack.

- He starts this attack by tampering with the medication of patients which they are due to receive later that day. By gaining access to the hospital's email account, he sends emails to all the patients, informing them that due to the improved health condition, their prescriptions have been changed and they have been reduced. As such, the medicine dispensers of patients will provide the new reduced dose to them. Since the hospital did not provide any report or notification to patients regarding the improvement of their health condition earlier, some patients are confused.
- He connects his laptop to the sensors of smart traffic operators- smart traffic furniture near to the hospital via wireless communication. His laptop is loaded with the sensor manufacturer and Bluetooth transmitter. Thus, Bob can control smart traffic furniture remotely through an uploaded malicious code. In addition, he can send manufactured messages to ambulances and patients vehicles that need to approach the hospital. This attack causes delays in ambulances and vehicles that try to reach the hospital. Furthermore, Bob has accessed sensors physically and made them unable to interact with vehicles and facilitate them to visit the hospital. In this way, he accessed data that is stored in the sensors that he compromised.
- After Bob has compromised the sensors system of ambulances and traffic operators, he accessed the automatic navigation system of Alice car making it choose the longest route to any selected destination.
- Alice's car is connected to her HAN, where her house lighting and heating systems are connected as well. This setup expands the attack surface.

4.4 Energy Factory

4.4.1 Use Case

Bob is a skilled computer expert and he works as a black hat hacker. He works from home and his PAN is made of his personal devices, such as his mobile phone, his wearable devices and his personal computer. Along with his colleagues, who work as black hat hackers as well, he tries to exploit security gaps of smart energy production factories by injecting malicious code that can be propagated to programmable logic controller (PLC), which allows the automation of electromechanical processes. Therefore, malicious code can tamper with the smart energy production factory system and give Bob control of factory operations.

A smart energy production factory provides energy to several cities that are based close to it. These cities can be considered smart since there is technological

integration and many technological enablers have been placed to address citizens needs. Smart energy production factory provides energy to citizens households and it is employed to provide energy to critical infrastructures of these cities, such as hospitals, traffic control systems, smart lighting systems, etc. Also, some of these facilities are equipped with smart meters that can record the energy consumption and share this information with the smart energy production factory, which determines the amount of energy that is consumed and the needs for energy production. These smart meters are implemented in public and private areas. Many households within these cities are provided with smart metering systems, which rely on the Home Area Networks of those citizens who have adopted it. As such, citizens who obtain smart lighting systems can manage it through their smart devices remotely. In addition, since smart cities are implemented and used by households, exploitation of these systems can provide access to the personal information of customers.

Alice obtains a smart metering system that is connected to her HAN, where her personal devices, like a smartphone and tablet, her smart vehicle and the smart heating system of her house are connected as well.

The exploitation of vulnerabilities of a smart factory, the malfunctions and the compromising of major devices and functions in it due to cybersecurity attacks can cause extensive damage, creating physical, cyber-physical and hybrid threats.

Hybrid threat term refers to the combination of conventional and unconventional, military and non-military activities threats, which are used in a coordinated manner by state or non-state actors, in order for specified political objectives to be achieved, while remaining below the threshold of formally declared warfare (Galinec, Steingartner, and Zebić (2019)). This kind of threat is multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics. They are designed in this way to not be easily detected or attributed. These threats target critical vulnerabilities and are intended to cause confusion that hinders rapid and effective decision making. Hybrid threats vary, from cyberattacks on critical information systems and disrupting critical services, such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions (Energy (2019)).

4.5 Healthcare System Breach

4.5.1 Use Case

Alice is an employee of a local hospital that belongs to national healthcare system and her duties involve the communication and reply to patients, visitors and public enquires. In addition, she is responsible for replying to email enquires.

In order to connect to her personal, corporate computer, and her email account, Alice is provided with credentials, a user name and a password that should be changed every six months by employees. Moreover, national healthcare system provides cyber security training to the staff, without these training sessions to be mandatory. Alice uses her credentials to login to her corporate computer to access her email account and available platform of national healthcare system, which she is authorised to access.

Alice is not aware of cyber security principles and she has limited knowledge of techniques that should be followed in order to be protected from cyber threats and attacks. Alice receives various emails on her email account every day, some of which come from unknown senders. On the other hand, Alice checks all of these emails, without keeping in mind that some of them may be malicious. One of these

emails is received, and Alice decides to open it and access the link that it includes. This is a malicious email that injects malicious code to her corporate computer that is part of the hospital network. The infected computer is interconnected with all the subsystems of the local hospital and the whole national healthcare system digital infrastructures. It have to be mentioned that hospital is interconnected with various service providers systems within the same city, where hospital is located, and exchange data that facilitate many city's services.

The national healthcare system is fully digital. All parties of the healthcare system are interconnected, giving them the chance to communicate between each other and exchange information. Patients can receive medical supports without visiting healthcare infrastructures, healthcare professionals provide guidance to patients through digital infrastructures and prescribe medicine to them in a digital way. Moreover, patients medical records are accessed in real-time by healthcare staff for various purposes. Patients medical records are stored on a database server provided by Microsoft SQL. Also, some files are kept by hospitals locally to facilitate hospitals' services and staff. In addition, a maintenance team, services provided by company Z, has been employed to ensure the business continuity of Healthcare System digital infrastructures, apply patches and take backups frequently. The time period between backups is not defined by stakeholders, but, by company Z, which does not adjust the services that it provides depending on the criticality of each system that it undertakes.

The server that hosts the healthcare system is protected by a firewall and is accessible by authorised users only through HTTP, FTP and RDP. Log files are by default activated enabling auditing, however, nobody is monitoring these log files to detect any security incidents. In addition, there is no centralised logging system that can facilitate security monitoring controls. Although some cybersecurity mechanisms have been applied for an incident to be identified and addressed faster, part of the healthcare staff struggles with using the digital version of the national healthcare system. Moreover, none of the staff has been provided with training for familiarising with the digital environment.

Furthermore, it should be taken into consideration the existence of cyber-physical systems that may be compromised and affect both cyber and physical plain. The hospital as a critical service provider gathers and maintains digital evidence objects frequently, before an incident takes place. A compromised system of local hospital may be responsible for compromising various other systems inside a city and threatening citizens safety, as well.

4.5.2 The Incident

- Alice opens an email and accesses the available link that is provided. This is a malicious email that injects malicious code and compromises Alice personal, corporate computer.

- Since Alice computer is part of the hospital's system, malicious code compromises the whole digital infrastructure of hospital, the interconnected systems as well.

- After the malicious code injection, various incidents take place. Some of them include the access and alternation of patients records, unavailability of various healthcare subsystems, such as digital medicine prescription, as well as various other services within city, making citizens being unable to track the next available buses, bus drivers receive notifications regarding the change of the

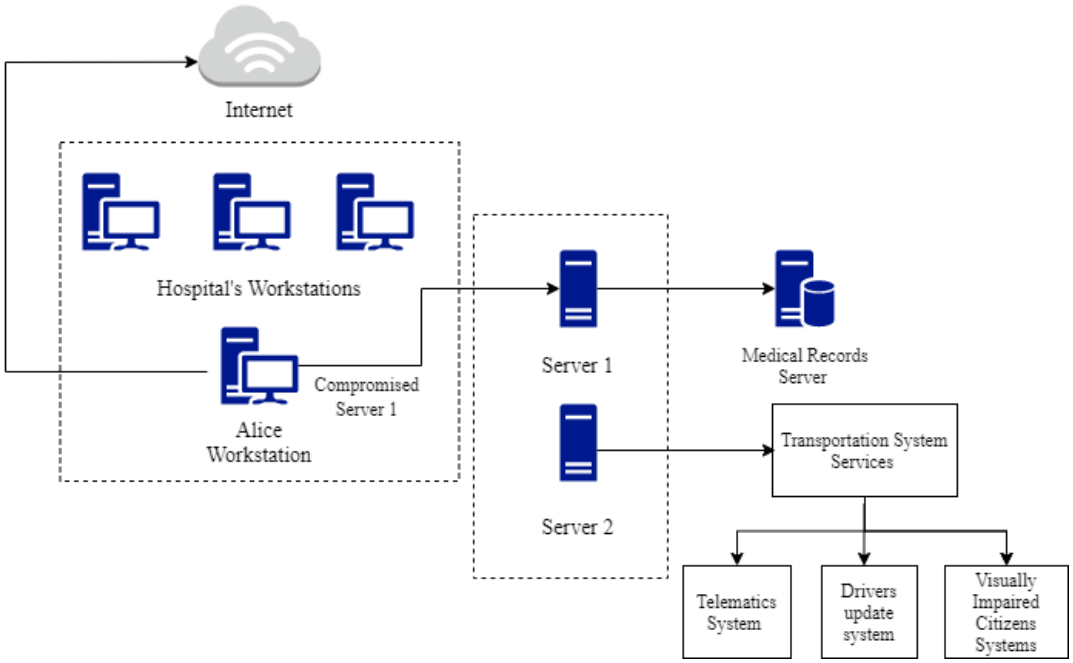

FIGURE 4.3: Overview of Hypothetical Scenario 3 (adapted from Bit_of_Hex (2019))

root, making them choose streets, where buses lanes are not available, making them unable to provide services to the citizens.

- A few days later, files and records stored on a database of the national healthcare system were locked and the only services that could be provided were the emergencies. The results of this attack include the encryption of the whole system and the attackers demand from the national healthcare system to pay in cryptocurrencies for the records to not be deleted. The attack is a ransomware attack. After the discovery of the attack, cybersecurity specialists are called to estimate the damage and to design the recovery plan. In addition, a digital forensic investigation is conducted for the incident timeline to be identified.

4.6 Discussion

The use cases introduced above designate the technological integration within particular sectors and the technological advancement of an entire urban environment. In addition, they designate the interconnection and the interdependency between the adopted technologies and systems, as well as the interconnection and interdependency between critical sectors and infrastructures within the same context.

Regarding the maturity model that is adopted from Ideal-Cities (2018) and presented in Chapter 3, the level of technological integration and the adoption of a CE agenda, indicate the maturity level that a city has achieved and how technological advanced it may be. On each of the presented maturity levels, technological enablers play a key role, facilitating a range of purposes, more constrained on lower maturity levels, to more vital and advanced to higher levels. The increase of the technological integration in city environments facilitates various purposes and addresses emerging challenges, but this comes along with the increase of new security threats and the exposure surface of a city.

For instance, the exploitation of a vulnerability or a risk in the case of a software defined superblocks environment - which is part of a Responsive city - may affect severely not only the superblock structure, but all the other interconnected sectors and infrastructures that facilitate that concept, since in the Responsive maturity level, all the technological enablers are in a complete sync. In addition, it should be taken into consideration that a city is considered as a system of systems that consists of cyber-physical and socio-technical systems, which interact between each other.

It is expected that the impact of the exploitation of a vulnerability or a risk on higher maturity levels will be higher, and will affect both cyber and physical plains, than the impact on lower maturity levels.

A representative example of this claim may be the energy factory use case, where cities and critical infrastructures of them are provided with energy by this particular factory. The impact of a particular risk may differ between maturity levels, being more severe on smart and responsive maturity levels and less severe on instrumented and connected levels.

4.7 Chapter Summary

In this Chapter, four city based use cases are presented, related to some of the major sectors and infrastructures of an urban environment. First presented the use case of superblocks is considered as a novel mobility model, adopted by Barcelona municipality for air and noise pollution and availability regarding public space for citizens to be addressed. This mobility model has been extended, by proposing a software defined approach adopting circular economy.

Moreover, two healthcare related use cases are presented, where cybersecurity incidents take place and affect not only healthcare related systems, but various other systems that are interconnected with the former mentioned, because of the interconnectivity property.

In addition, a use case related to a city energy factory is presented and impact that the exploitation of various vulnerabilities of those factories may affect severely business continuity of other city's critical sectors and infrastructures.

Finally, taking into consideration the maturity model that is introduced in Chapter 3, and adopted for this research, the impact of a risk or the exploitation of a vulnerability impact may differ depending on the maturity level that a city has achieved. In addition, it should be mentioned that the impact of the exploitation of a particular vulnerability, may not be the same on all the above mentioned use cases, being more severe on higher maturity levels and less severe on lower maturity levels.

Chapter 5

Technological Integration within Cities- An Architecture for Blockchain over Edge-enabled IoT for Smart Circular Cities

5.1 Introduction

The Circular Economy introduced as a novel model, where all *assets* are reused and not wasted before the end of their lifecycle. The IoT paradigm can underpin the transition to a Circular Economy agenda by enabling fine-grained and continuous asset tracking.

In addition, the employment of the IoT paradigm may rise severe security and privacy related challenges, due to its "*vulnerable*" nature. In addition IoT devices performance may be enhanced by the employment of other technological enablers. Blockchain is a promising technology, gaining popularity by its application as fundamental enabler of the Bitcoin cryptocurrency, introduced by Satoshi Nakamoto in 2008 Nakamoto and Bitcoin (2008). It is considered as an innovative technology, not only due to the deployment and operation of cryptocurrencies, but for various sectors, such as healthcare and transportation.

On the other hand, it should be taken into consideration that the adoption of innovative technologies is not a panacea and may raise other challenges. Significant issues are raised due to the constrained nature of IoT devices in terms of available computing and communication capabilities, and available energy resources in the case of the Blockchain application over IoT devices. For instance, in Blockchain applications, each node of the network keeps a copy of the ledger, which may increase considerably in size (in certain circumstances, in the order of several GBs) (Blockchain.com (2019)). For addressing Blockchain application related issues, the Edge Computing may be used.

In this Chapter, the deployment of a hybrid Blockchain-based architecture for IoT networks, in terms of a smart city ecosystem is presented. IoT devices act as nodes of a Blockchain system, employing Edge Computing nodes for the storage of the ledger to be facilitated. The proposed architecture is critically assessed against existing Blockchain architectures and under a broader context of emerging ICTs and their implications.

5.2 Related Work

During the recent years, various research works, such as Chakrabarty and Engels (2016); Abreu et al. (2017); Berkel, Singh, and Sinderen (2018) indicate the integration of technological enablers within a city in order to improve the provided services and deploy new architectures that can enhance the performance of the adopted technological enablers. The main technological enablers, employed for a smart city ecosystem include the Internet of Things paradigm, Cloud and Edge Computing, SDNs and NFV, 5G and Artificial Intelligence techniques. In addition, the implementation of the Blockchain technology has become popular.

In Bocek et al. (2017), authors present a traceability application, used for verifying the integrity of data and the accessibility to temperature records in a pharmaceutical supply chain using IoT sensors and Blockchain. The traceability of medical products, the quality control and the environmental conditions are essential for the healthcare supply chain. For tracking purposes, IoT sensors are employed and placed on parcels and smart contracts are used to determine whether the values that have been received remain within the allowed range.

In Ekblaw et al. (2016), an MIT research team presents a decentralised, permission-based Blockchain platform for the management of health-medical records in order for security and privacy breaches to be prevented.

In Shae and Tsai (2017), authors present an architecture of a healthcare IoT application based on Blockchain which is used for clinical trials and medicine precision.

In Yue et al. (2016), authors introduce a Healthcare Data Gateway-centric architecture for enabling patients to control and manage their medical history records in a secure way. Authors present a three layer architecture, which includes data storage layer, data management and data usage layer, employing the Blockchain technology in order for security and immutability features to be applied on the medical data storage layer (Xie et al. (2019)).

In Cheng, Zeng, and Huang (2017), authors analyse the fundamental features of a decentralised power system and present a Blockchain-based electricity trading model, where the transactions' data is stored in the chain. In addition, an effective pricing mechanism is proposed for ensuring the electricity market.

Furthermore, authors in Tanaka, Nagakubo, and Abe (2017), present a Blockchain-based electricity trading system with Digitalgrid for providing secure and decentralised control related to electricity transactions among providers and consumers. The target of the application of Blockchain is to ensure the security and immutability of transactions.

In addition, an architecture called *Helios* related to production and distribution of electricity energy is presented in Kounelis et al. (2017). The *Helios* architecture includes three layers, the energy grid, the middleware controller and smart contracts. The employment of smart contracts facilitate the monitoring and accounting energy exchange automatically in limited geographical areas. Smart contracts are connected with energy grid through the middleware controller.

Moreover, for overcoming security risks of centralised vehicular networks, research introduces Blockchain approaches for building decentralised and distributed vehicular networks.

In Yuan and Wang (2016), authors present an Intelligent Transportation System (ITS) framework based on Blockchain technology, which consists of seven layers, the physical, data, network, consensus, incentive, contract and applications.

In Sharma, Moon, and Park (2017), authors aim to propose an immutable, secure and distributed transportation management system for smart cities environments

and they introduce a vehicular network architecture based on the Blockchain technology called *Block-VN*.

Also, in Lei et al. (2017), authors focus their research on the security of vehicular network key management and present a distributed key management system, where the decentralised Security manager (SM) network replaces the third-party authority for authenticating the key transfer processes. In addition, they present the current models of Intelligent Transportation Systems, the way that they work and the challenges of these systems. These challenges are mostly concerned with privacy and security efficiency, safe communication among the parties of these systems and energy consumption.

In Toyoda et al. (2017), authors propose a product ownership management system (POMS) used in order to identify counterfeit products based on Blockchain technology and smart contracts, the Manufacturer Manager (MM) and Products Manager (PM), for tracking all the different production stages from manufacturer to consumer. In addition, authors use the Ethereum platform for validating their proof-of-concept.

Furthermore, a novel Blockchain based system for facilitating traceability is presented in Lu and Xu (2017). The traceability system or *originChain*, as this system is called, includes three parties, product suppliers, who are responsible for products management and enterprise information, labs, which manage the sample-testing results and the traceability service provider, who are responsible for the storage of product related information, certificates and further product details.

In Yavuz et al. (2018), in order for the authenticity and integrity of vote records to be assured, authors present an e-voting system based on the Blockchain technology. For the needs of this novel e-voting system, Ethereum Blockchain has been employed, as well as smart contracts that perform automatic processes, such as the check and counting the votes.

On the other hand, the adoption of the Blockchain technology comes along with some challenges regarding the processing power and time, the energy consumption and the limited resources and the constrained nature of IoT devices.

In Dorri, Kanhere, and Jurdak (2017), authors identify the limitations of IoT regarding memory capacity and propose a new architecture based on the Blockchain in combination with the Cloud Computing. The Cloud Computing is used as storage solution that enables the storage of Blockchain transactions, instead of IoT devices due to their constrained memory capacity. The deployment of this approach may not be efficient enough in terms of availability in real-time. Furthermore, Cloud Computing response to requests of an IoT enabled system may take more than 5 ms. As such, it is identified that the Edge Computing may be a better approach solution for addressing this issue. The Edge Computing is the key enabler of 5G networks and provides an IT service environment at the edge of the network, closer to end-users, reducing the latency, increasing the bandwidth and real-time access to radio network information (Sabella et al. (2016)).

In Babou et al. (2018), authors presented the advantages of Edge Computing systems, such as Cloudlet, Fog Computing and Multi-access Edge Computing, and deployed an Edge Computing based architecture, the *Home* Edge Computing, which involves three layers, the Home Server, the Edge Computing and the central Cloud.

The term *Home* refers to places, where users may be connected to the Internet, not to users' houses. The *Home* may include companies, hospitals, malls, and public space. This architecture aims to reduce the latency by employing storage and data processing devices closer to the end-users, and the workload of the Edge Computing Server by allocating resources hierarchically. In this way, the Edge Computing has

fewer spots and task to process. By comparing this new architecture with other existing Edge Computing concepts, the authors provide experimental arguments and results to improve their performance claims for their architecture.

In Reyna et al. (2018), authors study the IoT and Blockchain integration, and the major challenges related to the low-end specification of IoT devices and Blockchain scalability issues, regarding to efficient management of the big volume of IoT transactions on schedule.

In Dorri et al. (2017), authors proposed a Blockchain-based architecture for users privacy protection and increasing of vehicular ecosystem security in a smart city environment. Authors present only a description of their architecture without providing a working prototype.

In Novo (2018), authors present a distributed access control system, Blockchain technology based for IoT architecture, without presenting an implementation.

In Panarello et al. (2018), authors present a systematic review on the IoT and Blockchain integration, claiming that the former is able to address security and privacy challenges of IoT systems, due to its innate properties that include immutability, transparency, auditability, data encryption and resilience. While this may be true to some extent, it is suggested that this method is insufficient to declare an IoT networked system safe.

5.3 Model and Architecture

As discussed above, IoT devices may not be able to comply with Blockchain demands regarding memory capacity and energy consumption. The Edge Computing has been employed as storage service solution of the Blockchain ledger to enhance the performance of IoT devices within a smart city ecosystem, without draining their resources. The IoT devices are employed for this architecture include Class C devices.

The Class C refers to devices with significant communication capabilities and processing power with direct access to the Internet. These devices may include single board computers, sensors, actuators, cameras, smart devices, such as smart traffic furniture, vehicles, smart wearables, and so forth. These devices are nodes of a Blockchain network and may perform mining processes for validating new transaction.

Based on the constrained resources of these devices and the IoT paradigm in general, there is need for alternatives. In addition, security and privacy issues related to the IoT paradigm must be addressed, especially within a smart city environment.

Our proposed architecture combines the Edge Computing and the Blockchain that can enhance the performance of IoT devices of a smart city. These devices are employed to facilitate various purposes, such as collection, exchange and storage of useful data that facilitates the needs of citizens. These devices are nodes of a Blockchain network and all the interactions are conducted in Blockchain transactions form. These transactions are verified through the mining process of the Blockchain. Stored data in a transaction form may include mobile devices location data, data related to availability and condition of devices, data regarding weather and climate, etc.

One of the major challenges is that when more transactions are performed, the number of Blockchain blocks created grows proportionately. As a result, the size of the ledger that these devices must store has increased. In addition, it should be taken into consideration that the memory capacity of these IoT devices is limited.

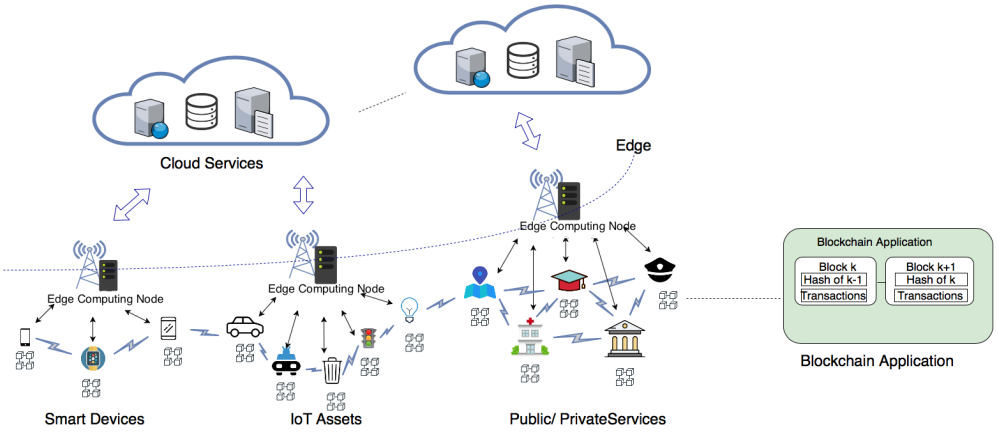

FIGURE 5.1: Employed Edge Computing as storage enabler of the Blockchain ledger for IoT networks in a smart, circular city

The employment of the Edge Computing may facilitate the communication of IoT devices within a smart city environment by providing a ledger storage solution. Thus, even IoT devices will be able to create and verify new transaction and generate new blocks of the chain, copy of the ledger will not be stored locally by devices, but by employed Edge Computing nodes that will be placed inside a smart city environment. It is assumed that employed Edge Computing nodes are trusted and reliable from the outset and not controlled by any central authority in order to comply with Blockchain principles. IoT devices will be able to access the stored ledger, in order for the demands for memory consumption to be mitigated.

The interaction of IoT devices and Edge Computing nodes is performed through Low Power Wide-Area Networks (LPWAN), such as LoRa and SigFox, for achieving low latency levels. Every device maintains a communication channel with employed Edge Computing nodes, in order for the access to data be faster, as every communication channel serves only one IoT device. The proposed architecture is presented in Figure 5.1.

5.3.1 Mining Process

Although the mining process is performed by IoT devices, which are the nodes of a Blockchain network, as in *traditional* Blockchain systems, the difference is related to the ledger storage, not by the nodes of the systems, but by the local Edge Computing nodes.

The IoT devices may still act as miners, enabled to validate transactions and compute PoW values in order for consensus to be achieved within the network. Because of Blockchain network nodes trade and gather data in transaction form, a miner must first compute the PoW value before generating a new block. In order to create connection between the blocks, the mining process contains the hash of the previous mined block. As a result, miners should be able to retrieve the hash value of the previous mined block in order to compute the hash of the new one. The miners may access this block via the Edge Computing nodes since the ledger is stored there. The devices which are Blockchain network nodes, will have access to the stored ledger upon request.

Similarly, the Edge Computing nodes will be able to return the hash value of the most recently added block to each of the asking nodes once they are ready to mine

a new block, utilising each communication channel. As a result, all nodes in the Blockchain network will be able to continue operating, increasing their performance, since they will be able to use their memory capacity without concerning about the size of the ledger or the availability of the last generated block hash value to mine the new block, verify new transactions and receive the rewards. The new block will be mined by one of the network's miners and stored on Edge Computing nodes. The produced block will be sent to the Edge Computing nodes over LPWAN and stored with the previously mined blocks, keeping the chain up to current.

Following the mining process, the miner of the new block is the Blockchain node that initially computed the most appropriate PoW value. Each block's miner sends it to the Edge Computing nodes through the LPWAN communication channel and stores it there.

5.3.2 Comparison

The introduction and deployment of a new smart city architecture based on the usage of the Edge Computing and Blockchain aim to enhance the performance of critical devices and infrastructures of a smart city environment. In addition, the employment of Blockchain may play a key role for enhancing the security and privacy of IoT networks, as embedded vulnerabilities and risks of the IoT paradigm may increase the threat landscape and affect not only the performance of it, but the whole smart city ecosystem.

When comparing standard Blockchain design to ours, the first difference is related to the Blockchain distributed nature, since the ledger will be stored away from network nodes, on the Edge Computing nodes. By retaining a single copy of the ledger on the Edge Computing nodes, we recognise that the distributed features of the Blockchain is relaxed. There are two approaches that may be used to address this challenge. Our initial assumption is that there are several Edge Computing nodes where the ledger may be kept, despite the fact that our first assumption is that the Edge Computing service provider is totally trustworthy and reliable.

This method has several advantages, including the fact that the ledger will always be available and shared among many Edge Computing nodes when one or more of them may be unable to service. The Edge Computing nodes placed around a smart city have been employed to facilitate the ledger storage. This method addresses a second challenge that refers to the distance among the Edge Computing nodes and devices, as well as the devices ability to have access to the stored ledger. Employing a number of Edge Computing nodes, devices may operate properly, despite their location and distance from the Edge Computing servers. The usage of the Cloud Computing is the second alternative that may be used. The assumption here is that the ledger is pushed to a Cloud service provider on a regular basis. The Cloud provider must be considered as reliable, always accessible, and trustworthy from the outset, in order to be eligible in this case.

In regular time periods, Edge Computing nodes need to update the Cloud-stored copy of the ledger, which is used as a backup for ensuring safety and availability of it. Although the decentralisation features of the Blockchain is not followed completely by adopting Cloud-based solutions, we believe that our approach can improve the network performance and keep the ledger safe.

Moreover, in Xiong et al. (2017), authors proposed a new architecture, based on the Edge Computing and Blockchain for mobile and IoT devices. The aim of this architecture includes the enhancement of devices, which run Blockchain applications, performance by helping them to operate faster, without consuming their resources

for the computation of the PoW value. In order for this to be achieved, devices of the network that act as miners request the computation of the PoW value by the employed Edge Computing. The proposed architecture is presented in Figure 5.2. The security of computation of PoW value and the mining process is ensured by the adoption of techniques, such as masking and obfuscation. In exchange for this services, the Edge Computing service provider requests fees from miners. After the achievement of consensus among miners and Edge Computing service provider and the transfer of fees, the latter starts the PoW value computation process and returns the value to miner device when it is ready. The miner receives the value, and broadcast it to the rest of the network. If consensus among miners is achieved, the miner generates the new block and adds it to the chain, receiving the rewards for this process. Rewards are expresses as a utility function.

The main goal of this approach is the decrease of energy and CPU consumption of IoT devices that obtain a Blockchain based application. Although the results of simulation that authors conducted reveal efficiency of proposed architecture, there are still some drawbacks related to the offloaded mining process.

First of all, since miners are nodes of the same Blockchain network and users of the same Edge Computing services provided for mining purposes, competitions among them may take place, since each of them wants to achieve the generation of a new block of the chain and receive the rewards. As such, there are some "blind spots" related to the transparency of the process.

In addition, issues related to the complexity of a chosen consensus mechanism used by a Blockchain system may be addressed by adopting a different consensus mechanisms with lower demands regarding CPU and energy consumption. In addition, the complexity of the Proof of Work computation relies on the need of a Blockchain network to be protected and resilient against malicious parties that try to harm the network. Mitigating this process to a third party provider may cause related to security and accuracy of transactions issues, affect the nodes and the performance of the Blockchain network, by verifying malicious transactions.

It should be taken into consideration that the application of Blockchain over IoT networks brings challenges, however, we believe that the computation of the Proof of Work value must be performed by miners of a Blockchain network for the reasons that have been identified above, in the case of the implementation of the PoW consensus mechanism.

Blockchain networks operation is based on this process and guarantees that a node is trustworthy. As such, the performance of the mining process by a third employed party, like the Edge Computing, can have harmful consequences for the network.

5.4 Discussion

The high growth and adoption rate of IoT, Distributed Ledger Technologies, like Blockchain, and new paradigms, such as Software-Defines Networks, for addressing challenges related to sustainability within an urban environment and enhancing the operation of infrastructures and ICTs, are constructing the mosaic of emerging technologies in terms of smart cities ecosystems. The sustainability reminds us that the ultimate aim of a city is to become *circular*, not only *smart*, where the first term enables the achievement of the latter.

In addition, smart cities main purpose includes the provision of services to citizens and visitors and facilitate the daily needs and the improvement of the quality of

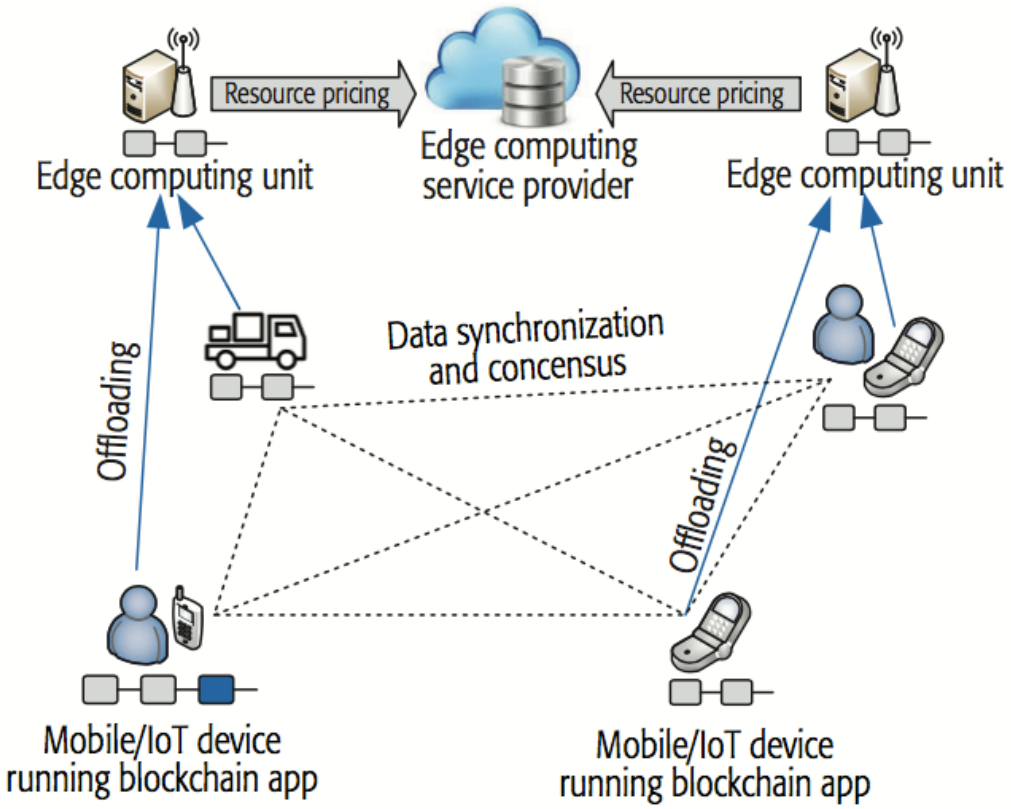

FIGURE 5.2: Edge Computing for Mobile Blockchain (Xiong et al. (2017))

life. The integration of technological enablers involves the generation and exchange of vast amount of data that flows through the cities' systems and infrastructures (Al Nuaimi et al. (2015)). The Blockchain technology may be considered as a solution to key smart cities challenges, since it is able to provide essential features, such as security, privacy, integrity, transparency and immutability.

The adoption and the usage of DLT applications and services may create a fertile ground for dealing with complex procedures and providing high level of smart cities services autonomy (Ibba et al. (2017)).

As discussed above, the contribution of the Blockchain mainly focuses on the security and privacy enhancement and the provision of valuable features, such as integrity and transparency. The complexity, interconnectivity and heterogeneity have been also discussed and identified as key challenges for the preservation of sustainability and operation of an urban environment, due to the variety of technologies, infrastructures and stakeholders interaction. Furthermore, the security and privacy enhancement may facilitate and improve the performance of other technological enablers, such as the IoT paradigm and provide an additional level of protection against cyber attacks that may affect the performance of smart cities services and violate security and privacy of citizens. The employment of the Blockchain technology and the application of a lightweight version of it on the top of all technological enablers and digital infrastructures may provide valuable services and address major challenges, reducing the cost of further solutions deployment. In addition, the heterogeneity of technologies and systems within the same environment may rise challenges related to the management of data, integrity, and legislation. Blockchain can be considered as a technology that can be adopted as a "united" solution for

providing a common ground of integrity, and data management.

In Chapter 8, we present how Blockchain contributes to the adoption of a digital forensic readiness framework in terms of an urban environment concept, taking into consideration various limitations of current solutions and solutions that cannot be overcome by adopting traditional and established approaches. The main purpose of the deployment of a Blockchain-based digital forensic readiness framework is to preserve the integrity of Chain of Custody (CoC) and the authenticity of digital evidence until their presentation as artifacts.

Simultaneously, research and innovation frenzy toward the adoption of innovative and promising technologies, like Blockchain, evangelises to solve a number of issues across a wide range of smart city use cases and projects. On the other hand, a closer look into these new technologies and paradigms may reveal that they do not work as panacea. It may be noticed that some of these innovative applications and proposals may not be that effective or feasible, not to mention that they may have adverse effects, contradicting their purpose.

The Jevons Paradox York and McGee (2016), may be an example for the autonomous vehicles use case. Vehicle autonomy requires the deployment of all the technological advancements of all IT innovation, such as AI, pioneering 5G frequencies for facilitating communication, Big Data and machine learning and results to energy consumption demands increase. Since, we assume that autonomous vehicles will be electric, due to the need for reducing fuels and find alternatives for the protection of the environment and the advancements of research into electric energy efficiency, we will have to invest the majority of energy of a vehicle for addressing the expensive computations and cooling needs.

In essence, the Blockchain implementation and operation may be expensive from the outset, even Blockchain implementation may provide valuable features by ensuring security of transaction and integrity and offering traceability.

Furthermore, reflecting upon Wriston's Law (Karlgaard (2005)), stating that *capital*, when freed to travel at the speed of light, will go where it is wanted, stay where it is *well-treated*, it could be claimed that in a data-driven Circular Economy ecosystem, capital refers to information, which requires a suitable architecture that will allow it to travel in order to identify equilibria and locations, where it can be utilised well.

5.5 Chapter Summary

In this Chapter, the technological integration of smart cities environments is presented, by introducing the Edge Computing and its contribution to the IoT and Blockchain collaboration, addressing the rising issues of it. As IoT paradigm includes issues related to the limited storage capacity of devices, and the volume of generated data within an urban ecosystem, the Edge Computing is employed as a solution for addressing the issues that lie on the collaboration of the IoT and Blockchain. The employment of Edge Computing may facilitate the operation of IoT devices, making them more efficient, achieving the information circularity within a smart city ecosystem.

Chapter 6

The adoption of Distributed Ledger Technologies and IOTA for Threat Modelling of IoT Systems

6.1 Introduction

The emerge of the IoT paradigm and the growth of related adopted approaches have increased the need for addressing key challenges, such as schemes of embedded devices, sensors and actuators seamless interconnection to the Internet and long-range wireless communication of low power embedded devices. In order to address these challenges, various technological advancements have been employed. As such, the deployment of stand-alone IoT systems that operate in isolation transforms into large scale well-connected IoT systems that cover big areas of interest, like smart cities.

As already discussed, the IoT paradigm plays a key role in the development of smart cities ecosystems, along with various other technological enablers, such as DLTs, AI and machine learning, Cloud and Edge Computing and 5G, illustrating the technological roadmap for a city ecosystem to become smart.

While much effort is spent on improving the efficiency, interoperability, and impact of the IoT paradigm, less effort has been spent on the investigation and improvement of their cybersecurity aspects, adopting techniques, tools, and methods that are originally developed and adopted for regular computer systems. Thus, the latter do not address the challenges related to the novel IoT paradigm. Furthermore, cybersecurity is frequently evaluated after an incident has occurred.

In this Chapter, the deployment of a DLT and IoT Proof of Concept (PoC) system, which aims to enhance the performance of IoT devices under the prism of Intelligent Transportation Systems is presented. In addition, potential attack vectors of Intelligent Transportation Systems, categorising them into three tiers, devices, network, and DLT layers, are identified and the DREAD threat model for their evaluation has been employed.

The presented PoC system employs the IOTA Tangle distributed ledger for storing the generated data. The model aids in critically evaluating the system's architecture against the DREAD evaluated threats as critical, demonstrating how threat modelling may be included into the development lifecycle of IoT systems.

This Chapter is based on the publication with title *"Threat Modelling of IoT Systems Using Distributed Ledger Technologies and IOTA"*.

6.2 State of the Art

As mentioned above, the increase of the population of urban environments around the world rises various challenges, as it has been estimated that they consume 75% of the available natural resources, producing more that 50% of the global waste (Morlet et al. (2016b)). As a growing amount of the global population is expected to live in cities in the coming years, smart cities (Geissdoerfer et al. (2017)) seek to embed emerging ICTs for designing and developing more efficient services as well as deploying improved decision and management mechanisms. The IoT paradigm may be considered as a key contributor, regarding the massive number of devices employment, which facilitates the generation, collection and exchange of data.

The constrained and ephemeral nature of the IoT paradigm as well as the vast volume of generated data increase the concerns in regard to data quality. The coordination of the IoT paradigm and Distributed Ledger Technologies, such as the Blockchain, is considered as an efficient solution for mitigating those issues.

The IOTA may be considered as a representative example of a DLT that has been deployed and developed in order to address the challenges of the IoT paradigm. The IOTA is a DLT that is used in the following presentation of proposed PoC system. The specialised desktop client *Trinity* was hacked in February 2020, resulting in the loss of money from user wallets and the IOTA Foundation shutting down the whole network for nearly two months. The use case of the attack is presented in Bocetta (2020). In 2017, for the IOTA payments to be facilitated, the IOTA Foundation attempted to develop a hash function scheme.

On the other hand, vulnerabilities that can affect the payments have been revealed by an MIT research team (Narula (2017)). In addition, in 2019, the IOTA network experienced availability issues for over than 15 hours, making users unable to send or receive any transaction over the Tangled. The reason of the unavailability of the IOTA network was a bug that affected the Coordinator of IOTA (Simmons (2019)). In the threat model section, related to the Blockchain or other DLTs risks that many affect their performance are identified.

Threat modelling process is a critical task for the identification of potential threats that may affect specific systems. In Aufner (2020), common threat modelling frameworks are reviewed, even they were designed for normal computer systems operating via the Internet (e.g. banking systems). As a result, these models strongly emphasise or include just software-based systems, causing numerous vulnerabilities to not be revealed when applied to IoT systems, which are typically cyber-physical. In Omotosho, Ayemlo Haruna, and Mikail Olaniyi (2019), authors introduce a threat model by considering common health devices.

In this Chapter, we consider Intelligent Transportation Systems (ITSs) in smart cities in order to address the threat modelling gap in the IoT and DLT correlation. For the needs of our threat model, we adopt a more generic form that can be easily adapted to other domains as well.

6.2.1 Intelligent Transportation Systems Risk Assessment

In this section, some of the cyber security incidents that have affected Intelligent Transportation Systems and will facilitate us to perform our risk assessment and identify potential attack vectors are presented.

The Intelligent Transportation System term refers to smart cars and traffic furniture, smart railway and air craft control systems, smart maritime surface, etc. The integration of technological enablers is high. Thus, the threat landscape increases,

especially over modern cars, which may be considered as *computers on wheels* (Stellios et al. (2018)).

Smart Internet enabled devices have replaced the *old* mechanical systems of vehicles and manage embedded subsystems, such as infotainment systems. Modern vehicles are provided with the Controlled Area Network (CAN) bus and an On Board Diagnostics Socket (ODS) that enables physical access to the system of a car. Since CAN bus is an established technology, various vulnerabilities have been identified (Rajbahadur et al. (2018)).

Since new services have been introduced, some of which are enabled with Internet connection, like remote software update, emergency calls to drivers and on-line infotainment, exploitation of existing vulnerabilities poses a significant risk, especially related to the safety (Wachenfeld et al. (2016)).

Moreover, since modern vehicles obtain additional on-board sensors and communication systems, like Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), enabling the communication among vehicles and infrastructures, the threat landscape increases even more (Al-Sultan et al. (2014)).

There are various categories of IoT-enabled attacks over ITS. Several preliminary work has identified different real world use cases of attacks that have been conducted against ITSs during the last years.

The first category includes exploitation of CAN bus, unauthorised access to subsystems, and injection of malware and crafted messages that affect the performance (Stellios et al. (2018)). Attacks related to IoT involve exploitation of vehicles infotainment vulnerabilities, exploitation of vulnerabilities of embedded IoT devices, like embedded sensors and traffic control infrastructure, and exploitation of radio communication protocols, such as LAN, DAN, and WiFi.

In Mearian (2015), a remote attack against the CAN bus of a vehicle by using a low-cost radio equipment is presented. Attacker uses a $15 radio transmitter for exploiting the CAN network and various software vulnerabilities in order to connect to the CAN bus and send commands to it. Attacker must be nearby the target vehicle.

In Vallance (2015), a similar attack is presented, but the distance between the attacker and the target vehicle is extended by setting up a bogus radio station that transmits crafted Digital Audio Broadcast (DAB) messages. The main goal of this attack is to compromise the infotainment of the target vehicle by sending crafted messages in order to control it. In Yadron and Tynan (2016), a similar attack is presented, in this case based on the exploitation of the Bluetooth or the telematics unit.

The exploitation of WiFi vulnerabilities have been conducted by teams of professional penetration testers, who revealed that mobile apps used for the remote control of a specified car model do not use Global System for Mobile Communications (GSM) module, but WiFi access point.

By compromising the WiFi passwords and injecting old commands from the compromised mobile application, attackers are able to control the whole vehicle remotely. This type of attack requires either the attackers being physically close to the target vehicle acquiring certain unique characteristics, such as DAB and WiFi protocols.

The exploitation of the infotainment vulnerabilities may have serious impact on different vehicle subsystems. Also, the infotainment system alone can be considered as vulnerable as well. In Miller and Valasek (2015), authors present a use case of the exploitation of the infotainment system of a vehicle (a Jeep Cherokee). Researchers discovered an open port used by the Harman Unconnect infotainment in

cellular networks. As such, malicious parties can scan for open ports and compromise vulnerabilities in the Open Multimedia Applications Platform (OMAP) chip of the head unit. Different types of sensors enable autonomous driving systems and supply with data systems such as Adaptive Cruise Control (ACC), collision avoidance or lane keeping assist system. Applied connectivity systems keep these sensors exposed to remote attacks and system failures.

A use case released by Tesla Motors Yadron and Tynan (2016) presents a deadly car accident caused by a self-driving car due to car sensors system failure. The car collided with an 18-wheel truck and trailer.

In Petit et al. (2015), a low-cost laser blinded a vehicle's camera by exploiting the authentication in Light Detection And Ranging (LiDAR) messages lack. Due to this vulnerability, malicious parties were able to gain unauthorised access to older commands and replay them in order to produce false artifacts and confuse the system. Other attacks, such as relay station and amplification attacks, highlight vulnerabilities in Remote Keyless Entry (RKE) systems (Garcia et al. (2016)).

The attacks that presented above require physical proximity to target vehicles in order to compromise the embedded communication sensors. Also, it should be taken into consideration that the control of a vehicle has been assigned to embedded autonomous control systems instead of drivers for the automation of driving process to be achieved. Consequently, the security of vehicle sensors against remote attacks through the Internet or other wireless networks should be considered as part of the threat landscape.

A medium-risk threat must also be addressed, although not as urgently as a high-risk threat. A low-level threat may not be handled at all since it does not constitute a substantial threat or risk.

6.3 Threat Modelling for Intelligent Transportation Systems using DLTs

Threat modelling may be considered as an essential task in order to estimate the severity of the identified attack vectors and the impact that these attack vectors may have on an ITS and to its users. In order to employ a threat modeling approach, a rating scheme must be adopted since it will help to calculate risk rating values to each type of attack vectors.

For the needs of this research, the DREAD threat model rating scheme, presented in Huq, Vosseler, and Swimmer (2017) has been adopted (see Table 6.1). A threat classified as high poses a significant risk to the system or its user and must be addressed immediately by adopting suitable countermeasures.

The DREAD threat intelligence modelling provides a rating system in order to assess the identified attack vectors and analyse various aspects of them. As such, the assessment of the damage caused by one or more attacks may provide useful information for creating damage assessment profiles for similar attacks in the future. The DREAD threat model provides a rating system and three categories of threats severity, low, medium and high (LeBlanc and Howard (2002), Singh and Singh (2012)). The DREAD threat model assesses identified attack vectors based on Damage, Reproducibility, Exploitability, Affected Users, and Discoverability of each of them.

Based on the severity of a threat and its threat rating, a threat is referred as low, medium or high. After the DREAD threat model application, each organisation

TABLE 6.1: The DREAD threat rating scheme (Huq, Vosseler, and Swimmer (2017))

Â	Rating	High (3) (score: [12-15])	Medium (2) (score: [8-11])	Low (1) (score: [5-7])
D	Damage	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information.	Leaking trivial information.
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers.	Some users, non-default configuration.	Very small percentage of users, obscure feature; affects anonymous users.
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

should address the identified threats in order to minimise the exploitation probabilities and the extensive damage and adopt cybersecurity techniques (Potteiger, Martins, and Koutsoukos (2016); EC-Council (2020)).

The DREAD threat model has been adopted for the needs of this research in order for the identified attack vectors of the ITSs to be assessed and categorised as low,

TABLE 6.2: Identified attack vectors over the device tier and DREAD evaluation.

Attack Vector	Damage	Reproducibility	Exploitation	Affected Users	Discoverability	Rating
Sniff traffic of network between device and back-end	1	3	2	1	3	Medium
Information leak	2	2	2	3	2	Medium
Cyber-enabled physical attacks	2	2	2	3	3	High
Recover credentials from flawed firmware	2	3	3	3	2	High
Modification of devices and exploit them	3	2	3	3	2	High
Files delete of compromised ITS devices	3	1	1	2	3	Medium
Man-in-the-Middle attacks	2	2	2	3	1	Medium
Unauthorised access/ Unauthorised controlling of ITS devices	3	2	2	3	2	High
Infection by malware	3	2	2	2	2	Medium
DoS/DDoS attacks	3	3	3	2	3	High
Attacks on IoT-enabled transportation systems	2	2	2	2	2	Medium
Unavailable speed limitation sensors	2	1	2	2	2	Medium
Ransomware attacks/ infection of devices with ransomware	3	2	3	3	3	High
Exploitation critical devices	2	2	3	3	2	High
Localisation of vulnerable devices through Shodan	2	2	2	2	1	Medium
Remote control of devices	3	2	3	3	3	High
Physical connectivity to exposed ports	3	2	3	2	2	High
Using brute force or guessing credentials on a device	2	2	3	3	1	Medium
Exploitation of vulnerabilities in software, hardware	3	2	2	3	2	High
Sending improper commands to the controller	3	1	1	3	2	Medium
Discovery of topology	1	3	1	1	1	Low
Storage device connection loaded with malware to install	2	2	2	2	2	Medium
Sending fraudulent messages	3	2	3	3	3	High

TABLE 6.3: Identified attack vectors over network tier and the DREAD evaluation

Attack Vector	Damage	Reproducibility	Exploitation	Affected Users	Discoverability	Rating
Exploitation of network flow to connect to car WLAN	2	2	2	2	2	Medium
Connection to CAN bus - vehicle remotely hijacking	3	2	2	3	2	High
Reverse engineer CANSW to control several systems	2	2	2	2	2	Medium
Send crafted DAB data to compromise the infotainment	3	2	1	3	3	High
Troubleshooting DAB reception	2	2	2	1	2	Medium
Unauthenticated CAN access	2	2	2	2	2	Medium
Crack the WiFi pre-shared key/ control CAN	2	2	2	2	2	Medium
Sniff and analyse of sensors/devices	1	2	2	1	2	Medium
Remotely control of sensors/devices	3	2	2	3	3	High
Injection of old command to car system	2	2	2	2	2	Medium
Identification and abuse network misconfigurations	2	2	3	3	2	High
Exploitation of software/hardware vulnerabilities	3	2	2	3	2	High
Installing malware/spyware on systems	3	2	3	3	3	High
Install malicious firmware	2	2	3	3	2	High
SQL injection attacks	2	2	3	3	2	High
Abuse of weaknesses of authentication mechanisms	2	2	2	3	2	Medium
Inject of malicious software via ads banners	3	3	3	3	3	High
Cross-site scripting (XSS) attacks	3	2	2	3	2	High
Eavesdropping sensitive information	3	2	1	3	2	Medium
Lack of encryption/ poorly implemented encryption	1	2	2	3	1	Medium

TABLE 6.4: Identified attack vectors over DLT tier and the DREAD evaluation

Attack Vector	Damage	Reproducibility	Exploitability	Affected users	Discoverability	Rating
Exploitation of embedded vulnerabilities	2	3	2	2	3	High
Distributed Denial-of-Service (DDoS)	3	3	3	2	3	High
Timestamp Hacking	3	2	2	3	2	High
Compromising centralised Blockchain – IOTA	3	2	2	3	2	High
Compromising users' wallet	3	3	2	2	2	High
Sybil Attack	3	2	2	2	2	Medium
Eclipse Attack	3	2	2	2	2	Medium
Man-in-the-Middle (Address Attack)	2	2	2	3	1	Medium
Exploitation of smart contracts vulnerabilities	3	2	2	2	2	Medium
51% or Majority Attack	3	2	2	3	3	High
Selfish Mining	2	2	2	2	2	Medium
Routing Attack	2	2	3	2	2	Medium
Dictionary Attack	2	2	2	2	2	Medium
Alternative History Attack	3	2	2	3	3	High
Flawed Key Generation	2	2	1	3	2	Medium
Vulnerable Signatures	2	1	2	3	2	Medium

medium or high risks. Other threat modelling methodologies have been taken into consideration, before the adoption of the DREAR threat model for the assessment of the attack vectors. Some examples of these methodologies include the OCTAVE and STRIDE threat models. The Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE) model has been developed by the Software Engineering Institute (SEI) for facilitating organisations to identify and assess the risks of information systems, improve the provided services and protect their infrastructures and assets from these risks. The OCTAVE method involves a set of rules that are followed by internal organisations' teams for conducting risk assessment procedures (Hashim et al. (2018)).

The STRIDE method has been introduced by Microsoft and it is based on six different types of security threats, Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege. The STRIDE method facilitates the analysis of identified attack vectors, vulnerabilities and risks against system components of an organisation that may be exploited by malicious parties to compromise the whole system (Khan et al. (2017)). For the needs of this research, only the DREAD threat model has been employed over OCTAVE and STRIDE for several reasons.

First of all, the DREAD model may be considered as easier and more understandable by non-technical people and organisation staff. Especially within the realm of smart cities, threat, vulnerability and risk assessment should be understandable by stakeholders, local authorities and citizens who may not be familiar with the technical aspects of this process.

Furthermore, considering the five factors that the DREAD assesses in terms of an Intelligent Transportation System risks and vulnerabilities, and in general a smart city ecosystem, especially for those that have achieved the higher maturity levels, affected users are an important part of this assessment since, in most cases, they may be severely affected by the exploitation of a risk or vulnerability. There are various risk assessment schemes, like the DREAD threat model, which take into consideration different factors than DREAD, such as confidentiality, integrity and availability. A representative example may be the CVSS scoring system (XM-CYBER (*What is Common Vulnerability Scoring System?*)).

Finally, in Chapter 7 the CVSSv3.0 scoring system has been employed for introducing the vulnerability dimension and the management of vulnerabilities in cities, taking into consideration the maturity levels that these cities have achieved. As has been discussed above, the CVSS system obtains a calculation process that takes into consideration confidentiality, integrity and availability. The adoption of DREAD threat model may complete the risk assessment process of this research, since the first is considered as compatible to CVSS. As such, identified attack vectors that have been assessed as high in this Chapter may be used and assessed again, against real CVEs that may affect the digital infrastructures and subsystems of a city.

In addition, considering the interdependence and interconnectivity of an IoT operational environment, exploitation of risks and vulnerabilities may affect critical infrastructures and systems, such as traffic management systems, supply networks, and e-health systems. ITS related risks are based on three important tiers, physical devices, network and Distributed Ledger Technology (DLT) are identified. The evaluation of identified risks of all the three tiers is conducted adopting the DREAD threat modelling. The identified threats and their assessed severity based on five factors of the DREAD threat model are presented in Tables 6.2 6.3 6.4. Every identified attack vectors has been assessed against the five dimensions of DREAD threat

model, Damage, Reproducibility, Exploitability, Affected Users, and Discoverability, taking into consideration the severity of each dimension within the realm of a Smart/ Responsive city (a city has achieved the higher or the highest maturity level). Each dimension is assessed taking into consideration the scoring system of the DREAD threat model, where 1 is considered as low and 3 is considered as high, depending on the severity of each attack vector in terms of the respective dimension. The attack vectors are considered as low, medium or high by calculating the sum of all the five dimensions of the DREAD threat model, as described in Table 6.1.

The DREAD risk can be calculated as follows (Cagnazzo et al. (2018)):

$Risk_p = DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTEDUSERS + DISCOVERABILITY$

6.4 An IoT and DLT Proof of Concept for Intelligent Transportation System

Smart cities projects aim to provide the efficiency of services in a range of application domains by leveraging emerging ICTs. This research focuses on Intelligent Transport Systems. The IoT paradigm and DLT are enabled for a secure and scalable infrastructures. A real application, where digital infrastructures of a smart city environment are in place and include microcontrollers and sensors placed on road infrastructures and on traffic furniture, such as traffic lights is introduced. In this way, traffic flow may be monitored and provide a vast range of metrics. In addition, the use case includes smart connected vehicles, autonomously or manually driven that are enabled to communicate with the traffic structure machine-to-machine.

The communication between vehicles and ITS infrastructures may facilitate future investigations related to accidents and the violation of traffic rules. Investigations can be split into two segments. The first segment may include physical investigations, examining aspects related to road and traffic furniture condition and availability and driver condition. The second segment may include digital forensic investigations, since both road and traffic furniture infrastructures and vehicles interact with the cyber plain, exposing them to cyber attacks that may compromise them and affect their performance. The proactive collection of data can be valuable for reconstructing the accident scene and facilitating a future investigation. As such, the employment of DLT may contribute, providing important features to the systems, like immutability, transparency, traceability and a timeline that can facilitate an investigation.

The presented Proof of Concept system adopts the IOTA platform (Hellani et al. (2019)). The IOTA is an open-source DLT designed to address IoT paradigm. The IOTA uses the Tangle, a distributed ledger, where transactions' blocks are organised in directed acyclic graphs. Currently, there are two available versions of the Tangle, the *mainnet*, which refers to the live version, and the *devnet*, which supports development purposes.

The employment of IoT devices, as vehicles and traffic structures and the IOTA devnet tessellates the presented PoC. The main goal of system is to serve as a functional testbed for the evaluation of systems that include IoT networks and DLT and to be utilised in their evaluation.

In Figure 6.1, the PoC high level architecture, as well as the technologies and hardware that are involved are presented. This architecture includes three tiers, the IoT tier, the Edge Network and the Devnet Tangle (DLT).

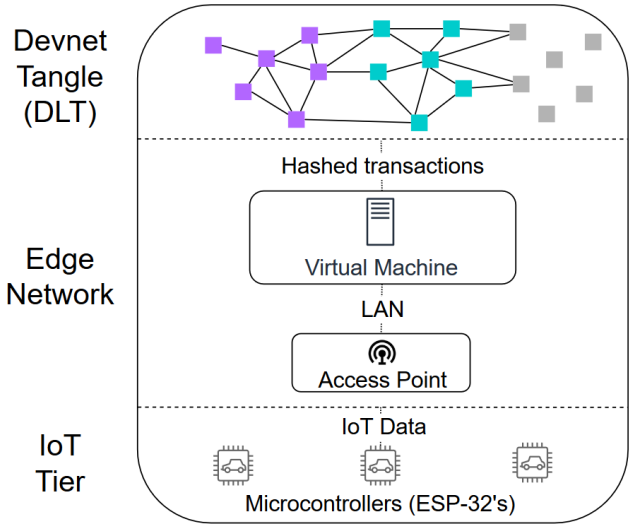

FIGURE 6.1: PoC architecture presented into separate tiers (a top-down perspective)

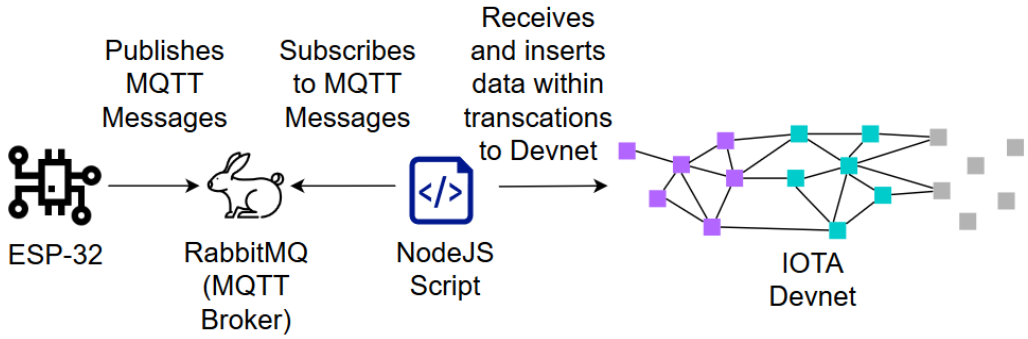

FIGURE 6.2: The interaction between the microcontrollers and message broker

The IoT tier involves the IoT microcontrollers used for data collection from vehicles. This data may be related to speed of travel, location of ping or *HELLO* messages to other vehicles or data structures within a city. The microcontrollers used for this PoC system are Espressif ESP-32 with WiFi radio interface.

At the second tier, the Edge Network, the employed IoT devices communicate to a virtual machine (VM) in a wireless way.

A MQ Telemetry Transport (MQTT) message broker, RabbitMQ is embedded in the virtual machine, and allows to the IoT devices the communication with the server using MQTT messages. The MQTT was chosen due to its emphasis on restrained hardware. When IoT devices have connected to the LAN and communicate through a lightweight messaging protocol, they start the messages publishing to the broker.

Furthermore, a NodeJS script is used for running on the VM. The NodeJS purpose is to connect RabbitMQ and subscribe the incoming messages. The incoming messages are subscribed directly into the IOTA Tangle. Data of transactions are the vehicles related data, collected from IoT devices. Once transactions are verified and

inserted into the ledger, NodeJS script generates the hash value, necessary for retrieving data from the Tangle.

In Figure 6.2 the message broker and the script operation is presented as middle mean between the employed IoT devices and the Tangle. The IoT devices are considered as low-power, constrained regarding their resources capability, and vulnerable to cybersecurity attacks. On the other hand, the IOTA Tangle is considered as a secure storage mean. IoT devices generate and collect data and the Tangle stores it, allowing them to work in synchronised tandem. In this way the constrained and vulnerable nature of the IoT paradigm is addressed. All source code of the testbed is freely available on Github (s5068096A (2021)).

6.4.1 Comparison to a Real World Use Case

There are differences between the testbed prototype and a real-world implementation of this technology. The private Tangle instances may be established and maintained within the IOTA framework. Nodes run the software that provides read and write access to the Tangle (IOTA (*IOTA-Nodes*)). In a smart city scenario, where citizens personal information and location of people may be included, the read and write access must be provided to the local authorities or another trusted authority, which can create and manage these private nodes.

In addition, in a smart city scenario, the employed technological enablers that establish the communication channels between vehicles and traffic infrastructures may differ. For instance, the MQTT messages over WiFi may be replaced by a peer-to-peer connection that uses 5G networks. The system may be able to collect data from the vehicles once the infrastructure is in place. The collected metrics may involve the same data, as discussed above.

Some representative scenarios implemented in the PoC system are presented below:

- **Congestion Detection**: the ability to detect and record traffic offers important information related to the road or routes congestion at a particular time period. This information may be useful when considering modifications to existing roadways or developing future traffic flow systems.
- **Adaptive Control**: The application of adaptive controls over roads and traffic flow may improve the traffic flows and road usage by vehicles. This may be related to other statistics, such as the number of lives saved by emergency service vehicles. This can be achieved by the creation of green paths. In Figure 6.3, a demonstration related to the adoption of adaptive control for providing green routes and facilitating emergency service vehicles is presented. In this way, traffic is adjusted to the current needs of a smart city environment and enables the facilitation of emergency and critical services, such as healthcare, based on decision making algorithms.
- **Connected vehicles and roads**: The interconnectivity and the proactive data collection regarding vehicles, traffic flow and performance of traffic furniture may enable the conduction of digital forensic investigations after a cybersecurity related incident occurrence on roads.

6.4.2 Applying the ITS Threat Model

The threat model application over the implemented system focuses on the identified high rated attack vectors related to devices, network, and DLTs. Based on the threat

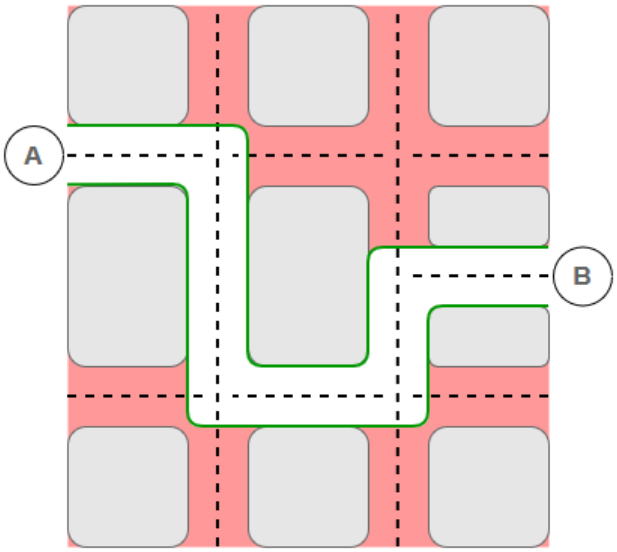

FIGURE 6.3: Facilitation of an emergency vehicle demonstrating the ideal route from point A to point B

model presented above, the highest rated identified threats in terms of an Intelligent Transportation System include cyber-enabled physical attacks. Cyber-enabled physical attacks refer to cybersecurity breaches that may affect the physical plain, as well. Corresponding attacks related to network and device are rated high for identical reasons, since they can be possible entry point for a cyber physical attacker. On the other hand, based on our PoC, remote over the air (OTA) updates have been disabled as a mitigation measure against the malware injection.

Furthermore, physical connectivity to exposed ports attack vector is high rated, due to the instantaneous repercussions that it can incur. In the context of the PoC, in case of exposed ESP-32 micro USB ports, malware injection may take place. This will affect the entire network, apart from the device alone, driving to installing malware and uploading malicious firmware network attacks that are both rated high, as well. Our PoC remains exposed to these attacks.

Finally, DLT networks may be severely affected by distributed Denial of Service attacks. In the Tangle case, the bottleneck of transaction validation grows as transactions number increases rather than shrinks, as in typical Blockchain systems. This is due to scalability of the Tangle, which makes DDoS attacks less severe in certain use cases. This applies both to our prototype and real-world implementation.

6.5 Chapter Summary

The Internet of Things paradigm is considered as a key technological enabler for various paradigms, such as smart cities. On the other hand, IoT is considered as a constrained technological enablers regarding its memory capacity and cybersecurity resilience. The adoption of other technological enablers along with the IoT paradigm may address the constrained nature of the latter.

The Distributed Ledger Technology is one of the technological enablers that can facilitate the IoT paradigm to overcome some of its challenges pertaining to data

immutability, data timeliness, and data security and privacy. Literature provides a variety of works that have investigated the coexistence and collaboration between IoT and DLT and propose new theoretical architectures for the implementation of both technological enablers, without demonstrating a real world implementations. In addition, there is a lack of IoT-specific threat models in the literature.

In this Chapter, the aforementioned research questions have been addressed under the prism of Intelligent Transportation Systems. It has been considered that ITSs involve both IoT and DLTs systems and three tiers of attack vectors based on devices, network and DLT layers are identified.

For the evaluation of the identified ITSs based attack vectors, the DREAD threat modelling scheme has been employed.

The presented threat model was demonstrated on a novel PoC IoT networked system, which uses the IOTA Tangle distributed ledger as a means of generated data storage by helping critical appraise the deployment of the system against the highest rated threats.

Chapter 7

Vulnerabilities Exposure Driven Intelligence in Smart, Circular Cities

7.1 Introduction

Smart cities have settled and transformed an urban environment into an intelligent ecosystem adopting various technologies and business models (Profile (2021)). In an effort by city stakeholders for supporting better decision-making, enhancing city operations and finding solutions to city problems, they provide data to end-users (Neshenko et al. (2020)).

The extensive growth of smart cities globally, comes along with the extensive increase of cybersecurity incidents. Various use cases indicate the increase of vulnerabilities and risks exploitation and systems tampering within smart cities ecosystems. For instance, back in 2015, more than 200,000 of people affected by a third party illegal entry into a power grid in Ukraine (Case (2016)). In addition, in 2017, a ransomware attack, called *WannaCry* performed against various service providers globally. National Healthcare System of the United Kingdom had been affected, without being able to provide any kind of services, apart from the emergencies (Mohurle and Patil (2017)).

Also, due to the lack of cyber-resiliency of employed IoT devices by Dallas city, hackers tampered the operation of traffic lights and the hurricane sirens, which were turned on in the middle of the night (Mettler (2019)).

The attack use cases above indicate the threat landscape of smart cities introduced by advanced technological enablers and the complexity of urban environments. In particular, traditional technology systems standards for cyber security cannot address threats of smart cities concepts. The complexity of interactions of technological enablers, such as IoT and Cloud, increases the impact of cyber attacks and incommodes the identification of threats and risks within a city. As such, the protection of a city from cyber attacks is critical, not only for the proper operation of infrastructures, but for the protection of public safety and legacy infrastructure.

Since urban ecosystems across the globe invest effort, resources and budget to evolve their infrastructures by the deployment of technologies, such as IoT paradigm, 5G, Software Defined Networks, and so forth. For the needs of this research, an empirical analysis of the current exposure of smart cities and the existing vulnerabilities, based on an updated vulnerability dataset that includes quantitative research data from independent studied and evaluates the maturity and performance of cities in order to be considered as smart is performed. We focus on the cities that have adopted a (data-driven) Circular Economy agenda, which we consider that it refers

to the increase of the potential vulnerability exposure of a city. On the other hand, findings indicate that although smarter cities obtain higher vulnerability exposure, the investment on technological enablers and human capital enables the moderation of this exposure, forcing it to be reduced.

From a cybersecurity perspective, attacks against either smart services and infrastructures or citizens, may discourage the latter to use the city provided services (Alsultanny (2014)). As smart cities include a variety of technological domains and themes (see for instance Ismagilova et al. (2019) for a comprehensive list of research themes), we declare that vulnerabilities comprise a horizontal theme, "*expanding*" and affecting many other domains.

Furthermore, the key contributor of risk and attack vector (when a comprehensive exploit is available) approaches is a vulnerability. As such, vulnerability management in terms of a smart city ecosystem is critical for the local government and responsible authorities, which should extend the scope beyond provided services and infrastructures and reach the end devices.

For instance, due to the dependency of smart city services on mobile communications, local authorities seeking into ways of becoming local Mobile Network operators, especially due to the 5G deployment. The inability of city authorities to identify cybersecurity risks may downgrade the development of suitable security policies.

This Chapter is based on the publication with title *"Vulnerability Exposure Driven Intelligence in Smart, Circular Cities"*.

7.2 Architecture and threat landscape of smart cities

Smart cities infrastructures combine cyber and physical components integrated into critical infrastructures, such as transportation, water and energy. In Neshenko et al. (2020), authors identified 5 tiers of a smart city environment architecture that include physical plain, enablers, data, applications and the management layer. The 5 tiers of smart city architecture are presented below:

- Physical plain tier is involved with physical urban infrastructure, such as roads, buildings and traffic furniture;
- Enablers refer to the technological enablers that facilitate the data collection. Enablers include hardware and software that deliver information to data layer;
- Data layer refers to collected and stored information that facilities various purposes. The collection and storage of information is considered as valuable for smart cities, since crowdsourcing techniques contribute to adopted decision-making algorithms;
- Applications' layer refers to smart solution that are provided to services receivers, citizens and visitors of a smart city ecosystem. This layer is responsible for data-driven application that address challenges regarding provided services. The integrated IoT devices, like sensors and cameras, provide all the necessary information to applications in order to be reconfigured in real time and adapt regarding the current needs of clients for facilitating the provided services;
- The last layer, known as the management tier, is responsible for service provisioning, asset management and security.

The architecture and threat landscape of smart cities ecosystems, as described above is presented in Figure 7.1.

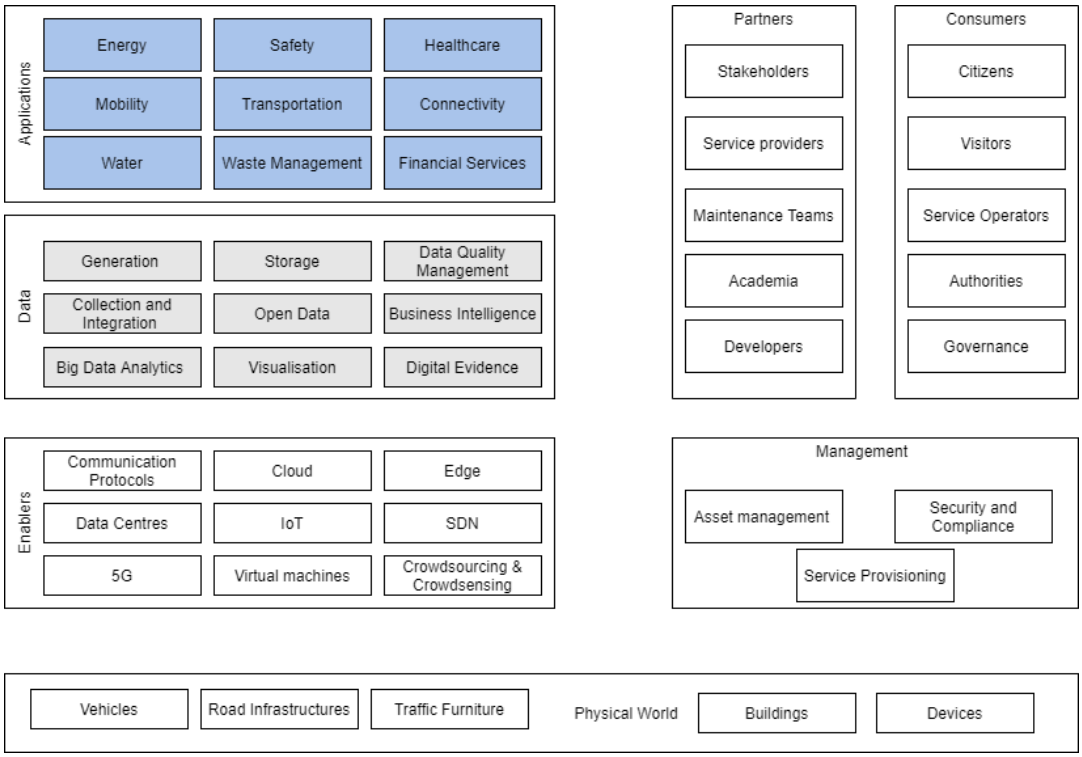

FIGURE 7.1: A high level smart city architecture (adapted from Neshenko et al. (2020))

7.3 Smart City threat landscape

The high integration of different technological enablers and the complexity of a smart city environment provide fertile ground for cyber threats and vulnerability exploitation challenges. Smart cities around the world have become victims of cyber attacks that affect their operation and quality of citizens' life. As such, the identification and assessment of potential vulnerabilities and risks in terms of a smart city may play a key role for the protection of city infrastructures and citizens safety.

The deployment and implementation of cyber security techniques into a smart city environment is critical and challenging, due to the heterogeneity of technological enablers, the constrained nature of IoT devices, the limitations determined by legal authorities, and the difficulties with security and privacy measurements.

Potential threats that may affect a smart city environment vary and refer to different layers of smart city architecture.

First of all, a smart city environment inherits vulnerabilities of traditional computer systems. These vulnerabilities include viruses, eavesdropping, malicious content injection, software hijacking, memory exploitation, access to personal and sensitive information and data misuse. Also, the interaction of digital and physical infrastructures, the usage of new communication protocols and the employment of third-party providers come along with new security threats and increase the exposure surface of a smart city ecosystem.

Furthermore, hardware failure, software and human errors and electrical interruption can be considered as threats as well.

In addition, as defined by Neshenko et al. (2020), there are four categories of threats within a smart city environment. These threat categories include exploratory threats, infrastructure sabotage, data manipulation and third party vulnerabilities.

Exploratory threats aim to identify the vulnerable resources and gain access to a smart city by guessing or stealing users identities. The impact of these threats may involve gain of privileged access to data or subsystems, control of infrastructures, alteration of valuable information and data loss, reputation damage, performance reduction, and so forth.

Infrastructure sabotage threats main goal involves the injection of malware to a smart city systems or the overwhelm of core resources in order to take control over city's infrastructure and make them unable to serve citizens. Threats of this category may affect the public safety, causing physical damage and data loss, performance reduction and data leakage.

Data manipulation threats refer to compromising of data confidentiality and integrity through different ways, such as data tampering, corruption, misuse and disruption of decision making processes, affecting public safety, personal identity theft and privacy violation (Neshenko et al. (2020)).

Finally, third party vulnerabilities are related to integrated service providers, such as the Cloud and Edge Computing, vulnerabilities and risks, which attackers may exploit in order to gain access to smart city's resources and infrastructures. Some of the impacts that this threat category includes are related to the reputation of service providers damage, unauthorised access to city's infrastructure and financial loss (Neshenko et al. (2020)).

Four basic definitions of what a security incident, attack, vulnerability and threat are provided by NIST resource centre.

Security Incident

"An occurrence that actually or potentially jeopardises the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies" (NIST Special Publication 800-53 (2013)).

Attack

"An attempt to gain unauthorised access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality" (NIST-SP – 800-82 (2015)).

Vulnerability

"Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source" (NIST-SP – 800 37 (2018)).

Threat

"An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss. Note: The specific causes of asset loss, and for which the consequences of asset loss are assessed, can arise from a variety of conditions and events related to adversity, typically referred to as disruptions, hazards, or threats. Regardless of the specific term used, the basis of asset loss constitutes all forms of intentional, unintentional, accidental, incidental, misuse, abuse, error, weakness, defect, fault, and/or failure events and associated conditions." (NIST-SP – 800-150 (2016)).

7.3.1 Interdependency and Heterogeneity as Cybersecurity Threats Landscape

The heterogeneity of a smart city ecosystem comes as consequence of the coexistence of various technological enablers within the same environment provide solutions to city's issues and serve citizens needs.

In addition, the infrastructures' interaction with service providers and humans enabled through the information sharing creates new opportunities for supporting and enhancing operation of smart city. In essence, we can say that all services, stakeholders, infrastructures and citizens interact with each other through information sharing and reconfigure the operation of a city when it is necessary depending on its current needs.

On the other hand, this high interdependency and heterogeneity of smart city ecosystems raise the complexity, introduce new vulnerabilities and risks and increase the severity of the exploitation. An affected by a vulnerability exploitation service or infrastructure component enables the potential impact of others. As such, the effective operation of a city and public safety may be affected. The interdependency between components of a smart city ecosystem enables the occurrence of cascade effects. Depending on the nature of the interdependency, the cascading effect might be logical, cyber, physical or geolocation related (Kure, Islam, and Razzaque (2018)).

In addition, the identification and assessment of vulnerabilities within a smart city is challenging due to the complexity of the environment and the different cybersecurity requirements of all the city members and components. The deployment of a dependency model in terms of a smart city may reveal essential details related to fundamental characteristics and system topology, and contribute to the development of city's vulnerability profile, by identifying all vulnerabilities and risks estimating the severity over all the components of the city (Neshenko et al. (2020)).

7.4 The CVSS scoring system

Cybersecurity teams globally benefit from universal frameworks that can be used for evaluation and comparison purposes related to cyber risks and threats. One of the most well-known threats and risks evaluation framework is the CVSS scoring system that is used to determine the severity level of cyber vulnerabilities and help address vulnerabilities and risks in the right order.

The Common Vulnerability Scoring System (CVSS), in particular the CVSSv3.0 that this research takes into consideration, evaluates vulnerabilities of the principal technical characteristics of software, hardware and firmware. The version 3.0 of CVSS scoring system has been launched in 2015, which introduces a novel scoring system that presents a more realistic and accurate side of vulnerabilities (Balbix (2019)). The CVSSv3.0 introduces an addition vulnerability base metric, the critical, that may facilitate a strict assessment of vulnerabilities that may affect a smart city in order to be prioritised and addressed faster (Team (2015)). In this research, vulnerability assessment and prioritisation within the realm of smart cities plays a critical role for the definition of the vulnerability exposure of a city, and the employment of a Digital Forensic Readiness Framework (DFRF) dependent on the maturity level that the city has achieved, since vulnerabilities exploitation on higher maturity levels may affect more a city. The assessment of a vulnerability as *critical* may provide to frequent monitoring and collection of critical infrastructures and digital evidence that may facilitate an investigation after the exploitation of this vulnerability.

The CVSSv3.0 score calculation lies on various metrics. CVSSv3.0 scores range between 0 and 10, from low to critical severity vulnerabilities, with 7 to 8.9 scores represent *high* severity vulnerabilities and 9 to 10 scores represent *critical* severity vulnerabilities. The CVSS is composed of three metric groups, Base, Temporal and Environmental (Scarfone and Mell (2010); XM-CYBER (*What is Common Vulnerability Scoring System?*); Katos Vasilis (2019));

- Base metrics reflect the severity of an identified vulnerability according to vulnerability intrinsic characteristics. Base scores of vulnerabilities do not change over time. In addition, base score includes exploitability impact, which is a sub-metric element.
- Temporal metrics reflect the severity of vulnerability characteristics that are evolved over its lifetime. These metrics measure the current state of exploitability and the availability of remediation tools, such as patches (exploit code maturity, remediation level, report confidence).
- Environmental metrics evaluate vulnerabilities severity depending on a specific implementation or environment. The calculation of environmental score evaluates the requirements of a system or environment regarding confidentiality, integrity and availability.

Organisations that adopt the CVSS scoring can modify base scores measurements relying on the mitigation that they have applied or the current value of the assets that may be affected.

Since the CVSS scoring system provides valuable information for identified vulnerabilities and creates a standardised practice across communities, it has gained popularity, especially within the realm of the cybersecurity community.

On the other hand, the CVSS scoring system has received criticism regarding its reliability, although it is adopted by various organisations, including National Vulnerability Database, the Open Source Vulnerability Database and the Computer Emergency Response Team (CERT) Coordination Centre (Scarfone and Mell (2010); XM-CYBER (*What is Common Vulnerability Scoring System?*); Katos Vasilis (2019)).

7.4.1 Advantages and Limitations of CVSS

The use of the CVSS scoring framework is widely adopted by cybersecurity specialists. This framework is universally recognised as a useful tool for evaluating cyber threats and risks, despite the criticism regarding the validity of the calculation of severity of vulnerabilities exploitation.

The CVSS includes advantages and limitations. The advantages of CVSS include:

- The CVSS is a global practice that does not have multiple implementations. The CVSS defines a common vulnerability vocabulary, nomenclature and scoring framework;
- It provides a standardised practice and base metric across communities;
- The CVSS provides lists of existing risks, and their base scores, which need to be mitigated;
- The CVSS provides a standardised, vendor- and platform-independent method for assessing vulnerabilities. It is an open framework that provides transparency about the individual characteristics and methodologies used to derive final vulnerability score.

Limitations of the CVSS include:

- The calculation of the CVSS score is considered as *incomplete*, since only base score does not indicate the severity level of a threat or a risk. Temporal and environmental scores must be taken into consideration as well;
- In the CVSS scoring framework, there are many Common Vulnerabilities & Exposure (CVEs) that obtain the same base score. These identified CVEs are grouped together. As such, CVEs are not prioritised through CVSS and there is no factor that indicates the severity and the prioritisation order;
- The calculation of the base score in the CVSS includes limited variables, *low*, *medium*, *high* and *critical*. These values provide a finite number of possible scores and groups of threats with the same score;
- The CVSS does not take into consideration the age of a vulnerability; Thus, it is not concrete over time;
- Threats and risks base scores are publicly available and accessed by cybersecurity teams through a massive number of databases. Relying on these databases may not be considered as a good practice, since this data does not provide key risk context and does not reflect the true severity level of a real world exploit.

As discussed above, datasets from two primary domains were considered for this research. Data from that source includes identified CVEs in terms of connected and smart cities environments all around the world, their base and severity scores and metrics regarding confidentiality, integrity and availability.

Although the CVSS scoring system has been criticised severely, organisations and Computer Emergency Response Teams globally use this framework to evaluate a vulnerability and its exploitation can cause. For the needs of this research, identified CVEs, calculated base scores and confidentiality, integrity and availability metrics have been taken into consideration.

The CVSSv3.0 scoring system has been adopted over other vulnerability scoring systems, such as OWASP Application Security Verification Standard (ASVS) and Tenable Vulnerability Priority Rating (VPR).

The OWASP ASVS Project is responsible for web application technical security controls testing that provides developers with a list of requirements for secure web applications development. The OWASP ASVS Project provides to the testing of the security controls of web applications, as well as any technical security controls in the environment, against established vulnerabilities, such as Cross-Site Scripting (XSS) and SQL Injection. The OWASP ASVS may be considered as the mean of establishing a level of web application security (Manico (2015)).

On the other hand, the Tenable VPR facilitates organisations to improve their remediation efficiency and effectiveness, by assessing the identified vulnerabilities taking into consideration two components, the technical impact and the threat. The identified vulnerabilities are rated as Critical, High, Medium and Low. The technological impact measures the impact on confidentiality, integrity and availability after a vulnerability exploitation. The technological impact is equivalent to the CVSSv3.0 impact subscore. The second component, the threat, reflects both current and future threat activity against an identified vulnerability. Examples of threat sources affecting VPR include public proof of concept (PoC) research, exploitation reports on social media, the emergence of exploit code in exploit kits and frameworks, and

exploits on the dark web and hacker forums. The threat component of this standard plays a key role in prioritising the identified vulnerabilities that pose risk to an organisation.

First of all, the OWASP ASVS standard may not be compatible with a smart city ecosystem, since it focuses on web applications and the assessment of web applications vulnerabilities during their development. The available dataset for this research include identified CVEs, which are obtain a CVSSv3.0 base score. In addition, CVSSv3.0 takes into consideration the environmental score of an identified vulnerability, that is critical for a smart city ecosystem, since the achieved maturity level may be taken into consideration as well.

Also, the Tenable VPR standard can be considered as more compatible to smart cities concepts and to CVSSv3.0. In addition, according to (Nessus (2022)), the VPR is more efficient than CVSSv3.0, since it takes into consideration the age of a vulnerability and prioritises each identified vulnerability taking into account both technical characteristics and threat intelligence. However, it should be mentioned that both standards are considered as equivalent. In this case, the CVSSv3.0 is adopted more and established enough in order to be considered as more trustworthy.

Furthermore, the peer operators approach that is applied in this research and the coexistence of various partners, such as local authorities, stakeholders, organisations, CERTs that should exchange data and communicate with each other, and share information with other urban environments operators, may raise coordination challenges. The CVSS provides a common practice and common vulnerability vocabulary that is globally accepted, without being necessary to be customised in every case. As such, cybersecurity specialists can have easy access to data related to identified vulnerabilities and share this information with other cybersecurity specialists from different cities or countries without being necessary to adjust it.

Also, prioritisation of CVEs has been achieved for the need of this research, since this research does not rely only on the base score that a CVE obtains, but, on the maturity level and the exposure profile of a city and the sector where the exploitation may take place. Finally, this research does not rely only on identified CVEs for smart cities concepts, but, on other parameters that can form the exposure profile that a city obtains.

7.5 A Smart City Maturity Level and Vulnerability Exposure Profile

As discussed in Chapter 3, a maturity model facilitates the structure of a city *CE readiness* against a set of dimensions. For the needs of this research, a maturity model for smart cities has been employed, described in Ideal-Cities (2018). The adopted maturity model illustrates the technological roadmap for a city adopting a CE agenda. The levels of maturity that have been identified in Ideal-Cities (2018) involve *Instrumented, Connected, Smart and Responsive* city. In Figure 7.2, the maturity model paired with the potential impact of vulnerabilities in the respective level is outlined.

It is evident that reaching the Responsive maturity level, it is required from a city to achieve high levels of connectivity and integration with software services that are delivered in the whole vertical. Thus, the vulnerability exploitation impact at a particular maturity level is expected to be different from the impact of the same vulnerability exploitation on another maturity level.

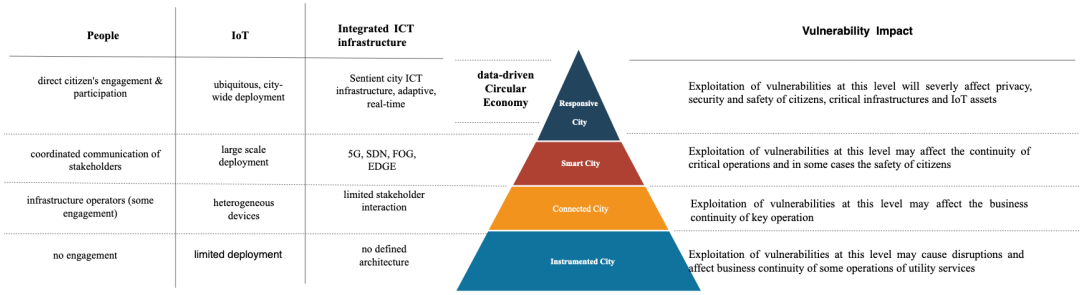

FIGURE 7.2: Vulnerability impact, dependent on the city maturity level (adapted from Ideal-Cities (2018))

This indicates that the impact of a vulnerability will be increased if the maturity level that a city has achieved is higher than another, carrying a large amount of risk, even if the vulnerability is the same in both cases. Expressed in a formal way, if $R_m(\cdot)$ is some risk calculation function with m denoting the maturity level, then for a particular vulnerability v the following should hold:

$$R_i(v) \leq R_j(v)$$

for $i < j$. This means that if two cities with identical vulnerability profile are affected by the same vulnerability exploitation, the city that has achieved the highest maturity level will also obtain the highest risk. This statement is captured in some quantitative vulnerability measurement systems.

One of these quantitative vulnerability measurement systems is the Common Vulnerability Scoring System (FIRST (2020)); Mell, Scarfone, and Romanosky (2006), where the severity of a vulnerability can be adjusted to the so-called environmental variables, apart from the base and temporal scores, provided by the CVSS.

To the best of our knowledge, a methodology development for the production of a suitable vulnerability scoring system with an environmental metric group in terms of a smart city infrastructure remains a challenging process. For instance, even a concise threat and risk model for smart cities is presented in Wang, Ali, and Kelly (2015), there is limited evidence regarding the adoption of the CVSS environmental score dimension. Actually, the CVSS scoring system itself has been receiver of criticism from research and practitioner communities (Johnson et al. (2016); Gallon (2010)), with alternatives being presented, as the proposed by Spanos and Angelis (2015). On the other hand, despite criticism that the CVSS has received, it is still applied and validated through various contexts and scenarios (Cheng et al. (2012)).

From the discussion above, it is fairly evident that the technological integration of a city may be reflected on the maturity level that city has achieved. The adoption of technical enablers for facilitating services and purposes of a city and for addressing challenges that are raised from the needs of citizens and visitors, come along with the increase of vulnerability and risk exposure of a city.

7.5.1 Datasets - limitations of research

For the needs of this research, two major domains datasets has been taken into consideration. The first domain covers the interdependent factors or variables of the study and it refers to the description of cities as presented in the Cities in Motion (CiM) research (Berrone and Ricart (2019)). The cybersecurity related dataset addresses the dependent variables. In addition, the ENISA vulnerabilities 2018-2019

dataset (Rostami (2020); ENISA (2019)) has been extended. This dataset includes contextualised vulnerability data from a variety of sources. Beginning with the NVD database and the included list of vulnerabilities, we enriched it with tactics and techniques as specified by the ATT&CK framework[1] as well as the exploit database[2].

Even though information from Shodan regarding the number of exploits is involved in the original ENISA dataset, it does not indicate the actual exposure, providing details of devices that are potentiality vulnerable to particular exploits. Thus, the ENISA dataset has been extended to include this information as well.

In addition, IP addresses geolocation of identified vulnerable devices was used for pivoting purposes between the vulnerability and city/country domain data. As a result, we came up with a collection of vulnerabilities associated with devices, which were then mapped to geographical locations. Consequently, the geolocation accuracy is constrained and bounded by geo-mapping process of Shodan. To that aim, the queries for geolocation searches used the (country, city) tuple to eliminate ambiguity in the city data and to overcome any city synonyms.

Several limitations of this research have been identified, starting by the fact that there is no information related to the type of service or ownership of vulnerable devices. As such, a city can be seen only as one entity, without being able to distinguish the variety of services and sectors within an urban environment (critical infrastructures, different sectors, devices of public and private domain and so forth).

Furthermore, the dataset does not cover IPv6, and as such not taking into consideration a considerable number of IoT devices. This fact may affect the results of higher maturity level cities and especially those that already use 5G. As a result, we acknowledge that the current study's findings represent the best-case scenario and the lower bound of the attack surface. Also, the scope would be limited to more *traditional* and core services, due to the exclusion of IPv6. Nonetheless, this limitation, combined with the geolocation method, highlights the necessity for a city's NOC/SOC equivalent to invest in asset detection and a register, which is a non-trivial effort in practise. Furthermore, IP addresses that expose devices via VPN or TOR networks were not filtered out, since were not expected to introduce any significant bias in the analysis.

It should be mentioned that the final dataset may include sparse entities. On the other hand, there are approaches for increasing the population of sample of a defined feature with a low number of data points (for instance, see ML based dataset imputation applied on the ENISA dataset (Rostami et al. (2020))), this was not mandatory for this research. A summary of the used resulting dataset features is presented in Table 7.1.

The second limitation is related to this research refers to the results volatility due to the live vulnerability exposure data nature. In particular, the recorded data from Shodan indicate a snapshot of a specified time period. For the purpose of this research, it is considered that vulnerability data are used for revealing if there are relationships between them and other types of data, related to different dimensions, such as behavioural and economic variables. It should be kept in mind that it would be more appropriate to acquire and store files with vulnerability data in order to run longitudinal research that may provide important and higher quality details. To this end, other vulnerability exposure databases can be considered, such as Censys[3] and

[1] https://attack.mitre.org
[2] https://www.exploit-db.com/about-exploit-db
[3] https://censys.io/

TABLE 7.1: Dataset description

Vulnerabilities		**City metrics**	
source	features	source	features
NVD (NIST (2020))	CVE, CVSS	CiM (Berrone and Ricart (2019))	96 variables over 9 indicator categories, including population, human capital, technology, city in motion score
Shodan	#vulnerable devices, geolocation	IMD (Bris and Cabolis (2020))	adoption of digital technologies, citizen perceptions, smart city ranking
MITRE (CWE (2020))	CWE	C40(C40-Cities (2020))	leading CE cities

Zoomeye[4]. It should be mentioned that the latter includes historical exposure information. Finally, since exposure metrics have been conducted regarding the Shodan's assigning CVEs methodology to devices and services, the results and finding accuracy rely on the implied vulnerabilities disclaimer of Shodan.

Finally, according to the vulnerabilities quantitative measures, this research inherits the challenges of the CVSS scoring system. Although the CVSS approach is an acceptable one and it is considered as trustworthy (Johnson et al. (2016)), various applications present conflicts related to assigning values process and its validity.

According to the National Vulnerability Database (NVD), which can be used to keep an authoritative record of CVSS scores, there is a significantly poor correlation of several impact metrics (Confidentiality, Integrity, and Availability) between CVSS version 2 and version 3. Particularly, the integrity and availability correlation between version 2 and version 3 were found to be 0.34 and 0.38 respectively (ENISA (2019)).

7.5.2 Analysis and Findings

The analysis that follows is two-fold. Firstly, we use the available datasets as means for evaluating whether these published, available data are aligned with, or can interpret or support assumptions and policy directions as stated in the recent literature. Secondly, a series of approaches smart city stakeholders could adopt when developing vulnerability management capabilities is presented.

The approach followed for the analysis is a top-down one. The process starts with the analysis of data on a city level and the evaluation of countries vulnerability exposure by taking into consideration additional macroeconomic measures, along with the contribution of the hypotheses that are presented below. The following hypotheses are created for this research, taking into consideration the Cities in Motion (CiM) research, which indicates particular dimensions of a smart city and how these may be used as indicators of smartness, and how these dimensions may affect the vulnerability exposure of a city that is defined below. Then, it moves on to city comparisons and eventually to the cities themselves.

For developing meaningful comparisons, the variable of population to normalise the data of vulnerability is employed. Two approaches can be followed for doing this, namely dividing the variables of vulnerability by the population or adding the latter to interdependent variables set in the regression model(s).

[4]https://www.zoomeye.org/

Furthermore, the city vulnerability exposure E_c of city or country c is defined as:

$$E_c = \sum_{v \in V_c} |v| * b_v$$

where V_c is the multiset of discovered vulnerabilities for c and b_v is the CVSS base score of vulnerability v. Due to the vulnerability exposure Kolmogorov-Smirnov normality test failure, the natural logarithms value $ln(E_c)$ is investigated instead, since this variable stick to a normal distribution (K-S significance: 0.604), that allows to the regression models to be constructed and tested.

Scope: Country

A study on a country level enables the vulnerability exposure contextualisation, since it can indicate factors that may provide a country's historical efforts and profile based on geopolitical matters. A country level study analysis may be used as a base line for an operable cyber situational awareness capacity to be deployed. For example, the available budget for investment of a city may include external funding, such as national or international funding, and income from major stakeholders and citizens in a tax form. Keeping in mind that national level investments related to the cybersecurity capacity enhancement may depend on the Gross Domestic Product (GDP) of a country (Creese et al. (2020); Calderaro and Craig (2020)), the hypothesis below is investigated:

H_1 : The severity of vulnerabilities in countries decreases with GDP per capital.

TABLE 7.2: Country regression model

Model Info	**Model Fit**
Observations:177	F(3,173)=27845, p=0.000
Dependent variable: `log_exposure`	$R^2 = 0.326$
Type: OLS	Adj. $R^2 = 0.314$

	Coefficients					**Collinearity stats**	
	B	std. error	β	T	p	Tolerance	VIF
`intercept`	11.177	0.268		41.640	.000		
`GDP`	2.973e-005	0.000	0.218	2.917	.004	0.699	1.431
`GCI`	3.939	0.852	0.353	4.623	.000	0.667	1.498
`population`	3.501e-009	,000	0.210	3.232	.001	0.921	1.086

Table 7.2 presents the outcome of the regression analysis, which is based on vulnerabilities exposure against independent variables, such as GDP, Global Cybersecurity Index (GCI) and population. The Variance Inflation Factors (VIF) ranges below 10. Alternatively, it can be said that the Tolerance values are assigned values greater than 0.1, showing that no co-linearity exist between the interpretive variables, as such the H_1 is rejected. The importance of the adjusted R^2 is high, since it indicates that the Global Cybersecurity Index variable determines better the level of exposure, comparing to the others. More precisely, while GDP and population variables tend to increase the attack surface, the GCI follows a positive connection overall. In essence, the increase of GDP enables the investments in networked devices, but at the same time countries tend also to invest for deploying and improving their cybersecurity strategies, as presented by the GCI.

On the other hand, this approach is not standard for *all* the countries. Countries with low GCI score and high exposure do not have applied and efficient vulnerability management plan. At the time of writing, Cape Verde, Paulau and Erithrea are the countries with the lowest GCI and the highest exposure. Interesting is the fact that at the time of writing (Q4 of 2021), Cape Verde government approved the establishment of a Computer Security Incident Response Team (CSIRT) of national level and the introduction of a legislative framework along with a National Cybersecurity Centre (Telecompaper (2021)). This is a crucial development, since a country with high exposure and little cybersecurity investment may be an easy target, and the implementation of security controls and procedures is critical.

It should be noted that the regression model presented above is a vulnerability management agnostic. The existence of a vulnerability management scheme may be indicated by a high GCI score, even though there is no precise indicator for that, only the generic technical and capacity building pillars. As a result, a country government can employ only this model for benchmarking their position and do the comparison between the actual exposure and the estimated value. This will indicate them the cybersecurity related needs and enable the prioritisation of a vulnerability management plan.

A second metric that indicates the cybersecurity effort in regard to the exposure is the log of the ratio between E_c and the GCI. This metric is normally distributed (Shapiro-Wilk test significance: 0.056), with a mean of 14.685, standard deviation of 2.28 and within the range of [9.73, 20.92]. Countries obtaining the low end of distribution may have over-invested in cybersecurity even their actual exposure is low, whereas countries with higher distribution may be overexposed.

Scope: City

Moving on to a city level, the analysis is based on the cities current maturity level and adopted agendas.

The analysis is performed based on four classes of cities:

Class 1: the `plain` city, refers to cities without indicated progress or intention of deploying a smart city agenda;

Class 2: the `circular` city, refers to cities that have adopted a CE agenda. It is considered that these cities may not have adopted a clear data-driven approach;

Class 3: the `smart` city, refers to cities that have been evaluated and involved in the IMD or Cities in Motion study;

Class 4: the `both` city, refers to cities that have deployed both smart and CE agendas, as specified in the C40 dataset.

Due to the statement that CE cannot be delivered without the employment of technological ICT enablers based data-driven dimension(Askoxylakis (2018); Antikainen, Uusitalo, and Kivikytö-Reponen (2018)), it is proclaimed that cities with an employed CE agenda have adopted a more definitive and mature technological roadmap than others.

In Figure 7.3, the pairwise vulnerability means comparisons of different classes of cities is summarised. Even though the average CVSS base score fluctuates around the mid 7s in all cases, the highest score is obtained by `smart` and `plain` cities (not significant difference between them). The `circular` and `both` classes have statistically significant smaller scores.

	N	#CVE	mean
`plain`	87	16.8m	7.580
`circular`	5	6.2K	7.533
`smart`	91	22m	7.541
`both`	11	7m	7.339

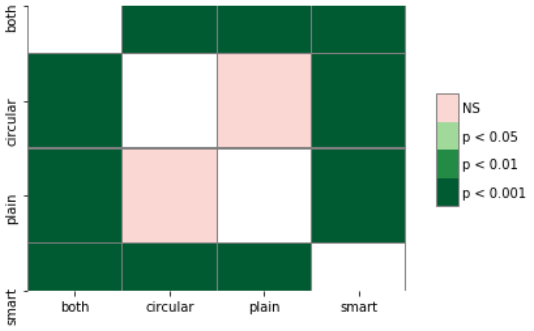

FIGURE 7.3: Pairwise comparisons of the four city classes

Since a comparison of means is a static technique, the first exploratory analysis is limited. Furthermore, the sample regarding the cities with an adopted CE agenda only is small ($N = 5$). As such, we consider an additional class of cities, the `motion`, which includes all the cities that present early indicators of *smartness* - low maturity level achievement. The cities in the `motion` class obtain higher levels of *smartness* than the `plain` cities, where there is no any technological integration.

The formulation of the following hypothesis is facilitated by the above:

H_2 The city type modifies the vulnerability exposure, so that smarter cities have a larger vulnerability exposure than plainer cities.

H_3 The population of cities increases the vulnerability exposure.

H_4 The level of technology decreases the cities vulnerability exposure.

The H_2 primarily focuses on the overall exposure than the score of severity. Since the technological integration is higher in smarter cities than in the plain, the cyber attack surface is expected to increase.

In addition, regarding H_4, we consider that there is an inversely proportional relationship between the technology score and exposure. This complies with the indicator definition in the Cities in Motion research, where innovation measuring indicators are included, the web index that measures the social, economic and political benefit that comes from the Internet, as well as social media popularity to users, WiFi coverage, speed of broadband, and so forth.

It is expected some of these indicators to increase the exposure of cities, but, it is also expected that the higher technological integration requires higher expertise in cybersecurity techniques for secure and safe infrastructures to be provided to the citizens. Although the technological integration within cities ecosystems is expected to affect the vulnerability exposure, it may be not enough for decreasing the exposure. It should be kept in mind that technical means alone may not work for reducing the exposure, but other aspects, such as human under the prism of a socio-technical system need to be taken into consideration as well.

The regression results are introduced in Tables 7.3 and 7.4. In model 1, the `city_type` independent variable is related to the four city classes, where `circular` has been replaced by `motion`. In model 2, this variable is exploded into its various types in order to validate $H2$. We should mention that due to the increase of the type variable, no intercept exists in this model for avoiding multicollinearity.

The results indicate the confirmation of hypotheses H_3 and H_4. More precisely, for H_3, it can be seen that it also holds by observing the β coefficients that confirm

TABLE 7.3: Regression model 1

Model Info			**Model Fit**		
Observations:170			F(3,166)=16727, p=0.000		
Dependent variable: exposure			$R^2 = 0.231$		
Type: OLS			Adj. $R^2 = 0.217$		
	Coefficients				
	B	std. error	β	T	p
intercept	793555.776	743060.891		1068	.287
population	.187	.038	0.348	4891	.000
technology	-20047.553	4737.873	-.304	-4231	.000
city_type	775686.647	276255.132	.196	2808	.006

the order of the city types in accordance to our initial hypothesis, that the cities with higher technology integration may be considered as more exposed that the plain cities.

In addition, the fact that technology alone is not able to address cybersecurity challenges may be confirmed as well.

TABLE 7.4: Regression model 2

Model Info			**Model Fit**		
Observations:171			F(6,164)=16290, p=0.000		
Dependent variable: exposure			$R^2 = 0.372$		
Type: OLS			Adj. $R^2 = 0.349$		
	Coefficients				
	B	std. error	β	T	p
population	.190	.040	.414	4746	.000
technology	-19471.425	4977.282	-.543	-3.912	.000
motion	1706746.558	621010.315	.278	2.748	.007
smart	2175288.130	496238.743	.405	4.384	.000
plain	2180776.000	763190.887	.220	2.857	.005
both	5468921.448	975307.816	.364	5.607	.000

The adoption of the hierarchical clustering provides the opportunity for the creation of a cluster tree, a dendrogram, as presented in Figure 7.4, where each cluster tree contains a group of similar data, in this case a group of cities with similar vulnerability exposure profiles (Statistics-How-To (2021)). The employment of the hierarchical clustering introduces a visual presentation of cities with identical vulnerability exposure profiles, the common ground among these clusters in terms of the vulnerability exposure and which cities may be able to build cooperative relationships in order to address potential vulnerabilities and risks that may affect their infrastructures. In addition, the available dendrogram may be easily understandable by authorities, stakeholders and members of a city, who are not related to cyber security, indicating the actions that should be taken regarding the establishment of collaboration with other cities that obtain identical vulnerability exposure profiles. It should be mentioned that the results of the hierarchical clustering are dynamic,

and the same process should be conducting frequently in order for new clusters to be identified, based on the measures that have been applied for addressing the vulnerability exposure profile of a city. Enriching the available datasets by taking into consideration other dimensions of a city in order to identify its vulnerability exposure profile or the measures that have been applied in order for vulnerability exposure profile challenges to be addressed, the results of a new hierarchical clustering may differ comparing them with the last one.

The Figure 7.4 introduces the vulnerabilities hierarchical clustering (Ward's methods) results on the cities that obtain both, a smart and a circular economy agendas (class `both`).

This information may be useful in two ways. First, this information may facilitate prioritisation and collaboration between the local authorities of a city with the authorities of others that may have the similar vulnerabilities and exposure profiles. Such intelligence might help with information sharing and operational collaboration. The establishment of CSIRTs on a local authority level can facilitate the creation of operational cooperation structures with selective peers by the respective councils. At the time of writing, there is no CSIRT managed by local authorities of a city that performs these activities, but, operators of essential services, such as healthcare, transportation, energy, and so forth. In addition, these operators are employed only by a few countries in Europe, (by four countries, Austria, Czech Republic, Italy, and Latvia). Also, these operators of essential services are managed by the national CSIRTs, and not by local authorities of a city. (see ENISA's CSIRT interactive map[5]).

Regarding the ENISA's CSIRT interactive map, there are not CSIRTs managed by local authorities that can handle and respond to a cyber incident to protect a Smart/Responsive city, and reduce its vulnerability exposure.

Although national CSIRTs can handle a cyber incident, there is a need for local authorities to be involved and be part of the incident response actions that will be taken during vulnerability exploitation. This involvement can be partial or complete and local authorities should be able to assign duties to individual operators that handle specified essential services of a city.

Second, vulnerabilities exploitation and attacks over a city may be an early warning for other *similar* cities with similar vulnerability profile. The lack of geo-political contextualisation of the data may minimise benefits of this approach by preventing severe attacks, like Mirai and Wannacry that affected both the economy and safety. An approach like this may provide to local authorities the ability to establish information sharing strategies with peer cities authorities for the increase of situational awareness and the deployment and improvement of incident response strategies. A representative example of how the vulnerability exposure information can be used from the clusters presented in Figure 7.4, is Paris and Amsterdam case, which belong to the same cluster, meaning that both indicate similarities regarding potential vulnerabilities that may affect them. This would trigger more analysis and research to determine why these two cities are clustered together, with one example direction being to check the exposure profiles against the types of employed devices, protocols and sectors. Both cities are considered as *smart*, since technological enablers are used for various purposes. In addition, both cities may be considered as *pioneers* in terms of smart building infrastructures deployment. Amsterdam maintains one of the most intelligent buildings of the world, the *Edge*, which was build to accommodate the headquarters of Delloite. The building obtains 28K sensors, and a state of

[5]https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

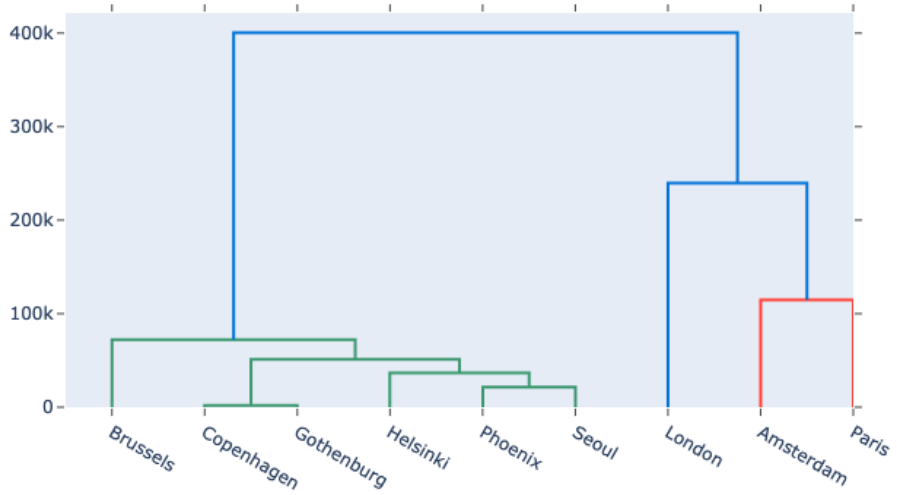

FIGURE 7.4: Hierarchical clustering of cities having a smart and CE agenda (class:`both`)

the art data centre that controls and monitors the building's internal environment (Vayona and Demetriou (2020)).

On the other hand, half of the innovative startups related to smart building industry are located in Paris (Ar (2021)).

A factor analysis was conducted taking into consideration the 20 cities with the highest exposure and vulnerabilities exploitation potential. Analysis generated three factors, each with a substantially high alpha in all cases - over 0.7- demonstrating strong internal consistency and allowing to respective dimensions, cities in this case, to not used and represented by the groups that have been assigned to them. The results of this analysis are presented in the Table 7.5.

The weakness profiles related to four city classes are introduced in the Table 7.6. Even though it is apparent that there are differences regarding the vulnerabilities distribution among city classes, this constitutes a simplistic overview, providing a crude level comparison across these four city classes that has to be further contextualised and verified for extracting actionable information.

Metrics indicating the percentage of most dangerous weaknesses may provide fertile ground for comparison performed on a city level granularity, for cities with similarities regarding to various dimensions. It is interesting to mention that cities that have adopted both smart and circular economy agendas, obtain the lowest percentage of dangerous weaknesses. These finding comply with the results in Figure 7.3. The `both` class of cities presents the least mean among all the classes, even though data of weakness profile are related to unique count of a specific weakness for each city instead of the totals (similar to the CVSS base score).

Scope: Human aspects

Although the scope of software vulnerabilities and exposure is related to employed interconnected devices in terms of an urban ecosystem, an approach of analysing

TABLE 7.5: Factor Analysis (loadings) of top 20 cities with the most potential vulnerabilities

Factor 1		Factor 2		Factor 3	
Ashburn	0.7724	Sydney	0.7245	Chicago	0.9596
Tokyo	0.6910	Central	0.8390	Miami	0.8154
London	0.9050	Incheon	0.8180	Buffalo	0.9574
Dublin	0.8811	Johannesburg	0.9552		
Columbus	0.8197				
Singapore	0.8458				
Amsterdam	0.9710				
Mumbai	0.8992				
Paris	0.8611				
Montreal	0.7529				
Moscow	0.7682				
Dallas	0.7713				
Nuremberg	0.9840				
Cronbach's alpha	0.9614		0.9335		0.9130
Bartlett's sphericity test:		chi square: 24144.232		p-value : 0.000	

and assessing socio-technical factors and non-technical data that are able to contribute to potential vulnerabilities is fundamental. The results of the regression with `exposure` obtaining the role of the dependent variable are presented in the Table 7.7. As defined in Cities in Motion, the first dependent variables were `human_capital`, `social_cohesion`, `technology` and the three cities classes `plain`, `smart` and `both`. Due to the low number of observation, the `circular` class has not been taken into consideration.

After four attempts, by removing one variable at each round, the backward regression was completed, and the end result includes `human_capital`, `smart` and `both`. In addition, the end result is remarkable, since it indicates that smart cities, smart cities with a CE agenda included, and human capital contribute to the prediction of the vulnerabilities exposure in higher granularity than the technological maturity level. From the β coefficients, the vulnerability exposure of smart and circular cities is higher than the vulnerability exposure of a smart city without having adopted a Circular Economy agenda, indicating that smart circular cities tend to become more technologically *hungry*, and more exposed. The deployed maturity model for urban ecosystems presented above is validated by this finding. Furthermore, the β coefficient for human capital negative sigh presents an inversely proportional relationship between the factor and the vulnerability exposure. Also, this finding is significant if the human capital indicators are considered. From the Cities in Motion study (Berrone and Ricart (2019), p.11):

"*The main goal of any city should be to improve its human capital. A city with smart governance must be capable of attracting and retaining talent, creating plans to improve education, and promoting both creativity and research.*"

Furthermore, the human capital variable involves 10 indicators, the majority of which focuses on the education and culture. For instance, the number of universities listed in the 500 top, investment on the education per capital, the number of theaters per city, and so forth, are some indicators of human capital. Taking into consideration this model, it can be stated that a "*sophisticated city is a (potentially) secure*

TABLE 7.6: Weakness profile per city class

CWE	plain	circular	smart	both
20*: Improper Input Validation	✓		✓	
399: Resource Management Errors	✓			✓
119*: Improper Restriction of Operations within the Bounds of a MB	✓	✓		
384: Session Fixation	✓			✓
416*: Use After Free	✓			
787*: Out-of-bounds Write	✓	✓		
287*: Improper Authentication	✓	✓	✓	
476*: NULL Pointer Dereference	✓	✓	✓	
732*: Incorrect Permission Assignment for Critical Resource		✓		
444: Inconsistent Interpretation of HTTP Requests		✓		
126: Buffer Over-read			✓	
200*: Exposure of Sensitive Information to an Unauthorized Actor			✓	
320: Key Management Errors				✓
362: Concurrent Execution using Shared Resource with IS				✓
390: Detection of Error Condition Without Action				✓
400*: Detection of Error Condition Without Action				✓
*In top 25 most dangerous software weaknesses list (CWE (2020)):	75%	83%	80%	16%

TABLE 7.7: Backward regression results

Model Info	**Model Fit**
Observations:173	F(3,169)=5738, p=0.000
Dependent variable: `exposure`	$R^2 = 0.163$
Type: OLS	Adj. $R^2 = 0.148$

Coefficients

	B	std. error	β	T	p
`intercept`	1849657.449	599408.291		3.086	.002
`human_capital`	-13431.430	4856,886	-.204	-2.765	.006
`smart`	1103603.507	501319.562	.166	2.201	.029
`both`	4214523.878	1036497.640	.296	4.066	.000

city".

The aforementioned empirical findings may be summarised in the positions of (Li and Liao (2018)), referencing (Bruijn and Janssen (2017); Klaper and Hovy (2014)): "*considering the way humans, government, and technology interact, security education is desirable to strengthen the knowledge of government officials and citizens with regard to cybersecurity issues*".

It is also important to mention that the dependent variable during the regression running was `exposure_per_person`. As such, the factors `technology, both` and `plain` were included in the most significant model. In other words, the technology factor predominates if the population is used for the normalisation of the vulnerability exposure.

7.6 Discussion

7.7 Chapter Summary

In this Chapter the vulnerability and risk dimension of a smart city ecosystem is introduced and how identified vulnerabilities can affect technologically advanced urban environments in a different way, dependent on the maturity level that the latter have achieved is investigated.

This research revealed that the injection of published smart cities studies data into the domain of cybersecurity and more precisely into the vulnerabilities one, enables the provision of details regarding the factors that affect the vulnerability exposure of a specific system. In particular, this research focuses on smart cities and maturity level-driven vulnerability exposure model for enabling the deployment of a contextualised risk based approach based on exposure data and vulnerability impact. Despite the fact that the used datasets were from independent research or sources, statistically significant correlations were identified.

The presented approach offers several research directions and practical implications. Cities obtain basic challenges in how they operate. Cities governance and business models are adapted to meet the citizens expectations, since they are the end users of deployed and implemented infrastructures.

As vulnerabilities management is critical for cities, and especially for those that have integrated a massive number of devices and technological enablers to address the needs of citizens, the adoption of incident response teams is crucial. Moreover, since cities may be considered as governed initially by local authorities, such as a council, the vulnerability management approach should be determined by these authorities. The involvement of local authorities is critical, for the vulnerability severity and vulnerability exposure of a city to be managed and decreased from the outset. As such, the creation or the employment of an incident response team that will handle a cybersecurity breach within an urban environment, especially within a responsive city, lies on local authorities management decisions, based on various factors, such as applied business plans and financial convenience.

Chapter 8

Digital Forensic Readiness Framework

8.1 Introduction

In this Chapter incident response and the stages of an incident response plan, digital forensics processes and the requirements of digital forensic readiness in accordance to ISO/IEC 27043:2015 are presented. Furthermore, we elaborate on the employment of Blockchain for Chain of Custody (CoC) integrity preservation of evidence objects within a technologically integrated urban environment. Asset identification that may facilitate a digital forensic readiness framework and the employment of NFTs and smart contracts that may facilitate the adoption of the said digital forensic readiness framework is performed. For the needs of this research, a digital forensic readiness playbook (DFRP) to be employed by a city's stakeholders (local authorities, stakeholders, and service providers) for facilitating future digital forensics investigations by preserving digital evidence objects before an incident affects critical infrastructures of a city is introduced. In terms of CE-compatible service model, a crowdsourced approach has been adopted. The core and extended teams and roles, and critical infrastructures of a city that are involved in the proposed DFRP are presented, always taking into consideration the corresponding maturity level of a city. In addition, the collection and creation of digital evidence objects, during the pre-incident phase, after the deployment of DFRP are presented and the steps that a data owner should follow in order for the Chain of Custody integrity to be assured. Moreover, the maintenance and the transmission of evidence objects, after an incident has taken place is introduced, as well as the actions of custodian or custodians responsible for new digital forensics investigation. Finally, the deletion phase of the proposed framework, the two types of evidence objects deletion - namely soft and hard - depending on the maturity level of a city, and the stages until the peremptory deletion of evidence objects by custodians are introduced as well.

8.2 Incident Response

According to NIST:

Incident response is an approach that addresses and manages the next phase of a security breach or a cyberattack. It is also known as IT incident, computer incident or security incident. Goals of incident response include the handle of a situation in a way that limits the damage and reduces the recovery time and cost after an incident (Cichonski et al. (2012)).

Incident response starts before an incident occurs, by creating and training the incident response team and determining all the necessary tools. Incident response

includes four stages, preparation, detection and analysis, containment eradication and recovery and post-incident activity.

The preparation stage involves the implementation of controls based on the results of risk assessment for imitating the damage after an incident. The residual risk will invariably exist even after controls are put in place.

Security breach detection controls play a key role for alerting an organisation when an incident takes place, before it damage severely the entire infrastructure. Incident severity determines if organisation will mitigate the impact of a breach or if it will recover soon from the incident. Analysis is necessary to be done for defining the damage and set it under control. Since an organisation has handled an incident, the report stage indicates all the details related to the incident, the cause and the cost of it and all the steps that organisation followed in order to handle it and prevent future security breaches.

8.2.1 Incident Response Stages

Preparation: Incident response focuses on the holistic preparation of an organisation regarding a security breach. This preparation involves the readiness of systems, networks and applications in terms of security breaches and the establishment of a suitable incident response plan based on the needs of organisation. Even incident response team is not responsible for incident prevention, this process is fundamental for the success of incident response plan. Some examples of available tools and resources that may facilitate an incident handling include contact information of incident response team, incident reporting mechanisms, issue tracking system for tracking incident information, encryption software, Digital forensic workstation and/or backup devices, blank removable media, packet sniffers and protocol analysers, digital forensic software, port lists, network diagrams and lists of critical assets, cryptographic hashes of critical files, and so forth.

Securing efficiently organisation systems and networks is important in order for an incident to be kept reasonably low and to not cause damages to business processes. Insufficient security controls means higher volume of incidents and overwhelm of incident response team.

This might result in slower and incomplete responses that can have a significant impact on business continuity (more extensive damage, longer periods of service and data unavailability) (Cichonski et al. (2012)).

Detection and Analysis: Since incidents may differ between each other and can take place through various ways, there is no any standard step-by-step incident handling process. As such, every organisation must be prepared to handle and defence any incident in a different way. Different types of incident require different incident response strategies. Incident response team may be able to identify some particular attack vectors that indicate incidents that may occur. Some examples of common methods of attacks are external/removable media that refers to attacks that are executed from removable media or a peripheral devices, attrition that refers to attacks that employs brute force methods to compromise, degrade or destroy systems, networks or services, web that refers to attacks from the web or from web-applications, email attacks executed via email messages and attaches, impersonation attacks that involve replacement of something begin with something malicious, improper usage, loss or theft of equipment, etc.

From an organisation point of view, the most challenging part is the detection and assessment of potential incidents. This process is challenging because an incident may be detected in various means of a system or a network, with different levels of details and fidelity. Solutions that provide automated detection include network and host based IDPSs, antivirus software and log analysers. In addition, an incident may be detected through manual means, like issues report by users. Another indicator of an incident may be the high volume of alerts that coming from intrusion detection systems and sensors that facilitate this purpose. Finally, experience and specialisation of incident response team play a key role for an efficient incident analysis. Sign of an incident may be precursor, which means that this incident may take place in the future or indicator, which means that this incident may have occurred or it is in progress now. Examples of precursors incidents include web server log entries, which indicate the vulnerable scanner usage, an announcement of a new vulnerability exploit targeting a specified service of organisation, and threats that target an organisation. On the other hand, some examples of indicators may include antivirus software alerts after the detection of an incident, an intrusion detection sensor's alerts, identification of unusual changes of traffic flow by a network administrator, and so forth.

Some of the most common sources of precursors and indicators are IDPSs, SIEMs, Antivirus and antispam software, file integrity checking software, thirds-party monitoring services, and logs, such as network device logs, network flows, information on new vulnerabilities and exploits, people from within organisation, people from other organisations, etc.

Incident detection and analysis are two of the most critical stages, as precursors or indicators may not be accurate. Since several incidents may happen for various reasons, apart from a security breach, detection and analysis processes are challenging. On the other hand, the occurrence of an indicator may reveal a potential likelihood of an incident to take place in the future. In order for an incident to be determined as a security breach or a false positive case, collaboration with information security personnel and evaluation of current situation are essential for making a decision. Finally, incident prioritisation is fundamental for the success of adopted incident response plan, since the impact of various security breaches must be evaluated and served based on factors, such as functional impact of an incident, information impact, the impact over confidentiality, integrity and availability of information and recovery time (Cichonski et al. (2012)).

Containment, Eradication and Recovery: Containment is a critical stage of incident response plan in order to prevent the further damage to system. Containment stage provides the necessary time for developing the remediation strategy and take decisions regarding the management of an incident. Containment strategies are not standard and depend on the type of the incident. In addition, the criteria for defining containment strategies include potential damage and theft of organisation resources, need for evidence, service availability, time and resources needed to implement each strategy, effectiveness of strategy, and duration of applied solutions. Another important process during deployment of an incident response plan is the evidence gathering and handling. Data related to an incident may be available for facilitating various purposes, such as for resolving the incident. Another purpose of evidence gathering is the need for data for legal purposes, since digital evidence for an incident may be available, and go through a digital forensic investigation process. The preservation of digital evidence objects is critical and documentation must be available during all the stage of investigation, from collection to report stages.

Digital Forensic Chain of Custody is defined as the process that is followed in order for the chronological history of the handling of digital evidence objects to be maintained and documented, facilitating digital forensic investigation (Giova (2011)). The role of Chain of Custody is critical , since it preserves detailed records of all the stages of an investigation. In addition, information such as how the gathering of digital evidence took place, its analysis and preservation, who had access to it, when, where and how is maintained in CoC. On the other hand, CoC may be considered as susceptible to compromise, if the maintenance of documentation fails during specif or the whole lifecycle of a digital evidence, making it unacceptable in court of law as evidence of a cybercrime (Lone and Mir (2019)). The preservation of integrity of Chain of Custody is critical for a successful digital forensic investigation. Details of every digital evidence file must be preserved and include identifying information, such as location, serial number of a device, model number, media access control (MAC), details of every involved in the process member, time and date, and location of evidence storage.

Eradication is the next stage after containment, as it is necessary to eliminate components of an incident. This stage is related to deleting of malware, disabling breached user accounts, and mitigating identified vulnerabilities that have been exploited. It is an essential process as it is necessary all the affected and vulnerable hosts to be identified. For some incidents, eradication is not essential or is addresses during recovery stage. The recovery stage includes the re-storage of all the affected systems in order to return to normal operation, be functional and not vulnerable to prevent similar incidents. Recovery stage involves system re-storage from a clear backup, system rebuilding from scratch, replacement of compromised files, application of patches. Eradication and recovery stages should be done gradually for the remediation process to be prioritised. Recovery may take more time in case of a major severity incident. The stages aim to enhance the overall security in order to prevent future incidents (Cichonski et al. (2012)).

Post-Incident Activity: An essential outcome of this process includes the learning and improving. Incident response team should plan their defence enhancing and improving technology and systems. Furthermore, after an incident, security measures and incident handling process should be two of the major targets of incident response team. Furthermore, incident evidence should be kept for a time period, depending on the severity of it. Organisations should establish policies regarding the evidence retention, which usually takes months or years (Cichonski et al. (2012)).

8.3 Digital Forensics

During the last decade, the number of computer related crimes has increased with law enforcement authorities making use of computer and network- based evidence in order for questions like who, what, where, when, and how a crime has been conducted to be answered. As such, digital forensic investigation processes have evolved to ensure the acquisition, preservation and analysis of digital evidence up to the production of an expert witness report and presentation in a court of law. Forensic tools and techniques facilitate every stage of digital forensic investigation process from the investigation of the affected system, collection of related evidence, ensuring their integrity (the so called admissibility), analysing the evidence, in order to eventually answer the aforementioned questions. In addition, forensic tools

and techniques facilitate various types of tasks, such as operational troubleshooting, log monitoring, data recovery, data acquisition and due diligence/ regulatory compliance (Kent et al. (2006)).

A typical digital forensic investigation process involves four stages (Kent et al. (2006)):

- **Collection:** Collection is the first stage of a digital forensic investigation process and refers to the identification of potential evidence sources and the acquisition of data related to a security breach. The preservation of data integrity at this stage of digital forensic process is critical. As such the collection stage must comply with predefined guidelines and procedures related to data integrity preservation. Collection must take place almost immediately after an incident, since volatile evidence, like network connections, may be lost after a constrained period of time.

- **Examination:** Examination stage is related to the forensically processing of collected evidence. The goal of this stage is the extraction of related to an incident evidence by using manual or automated methods when the integrity of data is preserved.

- **Analysis:** Analysis stage refers to the stage where legally justifiable methods and techniques are used in order for the necessary questions to be answered.

- **Reporting:** The reporting stage is the final one of the digital forensic process and refers to the reporting of the analysis stage findings, providing all the details regarding the tools and techniques that have been used, how these tools and techniques have been chosen and why, all the actions need to be performed and recommendations for the improvement of future investigations.

It is important for every organisation to obtain experts who can perform computer and network forensics by using all the necessary tools and techniques. The primary roles of a digital forensics team include an investigator who is in charge of investigating into claims of misconduct, IT professionals, referring to technical support staff, and system, network and security administrator, and incident handler, who is responsible for responding to security breaches.

8.3.1 A brief description of the digital forensics process

As mentioned above, the first step of forensics process is the data collection. During this phase, it is necessary to identify the potential data sources and to extract the underlying data. There are many data sources, where the forensics process could start from. The most common and obvious data sources are desktop computers, servers, network storage devices, and laptops. These devices include internal drives that can support media, like CDs and DVDs, and maintain many kinds of ports that can support external data storage media, like external hard drives, USBs, optical disks, etc. In addition, many other computer-related devices such as smart phones, digital cameras and audio players that maintain data, can connect themselves to a computer as well. People who conduct the forensics investigation - both first responders and forensic analysts - should survey a physical area and recognise the possible data sources. Furthermore, they should be able to recognise data sources that may not be located in an office or in an organisation, but, they are external, such as logs of the network activity of another organisation or personal files of individual. In order to gain access to external data, a court order is required in many cases. Also, the

organisation's policies regarding the externally owned property organisation's facilities, like an employee's personal laptop, should be taken into consideration, when a forensics process is about to start. In any case, forensics analysts should be ready to search for alternative data sources. Some helpful actions adopted by organisations for forensics process could be the implementation of centralised logging, the auditing and keeping records for certain events, regular backups of systems performing, frequent security and privacy controls monitoring, users' behaviour monitoring, etc. After identifying the data sources, the next step is to acquire that data from those sources. Data acquisition follows three steps, namely the data acquisition plan, the (actual) data acquisition, and the integrity verification of the data that has been acquired. The first step of this process, the data acquisition plan, is a critical and challenging step due to the potentially large number of possible data sources. The prioritisation of data sources is the first action that should take place establishing the order in which data will be acquired. Analysts should keep some prioritising factors in mind such as the likely forensic and evidential value a data source may have based on the experience of that analyst, the volatility of the data referring to the data of a live system that my be lost after the former shut down been lost, and amount of effort required to acquire various data sources. It does not only depend on the time that the acquisition will take, but the cost and the equipment that it will need. Taking these three factors into consideration, the acquisition of data can start. Acquisition phase includes the usage of forensic tools to collect volatile data, duplicate non-volatile data sources and secure the original non-volatile data sources. Data acquisition will be performed locally over the network. Local acquisition is preferable, without being always feasible. In the case of acquiring data from a network, decisions should be made regarding the type of data to be collected and the amount of effort to use. The next step following data acquisition is the integrity verification of data. This process typically consists of using verification tools to compute the message digest of the original and copied data, then comparing the digests to make sure that they are the same. It is important for analysts to keep records and log each stage of the forensics process, the tools that have been used, the data sources even for those that are not considered as important (Kent et al. (2006)).

The second step of forensics process is the examination phase. As the data has been collected, it must be examined in order to extract and store only the relevant information. Also, this stage of the whole process may involve bypassing or mitigating OS or application of data obfuscation techniques such as encryption or elaborate encoding. In order for this process to be faster and easier, there exist techniques that are used to reduce the amount of data for examination, the so-called triage. Text and pattern searches can be used to identify data that are related to the evidence and can help the investigation. Another technique is the labelling of each data file regarding its content (Kent et al. (2006)).

The third part of forensics process is analysis, where the extracted information from the previous step should be studied and analysed in order to get a conclusion from it. The forensics foundation is using a methodical approach for reaching appropriate conclusions based on the available data or for determining that no conclusion can yet be drawn. Analysis should include people, places, items and events, and of course information regarding the relationships between each other in order to reach a conclusion. Analysis may include data correlation among various sources. Furthermore, there are many tools, like centralised logging and security event management software that can facilitate the correlation process automatically (Kent et al. (2006)).

The final stage of the forensics process is reporting, where the preparation and

the presentation of the results from the analysis process take place. An important consideration is that the digital evidence may be subject to different interpretations as due to the uncertainty surrounding the investigation the digital information describing an incident may not be sufficient or complete. Consequently this may lead to offering more than one explanation about what happened in the case under question. In such case, the expert should use a systematic approach to prove or disprove each possible explanation that is proposed. The audience to which the analysis will be presented is also an important consideration as the audience may have limited understanding of technology which is often the case in a court.

It is important to note that during a digital forensic investigation, the maintenance of Chain of Custody during the documentation is essential for preserving and demonstrating the integrity of the acquired digital evidence. In addition, regardless the methodology that is followed in order for a digital forensic investigation to be addressed, the actions undertaken by investigators are underpinned by the Association of Chief Police Officers and ACPO Good Practice Guide for Digital Forensics report Williams (2012). The ACPO guide provides instructions to investigators regarding the collection, analysis and presentation of digital evidence.

8.3.2 Digital Forensic Readiness (DFR)

Digital Forensic Readiness involves a group of processes dealing with organisational setup, providing the ability to maximise the potential digital evidence usage whilst minimising the time and cost in the case of a digital forensics investigation. This class of processes is optional to the digital investigation processes since it is the prerogative of the organization to implement it rather than the task of the investigator(s).

According to ISO/IEC 27043:2015, four readiness process groups are included: planning process group, implementation process group, assessment process group and concurrent process group (Figure 8.1) (ISO/IEC27043 (2015)):

- Planning Processes Group is defined by ISO/IEC 27043, as the pre-incident planning activities, such as collection, storage, analysis and presentation of digital evidence and how they will be conducted. In particular, planning activities include:
  - definition of scenario process
  - potential digital evidence sources identification process
  - planning of the pre-incident evidence gathering process
  - storage and handling of data representing potential digital evidence process
  - planning pre-incident analysis of data representing potential digital evidence process
  - incident detection planning process
  - defining system architecture process

  This process group defines also actions to be taken when an incident is detected. In addition, the planning process group ensures the identification of the legal and business-specific requirements and their consideration into the Digital Forensic Readiness Framework.
- Implementation Processes Group implements the processes that have been identified during the Planning Process, and include installation of systems and

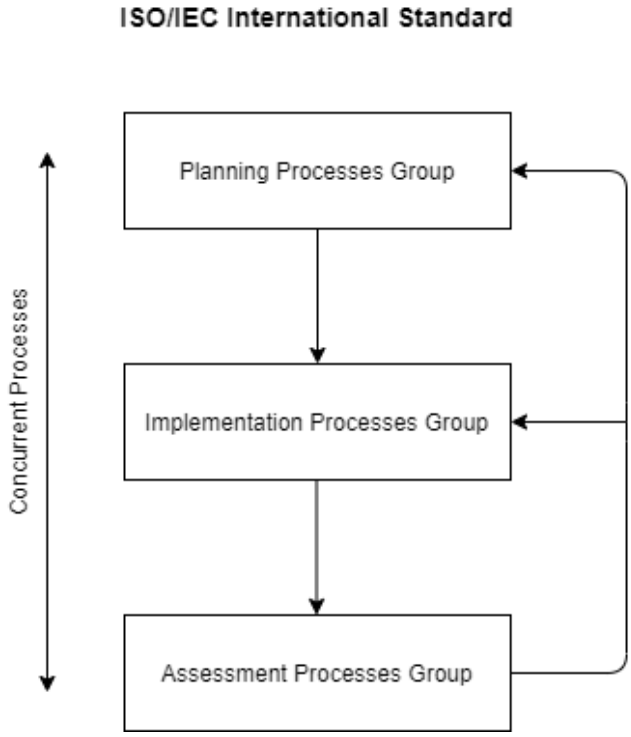

FIGURE 8.1: Readiness Processes Groups ISO/IEC27043 (2015)

policies that enable the collection of digital evidence before an incident occurs. Systems and policies may include incident logging, storage and change tracking software and hardware across the organisation.

- Assessment Processes Group consists of activities which evaluate the results of the Implementation Process Group activities, and compares them with an organisation objectives for achieving regarding Digital Forensic Readiness. The results are used to improve the DFR process.
- Concurrent Processes include activities that take place alongside digital investigation processes. As such, these processes are applied during a digital forensic investigation. For instance, the need for preserving the integrity of the Chain of Custody and eventually the digital evidence is present during all the stages of a digital investigation, let alone when digital evidence is handled by different parties and authorities.

Figures 8.2, 8.3, and 8.4 present all the digital forensic readiness groups along with their processes.

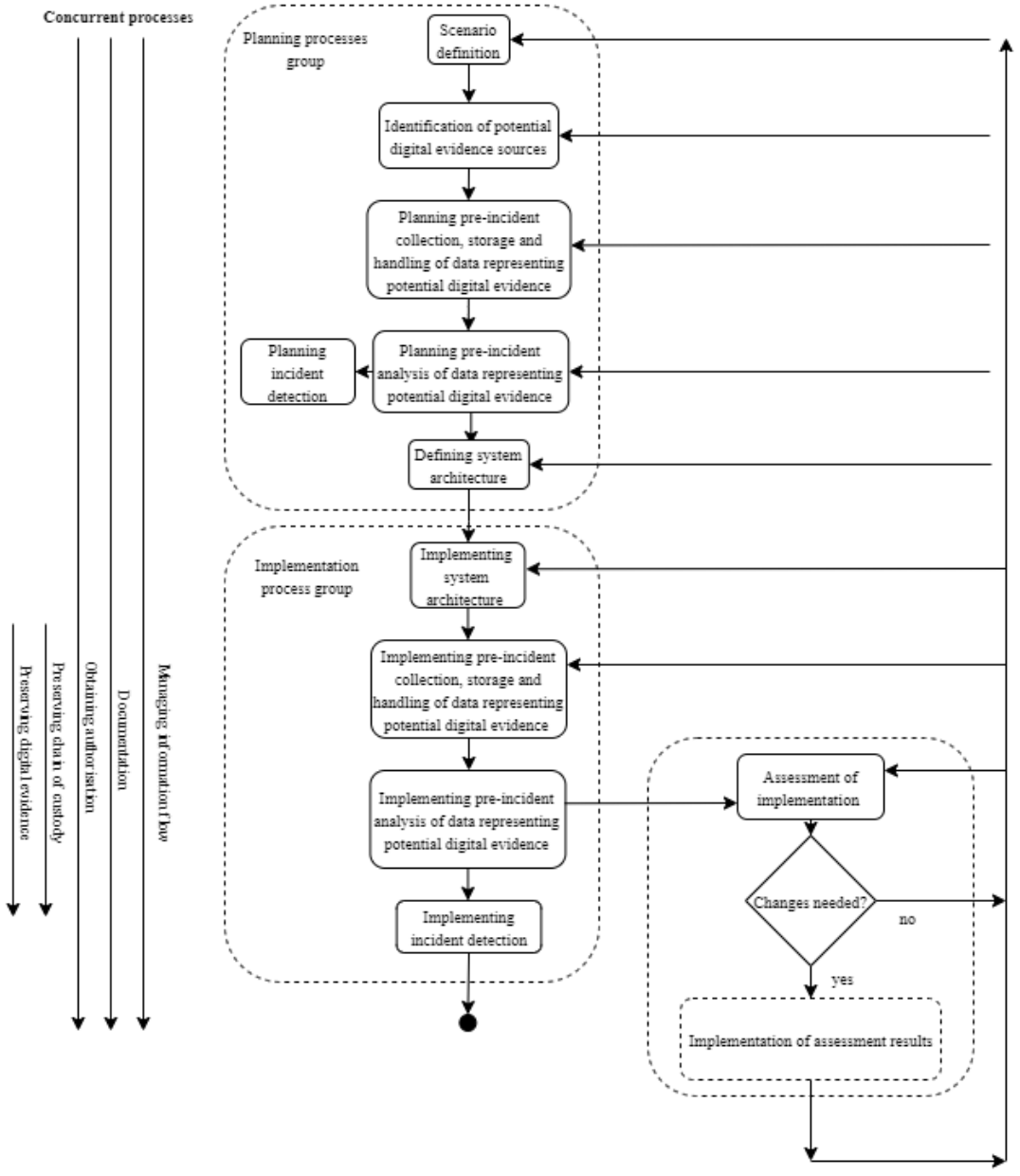

FIGURE 8.2: Readiness Processes- Planning and Implementation processes groups (adapted from ISO/IEC-27043 (2015))

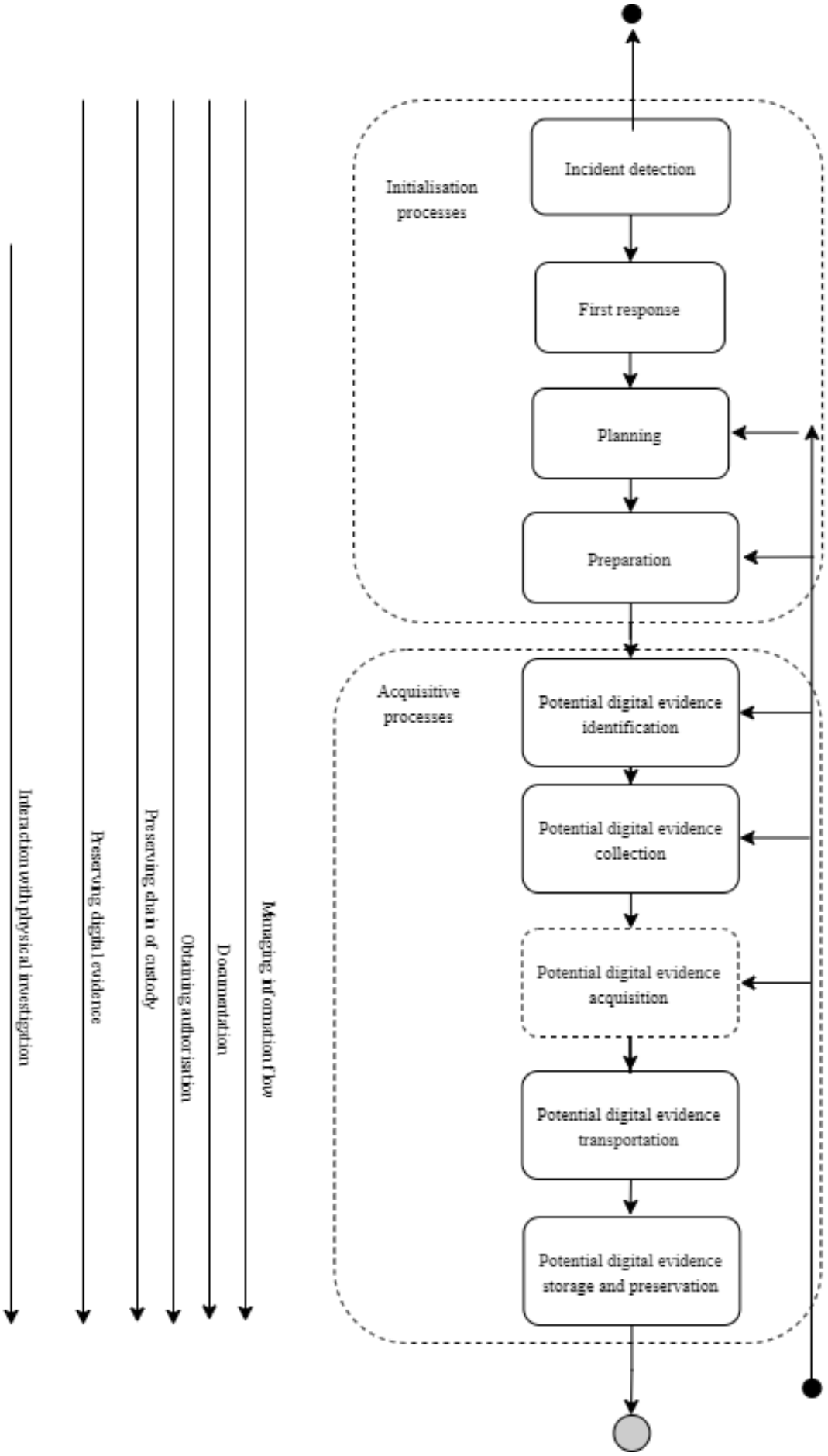

FIGURE 8.3: Readiness Processes-Initialisation and Acquisitive processes groups (adapted from ISO/IEC-27043 (2015))

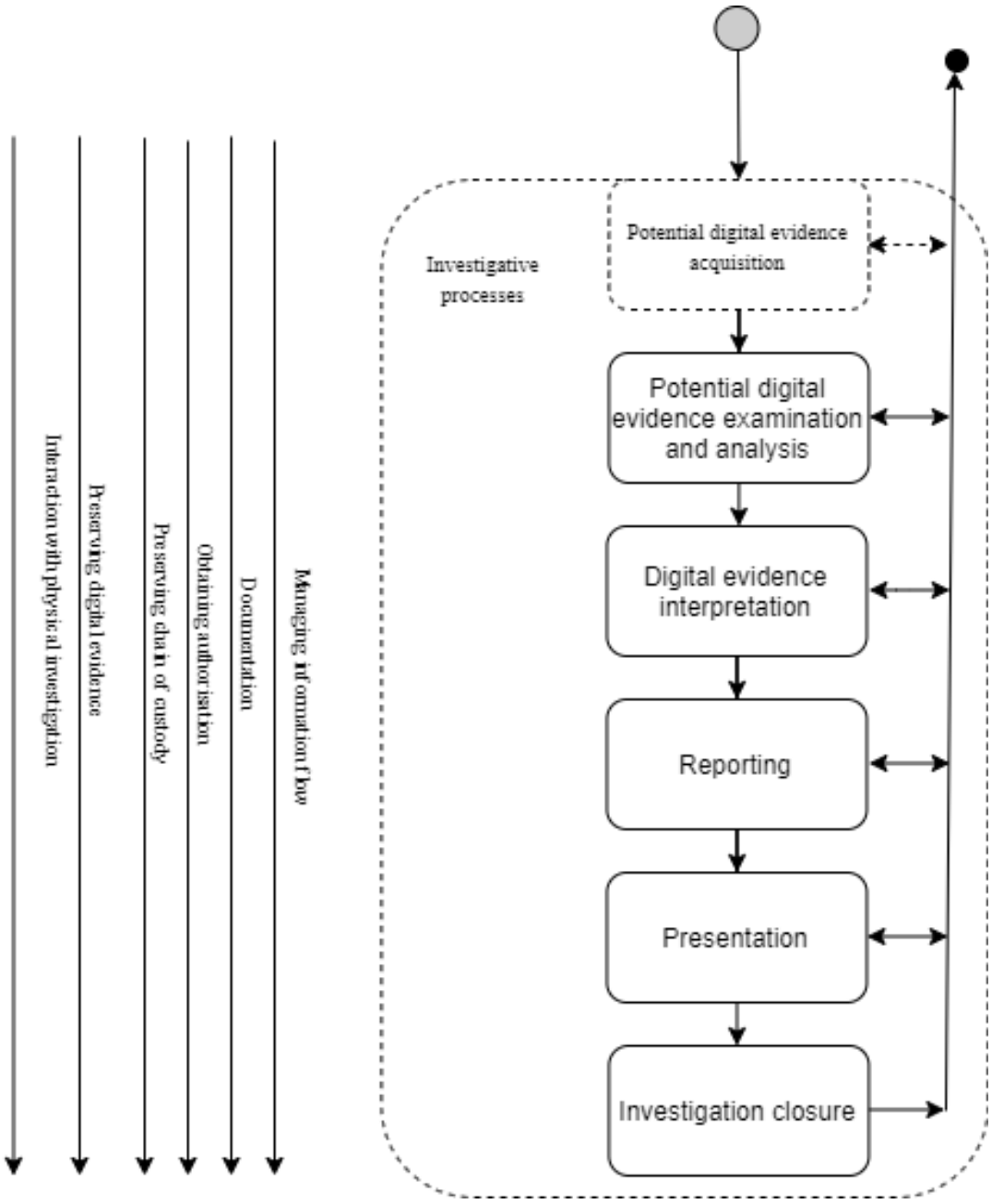

FIGURE 8.4: Readiness Processes- Investigative processes group (adapted from ISO/IEC-27043 (2015))

8.3.3 Discussion

The adoption of technological enablers in urban environments and the transition from traditional to smart cities create opportunities for improving the quality of services that are provided to citizens. The application of these enablers are consolidated to the generation of interdependent systems that generate and share data between their components, facilitating different tasks and improving the functionalities and connectivity of modern Information and Communication Technologies. Furthermore, the adoption of information and communication technologies by urban environments places interdependent systems across two interacting dimensions, the cyber-physical and the socio-technical. The coexistence of both dimensions of systems in the same environment enables the generation of useful data, facilitation of various services and cooperation of different stakeholders. Although this interconnectivity provides helpful aspects for urban environments and provides opportunities for the development of collaborations between authorities, stakeholders and other urban environments, it comes along with risks since vulnerabilities in both systems may potentially increase the probability of exploitation and overall (and potentially critical) infrastructure failure. From one point of view, these applications can become a fertile ground for revolutionary ideas, improvement of smart cities services and provision to every citizen. On the other hand, they introduce challenges that should be taken into consideration in advance.

In addition, interconnectivity raises several complex issues related to forensic investigations apart from the increase of cybersecurity challenges landscape. One of the main issues with digital forensics investigations in smart cities is users' data storage location. There are multiple users' data storage locations within a smart city. As such, custodians must go through various infrastructure environments (and sometimes through different jurisdictions) to gain access to these pieces of data. Furthermore, the employment of devices on a massive scale, their ability to be connected to public, private and organisational networks, and their constrained memory capacity which force them to store data on the Cloud, increase the number of digital evidence sources that forensic custodians should take into considerations, let alone the privacy issues raised (Baig et al. (2017)). According to Oriwoh et al. (2013), future digital forensics investigations issues include the expansion and heterogeneity of digital evidence sources. The number of devices, the data type that is not limited to standardised file format, the quantity and type of data, and the location of evidence. The heterogeneity of a smart city, where various technological enablers are involved, such as IoT, SDN and NFV, Cloud and Edge Computing, Blockchain, and so forth, and the fact that there are no standardised digital forensic investigation techniques for some of them, like IoT and Cloud Computing, increases the need and business case for developing, maintaining and adopting a digital forensic readiness framework.

Another challenge relating to the wider incident response capabilities of a city is that different sectors, environments, systems and even data governance realms may follow their own incident response plans and processes. It is fairly obvious that when the underlying systems are interconnected, the validity and appropriateness of the compartmentalised - and maybe in some cases conflicting - incident response processes may cause more problems than offering solutions. It is advocated in this research that different realms may maintain their own incident response plans, but at the same time agree and follow a commonly accepted digital forensics framework. In essence, each systems may have different security standards and needs, but should a interconnected system is attacked, the evidence will need to be collected,

processed and analysed in a standard and systematic and compliant manner. In an ideal setting, alignment of incident response processes is a desirable state and there is considerable literature in cyber threat intelligence and information sharing that attempts to address these issues. However, in a less-ideal and resource restrained world, the solution will need to be efficient and practical. This paves the need to finding a less perfect yet practical solution. It is therefore argued that a good starting point in a common incident response plan would be to have a digital forensics readiness framework.

The move towards a digital forensics readiness framework for a smart city unsurprisingly comes with a number of challenges. The interconnectivity and the heterogeneity of cyber-physical and socio-technical systems does not make the management and process of data an easy task. Consequently, the reluctance in data sharing and management due to established security and privacy practices, hinder the effectiveness of digital forensics investigations. Furthermore, in many cases, due to the heterogeneity of smart cities environments and subsystems, there are gaps concerning the legislation, the management and governance of data by authorities and in terms of smart cities the restrictions and local policies set by the council. In addition, form a digital forensics and evidence admissibility perspective, the collection, management, and exchange of data within a smart city, introduces challenges on the integrity of the evidence.

Despite the wealth of research describing established models for preserving integrity, identification and adoption of known and accepted models may not be appropriate. For instance, the Clark-Wilson integrity model provides a foundation for specifying and analysing an integrity policy for a computing system. This integrity model defines data items of a computing system and applies integrity policies. The model focuses on separation of duties and well-formed transaction (integrity) and addresses three integrity goals, authentication and authorisation, prevention of making improper changes by both authorised and unauthorised users, and maintenance of transaction consistency. The implementation of the Clark-Wilson integrity model could be considered as a solution in a smart city use case, regarding the maintenance of data records that can assure security, privacy, and digital forensic readiness aspects. Yet, the need for demonstrating and preserving the Chain of Custody (CoC) regarding digital evidence management and analysis is essential for computing systems and for the environment where they are embedded. In addition, transparency in every stage of data processing and digital evidence must be taken into consideration. Analysis of data and digital evidence must be performed based on enforcement rules for records to be kept about the actions that have been taken over, the alterations, the access rights that have been assigned to various authorities, the maintenance of this evidence and answers to questions, such as who has access, to which data, when and why. Furthermore, due to its non-tangible nature, digital evidence is considered volatile. Therefore, it should be protected and its integrity should be maintained during all steps of a digital forensics investigation process. Furthermore, integrity should be kept during all stages of a digital forensic readiness framework as well. Thus, it is essential for computing systems to come up with a solution, implementing one or more technologies that can facilitate the integrity of digital evidence and the Chain of Custody. Blockchain may be considered as a technological enabler that can be adopted to address the challenges regarding the preservation of Chain of Custody and the protection of digital evidence until it fulfils its final purpose, the presentation to a court of law. In general, Blockchain based solutions are employed to address challenges and deal with transparency, integrity, trust and accountability issues. In addition, the security of the data sharing process

is fundamental, especially in digital forensics investigations, since it is essential for data to not be modified while passing from one stage of the investigation to another and from one authority to another. Blockchain may be considered as the technological enabler that can be used to certify the authenticity of digital evidence in all stages of an investigation and assure that the final presentation to a court of law will be legitimate. Also, it can provide useful details regarding data in depth within the Chain of Custody.

8.3.4 Validation of Blockchain feasibility for digital forensic readiness framework

In what follows, it is assessed whether Blockchain technologies can be incorporated in a digital forensic readiness framework for smart, circular cities, by employing the feasibility methodology by Wüst and Gervais (2017) summarised by the following questions:

- Q1 Is there any requirement of storing the state?
- Q2 Do we have multiple writers in the system?
- Q3 Can we afford to have trusted third party (TTP) online always?
- Q4 Are all writers in the system known?
- Q5 Are all writers in the system trusted?
- Q6 Is there any requirement of public verification?

Taking these questions into consideration, the answer to Q1 is yes, because digital evidence passes through various levels of hierarchy during the digital forensic readiness and investigation process, after an incident. The answer to Q2 is yes, because in a smart city environment there is a big number of stakeholders and authorities. In addition, crowdsourced approaches are adopted in smart and responsive city use cases. The answer to Q3 is no, because there is a need for a decentralised, crowdsourced solution. The answer to Q4 is yes, because only known and authorised parties can have access to and analyse digital evidence. The answer to Q5 is no, because decentralised trust is necessary. Finally, the answer to Q6 depends on the need for public verification. By applying these answers on the flow diagram depicted in Figure 8.5, we arrive at the recommendation to adopt a private, permissioned Blockchain network.

8.3.5 Assets Identification and Digital Forensic Readiness Framework

As discussed above, according to ISO/IEC 27043:2015, a digital forensic readiness framework aims to maximise of the potential use of digital evidence, by minimising the cost of digital investigations and interference with and the prevention of interruption of the organisation processes. Therefore there are specified steps that should be followed for a digital forensic readiness framework to be applied and achieved.

The first step for developing an efficient digital forensic readiness framework is to consider the operational environment. This would specify the required inputs consisting of the system architecture, adopted technological enablers, hardware and software, policies, and procedures.

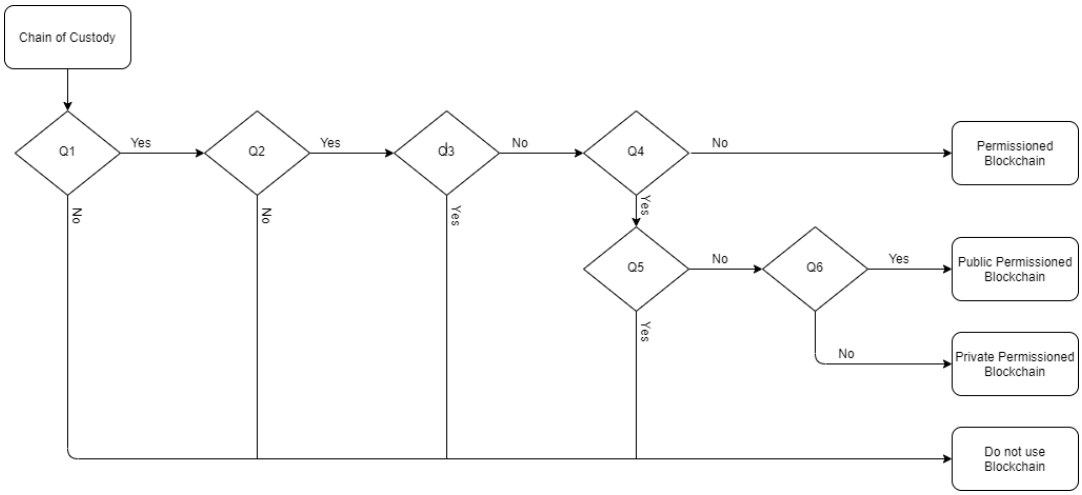

FIGURE 8.5: Is Blockchain an appropriate technical solution for solving an issue? (Lone and Mir (2019); Wüst and Gervais (2017))

As already discussed, smart cities environments consist of several technologies, people-citizens, stakeholders, law enforcement authorities and councils who cooperate to provide a better living experience and improved services to citizens and visitors. Especially, all the technological enablers that are employed within a smart city environment provide the smartness level that each smart city project aims to achieve. These technological enablers can be considered as the digital infrastructure of a smart city. The digital infrastructure obtains two dimensions, the physical and the cyber, since it involves actual assets, devices, such as sensors, cameras, smart devices, and non-physical assets, such as 5G, Cloud Computing and Blockchain. In addition, data generated by smart cities digital infrastructures are considered as assets as well. As such, adopted digital forensic readiness frameworks by smart cities concepts may use the data themselves as input in order to increase their efficiency. Furthermore, additional information regarding the data assets are considered as valuable for the operation and performance of a digital forensic readiness framework. This information involves data owners' identity, and of course metadata such as access rights details, type of data, location and service criticality level.

Also, the forensic level preservation of this information is important, since integrity, immutability, privacy and non-repudiation should be addressed.

For digital forensic readiness purposes, it is advocated that the information related to assets should be preserved through the employment of Blockchain. As it has been elaborated already, Blockchain technologies provide security and privacy features by design, preserving the integrity, transparency, traceability, immutability, and non-repudiation of information and data. In the digital forensic readiness framework, data is essential for the creation, maintenance, and update of the Chain of Custody that includes digital evidence for future digital forensic investigations to be facilitated with less cost and within less time. Moreover, the adoption of Blockchain for improving the digital forensics readiness metrics would be subject to the preceding discovery and analysis of vulnerability and risk profiles of every asset within the smart city ecosystem. In essence, this risk-driven approach on the level of implementation of a Blockchain solution would be aligned with the potential impact of vulnerabilities that may be exploited and having direct consequences to the smart city as a whole. In addition, in the case of cyber-physical systems, the identification of devices that produce and provide metadata and log files that can be used as digital

evidence is essential, since collection of data should be conducted adopting various and unambiguous techniques, such as taking snapshots of data frequently. In order for data related information to be preserved, DLTs can be employed, for keeping records of details regarding the kind of data, stakeholders and owner or owners, criticality level, data storage location, characteristics, date and hour of activation, ability to be taken offline and generation of log files of a smart city ecosystem asset. It is reminded that in critical infrastructure components availability is considered to be the highest priority security goal of the three (confidentiality, integrity, availability). The (non-forensic, pre-incident) acquisition process can provide future investigators with valuable information regarding the assets of a smart city and with essential digital evidence that have been preemptively collected and stored in order to be used during the post-incident phase. The purpose of this digital evidence collection is to minimise the time and cost of a future digital forensic investigation, to maximise the digital evidence volume that may be available to custodians and investigators after an incident and its usage, to preserve the business continuity of services and infrastructures, and to streamline security and privacy within a smart city. Also, IoT systems come with additional constraints with regards to digital forensics investigations, apart from vulnerabilities and risks, thus new approaches compliance with standards (such as ISO/IEC 27043) are essential. In addition, a heterogeneous system that includes various stakeholders, authorities and technological enablers should not adopt centralised techniques for the preservation of Chain of Custody and integrity of digital evidence as this would be impractical. For all the stakeholders and authorities to be compliant and facilitate the investigation, the digital forensic readiness approach should be crowdsourced. This approach may be considered as beneficial for the collection and maintenance of digital evidence by all the participants of a smart city environment. Moreover, the creation and application of a policy scheme, such as GDPR legislation, for addressing the digital forensic readiness framework will improve the services that it can provide. In GDPR, policies are followed to protect personal data. In the case of the digital forensic readiness framework, a policy and legislation scheme can be applied for authorities, which have to follow specific steps and processes to identify, collect and preserve digital evidence for future digital forensics investigations. In addition, general legislation for digital forensic readiness framework can provide the necessary processes that have been followed by local authorities, data owners, and custodians, in order for all the available evidence to be available for facilitating an investigation, in a more efficient time and cost manner.

8.4 Non Fungible Token (NFT)

The term fungible refers to everything that is transferable. Cryptocurrencies can be considered as fungible tokens, since each one is identical to another and they have the same value. On the other hand, the term non fungible term is used to describe a token that obtains a unique identifier and value. As such, non fungible tokens are not identical between each other and do not have the same value (Chevet (2018)). Some of the basic properties of NFTs include the uniqueness of each token, the ownership only by one and the easy verification of ownership, and the inability to be manipulated in any way (Ethereum-Org (*Non-fungible tokens (NFT)*)). ERC-20 is the first token standard that supports fungible tokens only and it is adopted by Ethereum. Since this standard does not support non fungible tokens, there was need for a new token standard. Thus, ERC-721 tokens standard that supports non

fungible tokens has been adopted. NFTs are attached to digital objects using metadata to help off-chain rendering or storage. Even ERC-721 supports NFTs, it does not support multiple tokens in a single, smart contract. In order for these limitations to be addressed, Ethereum introduced ERC-1155. ERC-1155 supports both ERC-20 and ERC-721 features.

8.4.1 Ethereum

Ethereum is an open source Distributed Ledger Technology platform, publicly available to developers for creating DLT applications. Ethereum provides decentralised, virtual resources that are available to developers for executing scripts based on a worldwide client network, allowing nodes to create and execute smart contracts. Ethereum nodes are provided with tokens, called "ether", which facilitates the online payments and the verification of transaction process (Damianou (2017); Ethdocs (2016)).

How Ethereum network works A list of verified transactions are stored in digital lists, called ledgers. Copies of ledger of the network are available to all the nodes and updated after the verification of a new transaction. Ethereum network is based on user accounts. An account includes four features:

- A nonce, a counter to make sure that a transaction will be processed only once.
- The account current ether balance.
- The account's contract code.
- The account's storage, which is empty by default.

Ethereum accounts are divided into two categorises, the externally owned accounts that refer to accounts that are controlled by the generated private keys of node owners and the contract accounts that refer to the accounts that are controlled through the execution of a smart contract (Ethdocs (2016); Buterin (2014)).

For transactions to be verified and executed through an Ethereum network, transaction fees have to be paid. The fees requirements of the network protects it from perfunctory and malicious users. Fees are paid in ether and they are controlled by network "miners", who are responsible for the verification of transactions and the generation of new blocks. Every miner is rewarded with ether tokens after the verification of transactions. As Bitcoin, Ethereum uses Proof of Work consensus mechanism. Miners have to deal with complex mathematical problems for a block to be mined (Ethdocs (2016); Buterin (2014)).

8.4.2 EOS

EOS is a Distributed Ledger Technology platform provided to users for developing decentralised applications (dAPPs) and smart contracts, as an alternative solution to scalability issues found in popular Blockchain networks, such as Etehreum and Bitcoin platforms. EOS implements delegated Proof-of-Stake consensus mechanisms and allows parallel processing and full-duplex communication in order for high transactional throughput to be achieved through decentralised applications. Regarding developers claims, the range of processing capabilities of EOS are around 5,000 to 1,000,000 transaction per second. It should be taken into consideration that there is currently no comprehensive analysis for determining the capabilities of the

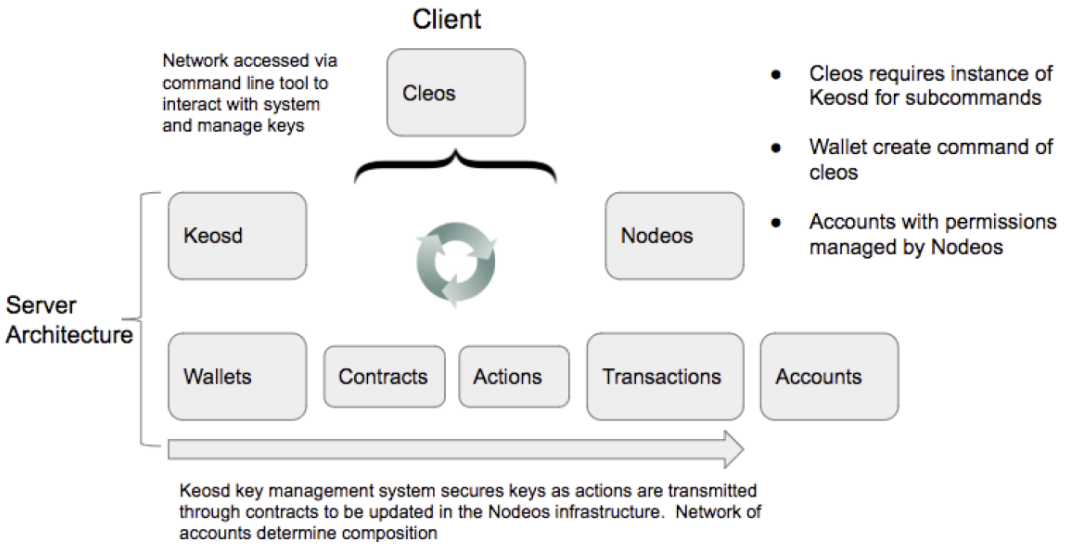

FIGURE 8.6: Overview of EOS System Architecture (Xu et al. (2018))

network and such performance has not been achieved in a production network (Xu et al. (2018)).

EOS includes the EOS token, which is the cryptocurrency token of the network, and EOS.IO, which is described as the operation system that controls the Blockchain network. Both play a key role, since EOS token allows users to develop and run decentralised applications on the EOS network and EOS.IO provides the resources for the development of these applications. In addition, EOS consists of three components that include Nodeos, Cleos and Keosd.

- Nodeos is the core service that runs on every node of EOS network. It plays an important role for configuring and processing smart contracts, validating transactions, generating new block of the chain with valid transactions and ensuring the validity of records of the Blockchain (EOS (2018b)).
- Cleos is a Command Line Interface (CLI) tool through which users can access EOS network. The interaction and the configuration of interactions with the overall EOS network through Nodeos are allowed by using Cleos tool (EOS (2018b)).
- Keosd is a component of the network that runs locally and it is designed to store private keys of nodes that are used for signing transactions. Users can use and retrieve their private keys through Keosd RCP application (EOS (2018a)).

Smart Contracts

As has been already discussed, smart contracts technology was first introduced in 1994 and it has gained popularity due to its application over Ethereum Blockchain system. The term smart refers to a group of software functions that are stored in a distributed ledger and executed when a new Blockchain transaction triggers them. Smart contacts software functions are executed inside distributed ledger. In other words, the execution of these software functions takes place in real time by all the Blockchain network nodes, based on the consensus rules that have been deployed, applied, and agreed by all the participants. In general, smart contacts may be considered as digital, legal agreements between two or more parties, in order for digital

assets to be protected. More than one smart contracts can be preserved by Blockchain networks, based on the users/ nodes requirements. One of the main advantages of smart contracts include the coexistence of different rules for multiple users-parties (GSMA (2018)).

8.4.3 EOS vs Ethereum: The Comparison

Ethereum is an established Blockchain system along with Bitcoin. In addition, Ethereum is the first Blockchain system that supports the development and support of smart contracts. Although Ethereum has gained popularity, there are some issues that have been identified by users, developers and research community. On the other hand, EOS is a new Blockchain platform that supports the development of smart contracts and works as an alternative to Ethereum platform, with its creators claiming that EOS can address Ethereum issues, without the scalability goals having actually been achieved.

Scalability

Regarding scalability, both Blockchain systems include challenges that need to be addressed. According to developers of EOS, network can process around 5,000 to 10,000 transactions per second because of inter-communication, a feature that it obtains, which handles more transactions. On the other hand, Ethereum can process fifteen transactions per second, which makes it inefficient to compete with established payment systems, like Visa which processes thousands of transactions per second (Xu et al. (2018); Sharma (2019)).

Transaction Cost

There is a different transaction cost approach between EOS and Ethereum. EOS is based on an ownership model, where users are the owners of resources necessary for platform operations and include CPU, RAM and network bandwidth. This ownership model does not oblige users to pay rent on EOS system for having access to these resources, making it to be considered as decentralised operating system rather than a decentralised computer, where access is required in order to develop and run Blockchain applications. EOS accounts, which facilitate the creation of EOS applications, are assigned to users for determinate time, terminating their ownership after three years of not using them. Furthermore, transactions validation fees are not required in the case of EOS systems (Xu et al. (2018)).

On the other hand, Ethereum is based on a rental resource mechanism, where every transaction within the network carries fees that must be paid by a user. These fees are paid in Ether coin and are used as fuel for verifying and completing transactions, as well as for ensuring security within the network. Ether coins that Ethereum system gains from the verification of transactions are used as "Gas", as fuel for the execution of smart contracts and maintenance purposes (Sharma (2019)).

Consensus Mechanism

Another difference between EOS and Ethereum is related to the consensus mechanisms that both systems use. Ethereum uses Proof of Work (PoW) consensus mechanism, which is used by Bitcoin as well. On the other hand, EOS system uses Delegated Proof-of-Stake.

Proof of Work introduced in *"Bitcoin: A peer-to-peer electronic cash system"* (Nakamoto and Bitcoin (2008)) as a prevention mechanism against double-spending attacks in Bitcoin network. PoW Blockchain networks demand from the responsible nodes of the network for transaction verification, the so-called miners, to perform complex computations in order for the validity of network entities to be assured. In Bitcoin, the transaction validation process includes the solving of a cryptographic challenge. The new block is added to the chain after the solution of cryptographic challenge by the winning node (Belchior et al. (2020)). PoW is performed under the premise that the network is consistent, and only the cumulative computing power of honest nodes is greater than the attacker's computing power (Chaudhry and Yousaf (2018)). Proof of Work is a consensus mechanism that is used by two of the most famous Blockchain networks and cryptocurrencies, Bitcoin and Ethereum. On the other hand, PoW consumes enormous amount of energy. For instance, Bitcoin PoW mechanism consumes around 1129.89 kwh per transaction. This amount of energy is equivalent to the power consumption of a household in the U.S. for 38.73 days (Digiconomist (2021)).

Delegated Proof of Stake (DPoS) works similarly to PoS, giving priority to nodes that have deposit more stakes than others. The major difference between PoS and DPoS is that in the latter nodes elect a specific number of other nodes as representatives to generate and validate new blocks. Because of the smaller numbers of nodes that take part to the consensus process, the time consumption for generating and validating a new block is significantly lower. On the other hand, the constrained number of nodes makes networks more centralised. Furthermore, the parameters of network, such as block size and block interval can be adjusted. If some of the elected nodes do not work properly and honestly, the rest of the network nodes can vote against and elect new representatives (Yang et al. (2019)). In contrast to PoW, DPoS is more energy efficient. One of the main drawbacks of DPoS is the fact that the consensus process is not able to prevent unethical nodes to be elected. Thus, these nodes can generate blocks over a long time, raising security risks to the network. The elected block validators are those which demand the major energy consumption. EOS, being currently the most popular Blockchain token that uses DPoS, is estimates to have an energy consumption at 1.8 kW per block and annual energy at 0.0012 TWh (Pagliari (2019)).

For the needs of this research, dNFT schemes provided by EOS DLT platform is employed. dNFT schemes will provide distributed ownership of digital and physical evidence objects and it is used as unique identifier of each of the objects. dNFT schemes facilitate the distribution of ownership and rights, in percentage (Singh (2019)). The adoption of dNFTs facilitates the digital forensic readiness framework by providing the uniqueness of each evidence object and by improving their identification and their transmission from local storage of each sector provider to digital forensic custodians during the post-incident phase. The way that dNFTs are generated are as follows. A dNFT token and the underlying ledger may offer transparency across the board and across all digital forensics processes, right from the creation of the token and its assignment to the evidence object to the ownership and transfer (custodian) history.

8.5 Proxy Re-encryption(PRE)

Proxy re-encryption (PRE) is a cryptosystem scheme, that allows to a third party - namely a proxy - to re-encrypt a ciphertext in order for a receiver to be able to

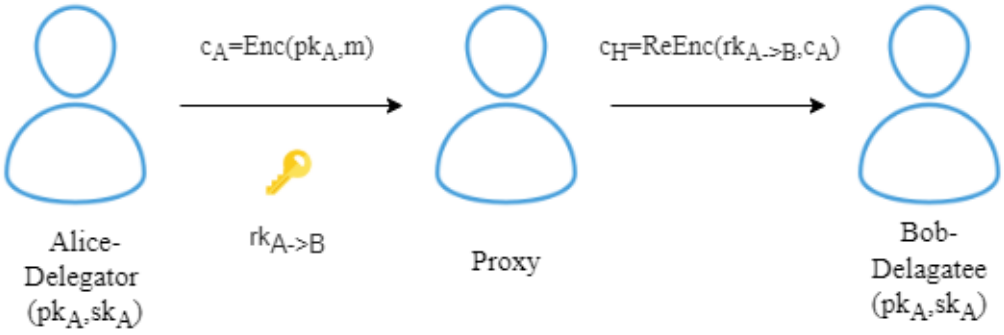

FIGURE 8.7: Main entities and interactions in PRE, (adapted by (Nuñez, Agudo, and Lopez (2017)))

decrypt it using his/her private key. Proxy re-encryption may be considered as a means for the delegation of decryption rights (Nuñez, Agudo, and Lopez (2017)).

The main concept of a proxy re-encryption scheme involves the transformation of ciphertexts by a proxy, making a delegatee able to decrypt them using his/her private key. In addition, the proxy is not able to learn any information about the ciphertexts. The proxy re-encryption scheme is presented in 8.7. Proxy re-encryption involves three entities, the delegator, the delegatee, and the proxy.

- **Delegator**: This entity delegates his/her decryption rights adopting the proxy re-encryption. For delegating his/her decryption rights, he/she creates a re-encryption key and he/she transmits it to the proxy. We refer to delegator as "Alice".
- **Delegatee**: This entity obtains a delegated right to decrypt ciphertexts that are re-encrypted with a re-encryption key that delegator creates and transmits to proxy.
- **Proxy**: This entity proceeds with the re-encryption process. Proxy receives ciphertext and re-encryption key from delegator. Proxy re-encrypts the ciphertext with the re-encryption key and transfers the new ciphertext to delegatee, Bob, without gaining additional information over it.

In order to adopt the PRE scheme, all the parties need to be assigned with a pair of secret and public keys. The PRE scheme includes two types of functions, key generation functions, and functions that manage ciphertexts and messages. There are two key generation functions, *KeyGen*, that generates the pairs of private and public keys, and *ReKeyGen*, that generates the re-encryption key, and three functions that deal with ciphertexts and messages, *Enc, ReEnc*, and *Dec*, where Enc encrypts the message, *ReEnc* re-encrypts the first ciphertext, and *Dec* decrypts the second ciphertext (Nuñez, Agudo, and Lopez (2017)).

- $KeyGen(n) \rightarrow (pk_A, sk_A)$. As input takes security parameter n, and outputs a pair of private and public keys (pk_A, sk_A) for Alice.
- $ReKeyGen(pk_A, sk_A, pk_B, sk_B) \longrightarrow rk_{A \rightarrow B}$. Private and public keys of Alice and Bob are the input of this function, and re-encryption key $rk_{A \rightarrow B}$ is the output.

- $Enc(pk_A, m) \rightarrow C_A$: Alice public key pk_A and message m are the input of this function, and ciphertext c_A is the output.
- $ReEnc(rk_{A\rightarrow B}) \rightarrow c_B$. Re-encryption key $rk_{A\rightarrow B}$ and ciphertext c_A are the input of *ReEnc* function and ciphertext c_B is the output of re-encrypting c_A using $rk_{A\rightarrow B}$ or the error symbol $\perp$ indicating that c_A is invalid.
- $Dec(sk_B, c_B) \rightarrow m$. Secret key sk_B and c_B are the input of *Dec* function, having as output the initial message m or an error symbol $\perp$ indicating c_B is invalid (Nuñez, Agudo, and Lopez (2017)).

8.6 Digital Forensic Readiness Framework for Smart Circular Cities

In this section all the necessary terms related to the introduced DFRP are introduced.

8.6.1 Digital Forensic Readiness Playbook (DFRP)

In this work, the term *playbook* refers to a synopsis of steps related to incident response processes, which is based on a set of rules, describing the options to execute with input data and the criticality of the situation. A playbook provides orchestrated actions, based on the NIST incident response lifecycle to security analysts in order to confront digital and physical evidence objects, in a simplified and automated way. Responsible authorities can use a playbook in order to evaluate costs and risks and plan future actions. Apart from the traditional incident response playbook approach that addresses cyber risks, attention has also to be given on the physical/control layer (Patzer, Meshram, and Heß (2019); Williams-Shaw (2019)).

8.6.2 Digital Evidence Object

The term *digital evidence object* is used to describe a self-contained artifact or a set of artifacts that meet all the requirements in order to facilitate a digital forensic investigation, the outcome of which may be presented to the court of law as an admissible crime evidence. These artifacts include digital data, such as files, hard disks, network traffic, memory captures, and so forth (Carrier and Spafford (2004)). In terms of their requirements, digital evidence objects must offer integrity, accountability, a unique identifier, provenance and be atomic. Digital evidence objects obtain specified and unique features based on their creator and their purpose. Integrity of digital evidence objects is essential for a digital forensics investigation in order for the artifacts to be considered as legitimate (Carrier and Spafford (2004)).

8.6.3 Core and Extended Teams and Roles

Computer Security Incident Response Teams are the main incident response teams and are designed to develop and implement incident response capabilities against threats and vulnerabilities while trying to reduce the impact of an incident and inform security community by conducting reports, providing guidelines and procedures for secure configurations and in-depth protection. The coordination of CSIRTs and Computer Emergency Response Teams contribute to the maximisation of digital, physical and critical infrastructures of city. Before an incident and after the employment of CSIRT and CERT teams from organisations, agencies and a city's local

authority, roles within the teams should be defined. Defining roles within CSIRT and CERT teams is critical for incident management and effective/immediate response during an incident. In addition, the pre-incident phase and the identification of exposure and risks of city is a critical process that must be done relying on staff with expertise. CSIRT includes various roles that facilitate the operations of the team and the incident response plan, such as CSIRT Team Manager, Legal Expert, Communication and Public Relations Specialist, Network Administrator, Physical Security and Facilities Manager and Disaster Manager, as presented below (Cichonski et al. (2012)):

- **CSIRT/CERT Team Manager** has the authority for recruiting of staff of team and takes important decisions for preserving sustainability of organisation (smart city infrastructure for the needs of this research) by identifying threats and incidents and communicating them with the executive staff;
- **Communication and Public Relations Specialist** is responsible for the public relations, informing the media after an incident. This role requires a person with high communication and diplomatic skills, who can handle employees, partners and customers after a major incident. In addition, social media monitoring is part of Communication and Public Relations Specialist duties;
- **Legal Experts** are responsible for the monitoring of the incident response plans and ensuring their compliance with law and federal guidance, especially the privacy right;
- **Physical Security and Facilities Manager** are responsible for investigating asset security incidents occur through physical breaches. Especially, in smart city case, where cyber-physical systems are fundamental part of city's infrastructures, compromising physical assets may affect cyber assets and business continuity of provided services;
- **Network Administrator** is responsible for ensuring the security of network topology and plays an important role to the development of incident response plan of a smart city. In addition, since various cyber security attracts try to exploit network infrastructures in order to damage further a city, Network Administrator keeps a determinant role. Network Administrator is part of the IT technical experts team, along with IoT Solutions Architect (Homeland Security (2019));
- **IoT Solutions Architect** along with Network administrator, works under the IT technical experts team and provides all the necessary information, such as "where", "how" and "when" IoT devices should be placed within a smart city;He has the understanding of the technological enablers that a smart city obtains and facilitates the coordination of IoT engineers and local authorities, such as council.

The smart city's administration should comprise of hired employees who serve as an upper management team of specialists, knowledge advisers, and consultants, as well as the personnel who have been elected at the local, municipal, and governmental levels. During an incident, the escalation is hierarchical, with hired officials passing information on to a city manager selected by the local council. The latter is in charge of managing all information received from the contracted team and disseminate it to the local borough for further investigation. In an event of a high-impact incident, a CSIRT manager or city manager should be given the authority

to interact directly with the city mayor or their close team, escalate the situation to a national level from a municipal level. This escalation may continue, in case of a major incident, until it approaches the highest escalation level, depending on the governmental structure of the country where the city is located.

A city-level CSIRT managed by local authorities and coordinating with other CSIRTs can improve the risk profile of a city and control the vulnerability exposure. Also, CSIRTs managed by local authorities of a city could evaluate the vulnerability exposure, create the exposure profile of a city, manage and prevent the expansion of vulnerability exploitation, protect critical infrastructures, and cooperate with other peer CSIRTs, through an operational cooperation structure. At the time of writing, there appear to be no local authority CSIRTs with a city wide constituency, but instead there are operators of essential services, such as healthcare, transportation, energy, and so forth. In addition, these operators are employed by only a few countries in Europe, (by four countries, including Austria, Czech Republic, Italy, and Latvia, see ENISA's CSIRT interactive map) [1] . Also, these operators of essential services are managed by the national CSIRTs of these countries, and not by local authorities of a city.

In addition, governments start to embrace and adopt vulnerability management projects for facilitating the disclosure of vulnerable devices, employed by the public and private sector. The most recent example is the UK government that announced the release of Nmap scripts in order to facilitate system administrators to reveal unpatched or vulnerable devices. The project called *Scanning Made Easy (SME)*, will be managed by the UK Cyber Security Centre (NCSC) and Industry 100 (i100), a collaboration between the NCSC and the UK private sector (Cimpanu (2022)).

Even if national CSIRTs could handle a cyber incident, a need remains for local authorities to be involved and be part of the incident response actions that will be taken during (local) vulnerability exploitation. This involvement can be partial or complete and local authorities should be able to assign duties to individual operators that handle specified essential services of a city. Since there are Cyber-Physical Systems within a city environment, and the inter-connectivity allows all the city parties to cooperate and communicate with each other, a successful exploit may potentially affect not only a particular sector but, the whole infrastructure. In a case of a physical attack, both cyber and physical infrastructures may be affected and unable to serve the citizens. As such, there is a need for direct intervention, which may not be able to be provided by any other operator, apart from a local one. Since vulnerabilities management is critical for cities, and especially for those that have integrated a massive number of devices and technological enablers to address the needs of citizens and visitors, the adoption of incident response teams is crucial. Moreover, since cities may be considered as, governed initially by local authorities, such as a council, the vulnerability management approach should be determined by these authorities. The involvement of local authorities is critical, for the vulnerability severity and vulnerability exposure of a city to be managed and decreased from the outset. As such, the creation or the employment of an incident response team that will handle a cybersecurity breach within an urban environment, especially within a Responsive city, lies in local authorities management decisions, based on various factors, such as applied business plans and financial feasibility. In addition, various governance-incident response plans may be adapted to the needs of a city local authorities regarding the management of vulnerabilities and vulnerability exposure.

[1] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

Each local authority should be flexible to make decisions in light of the city's technological integration and risk profile, keeping in mind the severity that vulnerability exploitation may cause to infrastructures and citizens.

Against the above, the adoption of incident response and vulnerability management solutions rely on local authorities commitment and engagement. In addition, for cities with high vulnerability exposure and constrained resources, such as financial and lack of human capital managing digital infrastructures, local authorities should be involved in cybersecurity investments and decision making.

For instance, if essential services of a city are managed and monitored by an incident response team that works independently from local authorities, it may be able to establish a cooperation structure and an information-sharing scheme to be involved in vulnerability management. Cooperation structures and information sharing among critical infrastructure CSIRTs and local authorities, must be established. Whereas a city, and especially a Smart or a Responsive city integrates a massive number of devices and assets in general, as well as a variety of systems, such as Cyber-Physical and Socio-Technical Systems that interact with each other, it is obvious that cooperative approaches can be more efficient to maintain an register of assets and attempt to gather intelligence on related threats and vulnerabilities that may eventually affect city services and business continuity. Centralised approaches regarding the management of cybersecurity issues within a city may not be efficient, because of the heterogeneity of these environments. On the other hand, the cooperation of many operators, such as different CERTs, and the information sharing between them, could support crowdsourcing service models. The advantages of this approach include immediate actions taken by CERTs of particular services and city sectors, detection of cybersecurity breaches and analysis, actions for faster recovery and protection of infrastructures of this particular service, assurance of business continuity of service, protection from exploitation of more sectors, and finally, information sharing for the purpose of effective vulnerability management and reporting activities related to the incident.

Cooperation and communication should not be limited only to CSIRTs with local authorities, but among all operators of essential services. The information sharing and communication between operators of essential services may prevent further damage from vulnerability exploitation and protect citizens' safety and business continuity of a city.

To summarise, decisions related to vulnerability management are made by local authorities in agreement with the crowdsourced approach, which involves operators of services, essential and non-essential, of a city, employed CERTs, etc. The establishment of cybersecurity activities within local governance is essential. Decision making of local authorities regarding the vulnerability management of a smart or a responsive city relies on the needs of each city and its risk profile. In addition, local authorities are responsible for the coordination and information sharing between operators of services for a city to be completely protected from all the kinds of threats, such as physical, cyber-physical, hybrid, etc.

Through this research a number of findings (see Chapter 7) showed the dependencies between the vulnerability management needs of a city and the maturity level it belongs to. A particular interest is shown for the highest maturity level - the responsive city - which enjoys a high degree of integration and therefore the highest levels or risk.

8.6.4 Smart City Critical Sectors and Infrastructures

The term infrastructure is used to describe all the public and private facilities that may be considered as essential for enabling public services and economic development. Two main categories of infrastructures have been identified, the technical infrastructures, which facilitate services like transportation, energy and water, and the social infrastructures providing to services like education and healthcare (Rome et al. (2015)).

According to the National Cyber Security Centre and CNI Hub, UK, a critical infrastructure is defined as *"the critical elements of Infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life."* (Maddinson and Petterson (2020)).

The identification of critical infrastructures is not a straightforward process, since it relies on a variety of scientific concepts (Fekete (2011)). One of the main criteria that studies use in order for an infrastructure to be identified as critical is the impact and the consequences that their failure state may cause.

In addition, interconnectivity of infrastructures may indicate their criticality, as their failure may lead to so-called cascading effect, affecting all the other connected to them infrastructures (Rinaldi, Peerenboom, and Kelly (2001)). Interconnectivity and failure of infrastructures are important especially in case of Critical Information Infrastructures (CII), which refer to interconnected networks and information systems the failure of which has serious impact on other infrastructures, such as healthcare, safety, and telecommunication.

There is a variety of interdependencies between infrastructures based on specified characteristics and effects. The four main categories of interdependencies include physical, cyber, geographic, and, logical. In Figure 8.8, examples of interdependencies between critical infrastructures are presented. Taking into consideration the maturity level that a city has achieved, it should be mentioned that interdependencies among critical infrastructures may be increased as the maturity level increases. For instance, in an instrumented city, the interdependencies between critical sectors-infrastructures may be less than in a responsive city, where everything is in a complete sync.

Some of the critical infrastructures according to CISA (2020) and Maddinson and Petterson (2020) are presented below:

Energy Sector

The energy sector is fundamental for a city since it is responsible for the production and delivery of energy, primarily electricity and gas for powering and enabling services and needs of a city environment. These services and needs include distributed assets, physical and digital, traffic furniture infrastructures, households powering, municipality-owned utilities, healthcare infrastructures, and so forth.

The reliance on the energy sector and the lack of it within a city concept may damage other critical sectors, such as healthcare, water and waste management since all the enabled sensors and actuators require energy for operating purposes. The energy sector must be well aware of risks and vulnerabilities that may affect the business continuity of its services by managing and addressing potential challenges. Industry collaboration plays a key role in the information sharing of best practices across the sector. Many owners and operators of the energy sector are

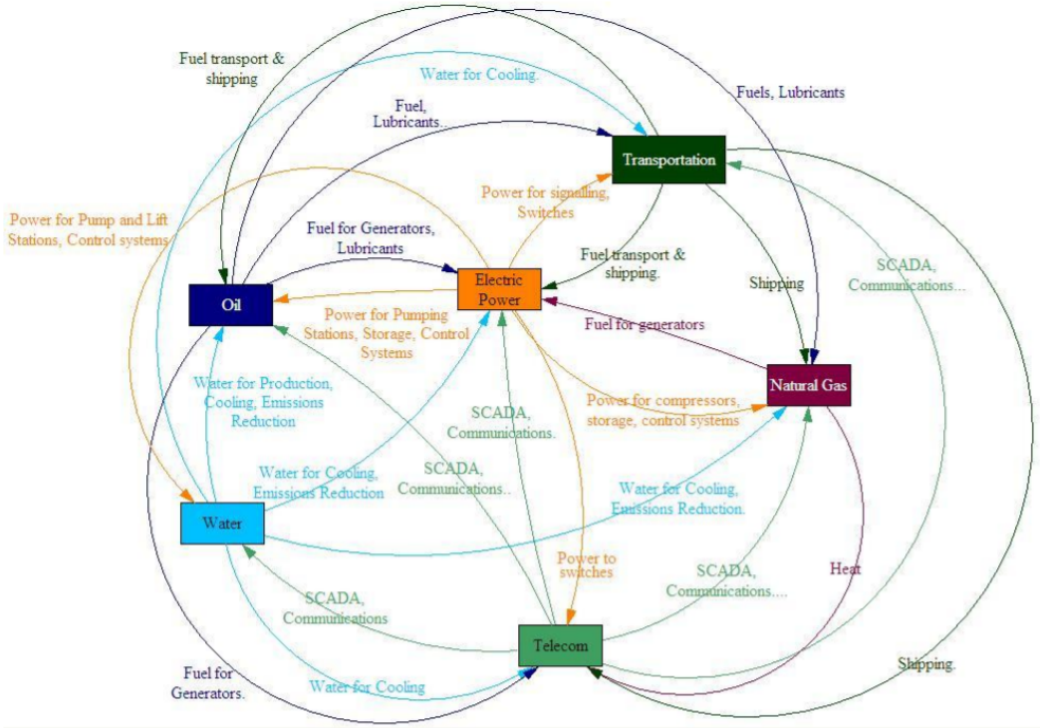

FIGURE 8.8: Interdependencies between critical infrastructures (Guthrie and Konaris (2012))

experts regarding infrastructure protection and they have turned their attention to cybersecurity during the last decades (CISA (2020)); (Frazer (2018)).

Water and Wastewater

Water and Wastewater infrastructures are another critical sector of a city since they are responsible for the collection, distribution, metering and reclamation of water resources. Especially in the case of massive urban environments, the access to clear water and the maintenance of a properly treated wastewater system are vital for the public health, the protection of public safety from diseases and the preservation and protection of the environment. Thus, the supply of drinking water and the maintenance of wastewater systems are essential for modern urban ecosystems.

It should be mentioned that the water supply and wastewater systems sectors may be considered as exposed to a variety of cyber-attacks that can affect their performance and the public health. These attacks include contamination of drinking water with deadly agents, physical attacks and cyber attacks. The effects of these attacks can be devastating to public health, causing serious illnesses, and financial damages. In addition, water and wastewater systems are vulnerable to natural disasters. Also, other critical dependent and interdependent sectors of a city may be affected by compromising water and wastewater systems, such as healthcare and energy (CISA (2020)); (Frazer (2018)).

Waste Management

Waste management sector is responsible for the collection and handle of waste materials. The waste management sector include waste management strategy, waste

prevention, waste collection, waste re-use, waste treatment and material recycling, energy recovery and waste disposal (CISA (2020)).

Communications

Communications sector refers to the underlying enablers that facilitate interactions among businesses, public safety organisations, citizens and government, in both physical and digital way. There are five areas of communications that involve telecommunications, the Internet, broadcast, media, and space (Maddinson and Petterson (2020)). According to the Presidential Policy Directive 21, communications is critical, since it provides communication among all the critical infrastructures (Press Secretary (2013)).

Healthcare

Healthcare and Public Health sector is fundamental for a city and addresses and protects the public safety from disease outbreaks and serious illnesses. This sector is divided into private and public operators, with the majority of healthcare assets, belong to private ones. As such the information sharing between private and public sector is enhanced for the resilience of the general sector to be increased. The role of the healthcare sector is vital in response and recovery across all other sectors, triggered by a natural or man-made disaster. Various levels of public health management include local, regional, and national, aiming for providing healthcare services to the majority of the population.

Attacking and tampering with the healthcare sector components may be catastrophic for the citizens' health. Attacks that affect the sector include physical, cyber and hybrid. Attacks can have serious consequences to the public safety and affect many other sectors of a city, due to the interdependence among sectors. Healthcare specialists tend to adopt techniques and technologies for identifying potential risks and vulnerabilities and addressing challenges that may have a great impact on sector infrastructures, public safety and city (CISA (2020)).

Transportation and Mobility

Transportation systems are useful and fundamental for a city. As the population of cities around the world increases rapidly, the need and demand for more efficient and more convenient transport means are mandatory. The transportation sector, within the realm of a city, refers to authorities that manage roads, streets, bike lanes, walking paths, vehicles, public transport, air and maritime ports, and so forth.

A city includes many types of transportation means and huge transportation networks that tend to expand. Cities have changed processes for accessing transportation systems, facilitating citizens and visitors. Electronic tickets and usage of contactless payment cards and smartphones, embedded telematics systems in buses and underground stations, sharing economy applications, such as Uber and Gett have contributed to the improvement of the transportation capacity of a city. Furthermore, various cities have adjusted intelligent transportation systems that are placed over modern vehicles to manage the traffic problems on the roads. These intelligent transportation systems are network platforms that support communication channels established among vehicles. Vehicles exchange information between each other through the established communication channels among vehicles and infrastructures.

The integration of technological paradigms, such as IoT, which enables the communication between embedded sensors and actuators for improving transportation services may come along with risks that affect the performance of the sector. The exploitation of vulnerabilities that the system obtains puts public safety in danger and because of the dependence and interdependence with other sectors, their operation is in danger as well.

Public Safety

The public safety sector refers to the infrastructures, agencies and personnel that preserve the safety of city human assets. The public safety sector includes first responders from the police, fire and emergency medical services, facilitates a wide range of prevention, preparedness, response and recovery services during ordinary activities and unexpected events. The main goal of the public safety sector is the protection of citizens' lives and properties, the protection of the environment, provision of aid to impacted by a disaster citizens and recovery aid during an emergency (CISA (2020)); (Frazer (2018)).

Financial Services

The financial services sector preserves is a fundamental sector within a city and includes banking systems, providers of investment products, insurance companies, credit and financing organisations, and the critical financial utilities and services that support these functions. Potential risks this sector may be damaged by include large-scale power outages, natural disasters and sophisticated cyberattacks (CISA (2020)).

Within the realm of a city environment, payments obtain a core role regarding the economic activities that include economic transactions, such as salaries, consumer spending, and taxes. In addition, economic transaction within a city refer to provided services, such as parking services. Finally, services may provided to citizens and visitors of a city by the municipality under a subscription scheme (Frazer (2018)).

8.6.5 Digital Forensic Readiness Playbook (DFRP) for Smart Circular Cities

The main purpose of introducing the playbook is to initiate and indicate a set of rules and a roadmap that should be followed by authorities in order to be considered as digitally forensic ready. The playbook adoption provides all the necessary actions that should be taken from local authorities, service providers, and stakeholders in order for digital evidence objects to be ready for a future digital forensics investigation, after the occurrence of an incident. All the stages of the adoption and preparation for the digital forensic readiness framework should be followed by all the participants of a city in order for consistency, facilitating information and collaboration sharing between CSIRTs and local authorities. The proposed DFRP is part of the digital forensic readiness framework, introduced in this research for the needs of smart cities, taking into consideration the maturity level that each city has achieved.

Various researches have highlighted the need for *forensic-by-design* principles integration within building and evolving systems (Ab Rahman et al. (2016)), and have introduces novel frameworks and models focusing on particular systems and services that should be considered as *forensically ready*.

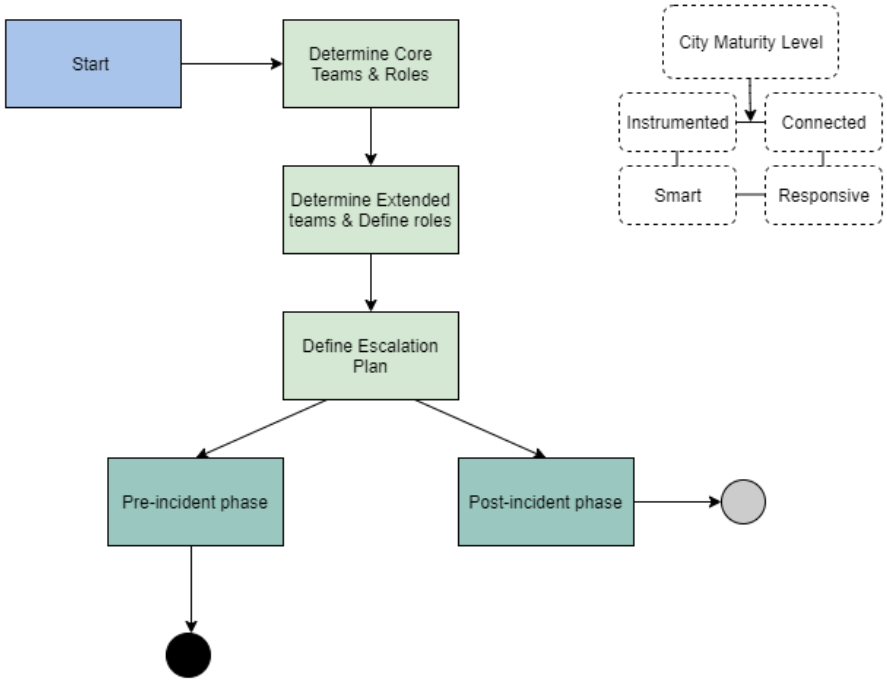

FIGURE 8.9: Identification and preparation of digital forensic readiness roles

In (Philomin et al. (2020)), authors identify the vulnerability exposure landscape of IoT devices and how their exploitation may affect the whole system, in their case a smart home, and they introduce a digital forensic readiness framework as a mechanism to reinforce integrated security in smart homes, by describing the collection of digital evidence process, which allows proactive forensics. This framework complies with the ISO/IEC 27043 standard.

Furthermore, in Kebande and Ray (2016), authors propose a generic Digital Forensic Investigation Framework for IoT (DFIF-IoT) that complies with ISO/IEC 27043 standard, and obtains three modules, the proactive processes, the IoT forensics, and the reactive processes. On the other hand, this research does not address the organisational level processes as an important part of the proposed DFRF across an organisation.

Also, in Ngobeni, Venter, and Burke (2010), authors focus on wireless network traffic and describe a wireless digital forensic readiness model. The model monitors and preserves the network traffic and maintains it for future investigation. It should be mentioned that the model does not take into consideration organisational and security processes.

In addition, there are several researches that have adopted Blockchain technologies for facilitating digital forensic readiness approaches and the integrity preservation of the Chain of Custody.

In Cebe et al. (2018), authors focus on connected vehicles, in particular on the on-board sensors, IoT devices and subsystems, and they introduce an integrated lightweight blockchain framework for forensic applications. The proposed framework is based on the application of a permissioned blockchain network that allows to the participants to communicate and exchange information on-board. In addition,

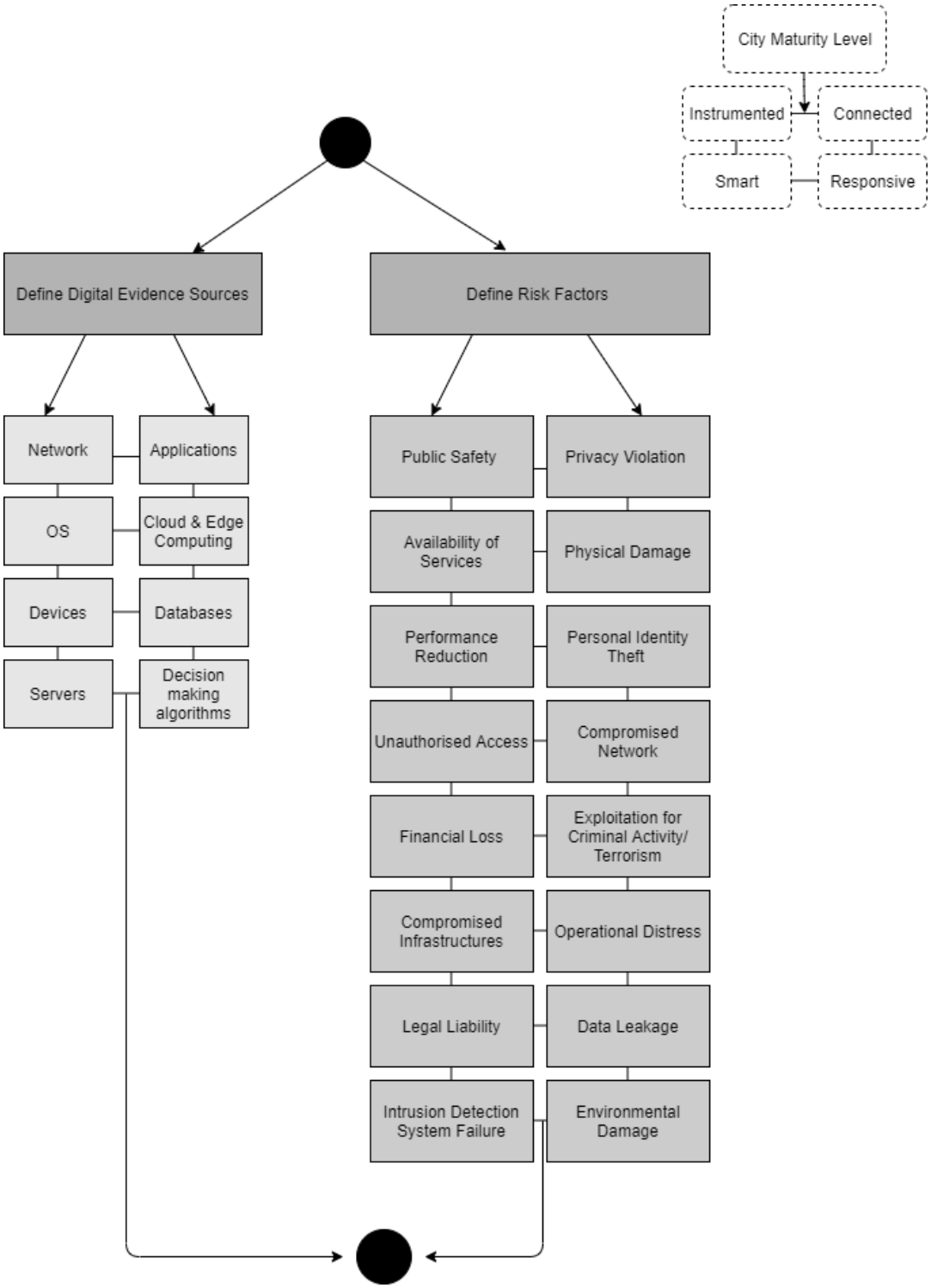

FIGURE 8.10: Definition of digital evidence sources & risk factors

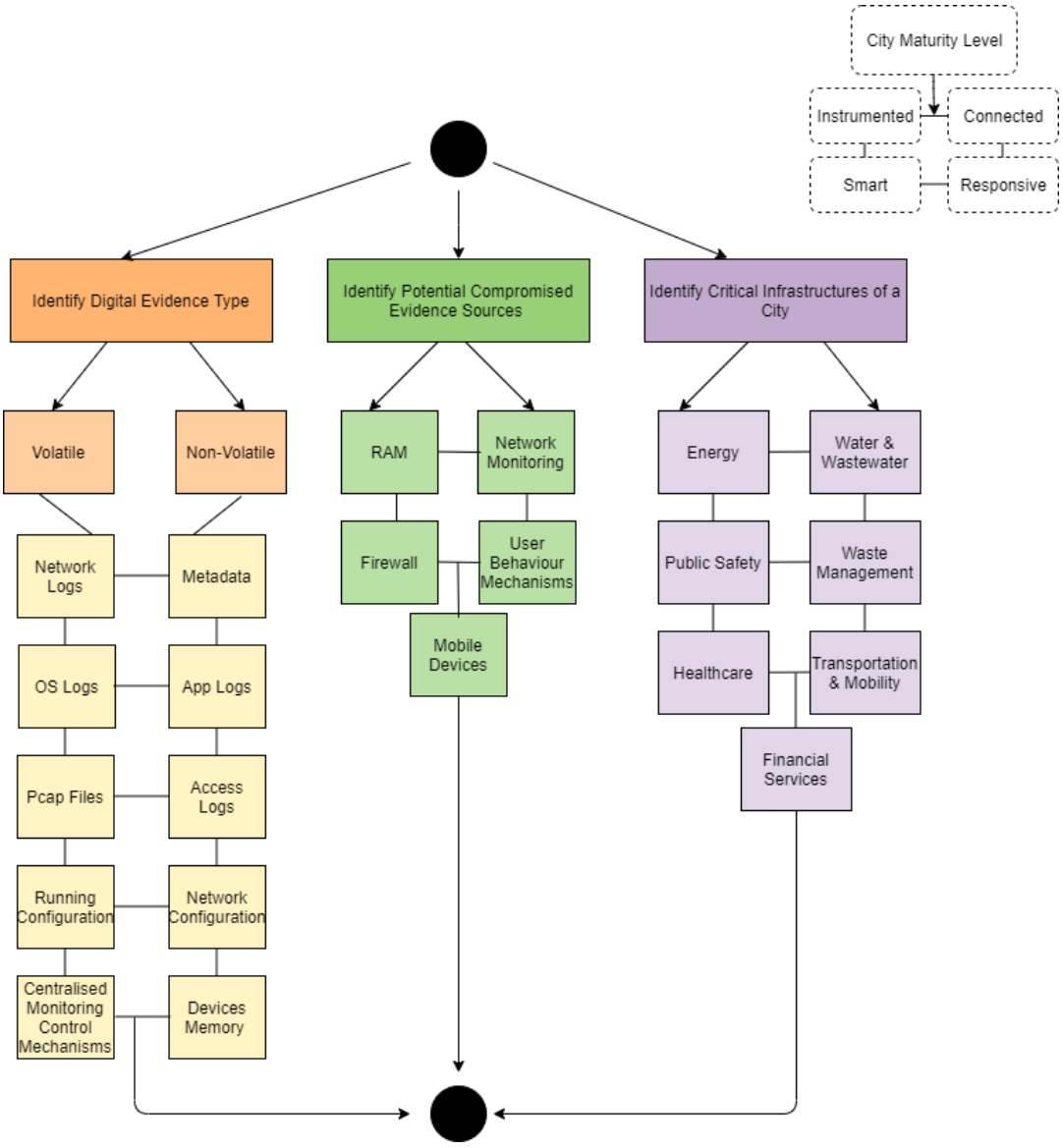

FIGURE 8.11: Definition of digital evidence type, potential compromised evidence sources, critical city sectors, & maturity level

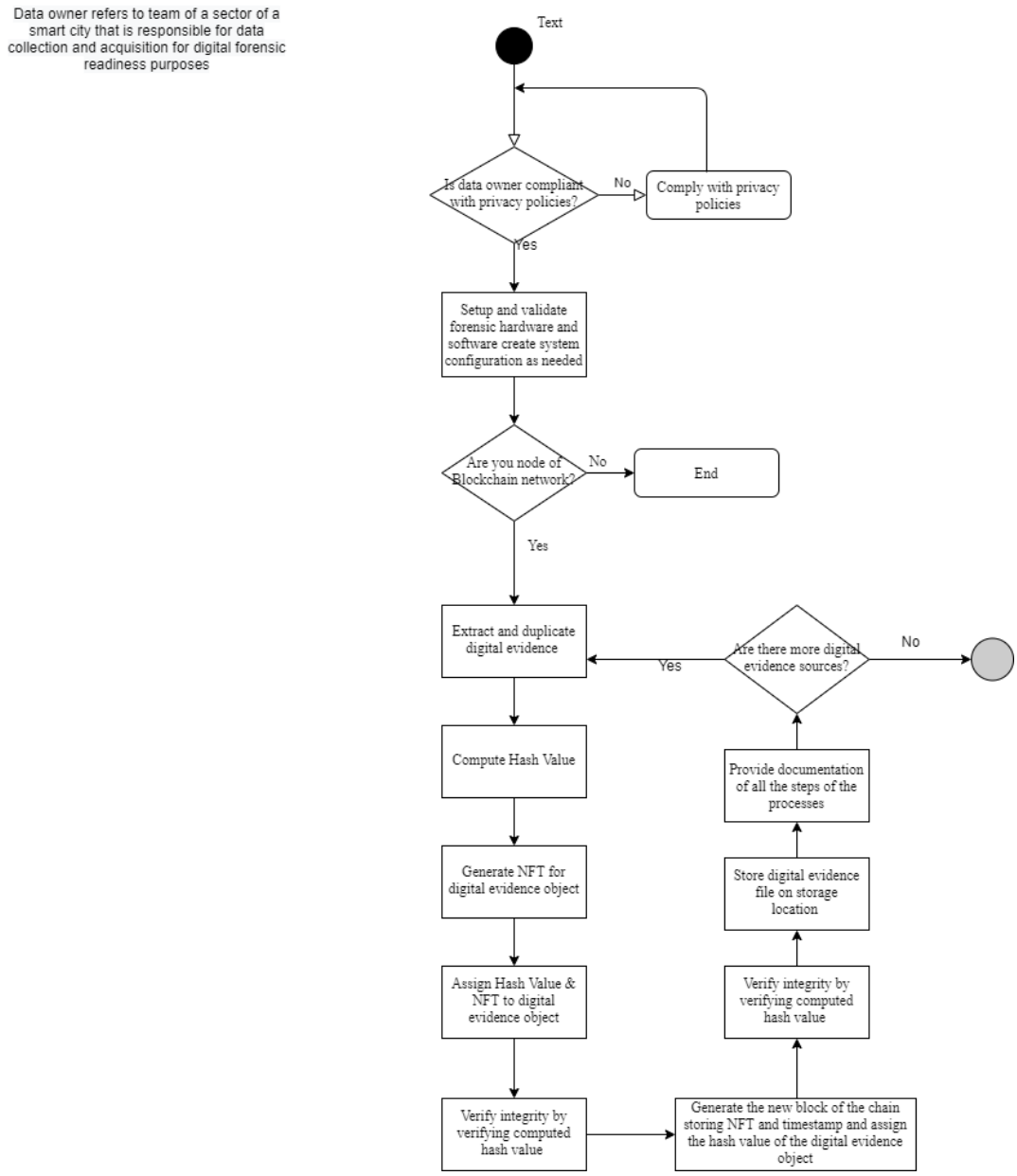

FIGURE 8.12: Pre-incident digital forensic readiness phase

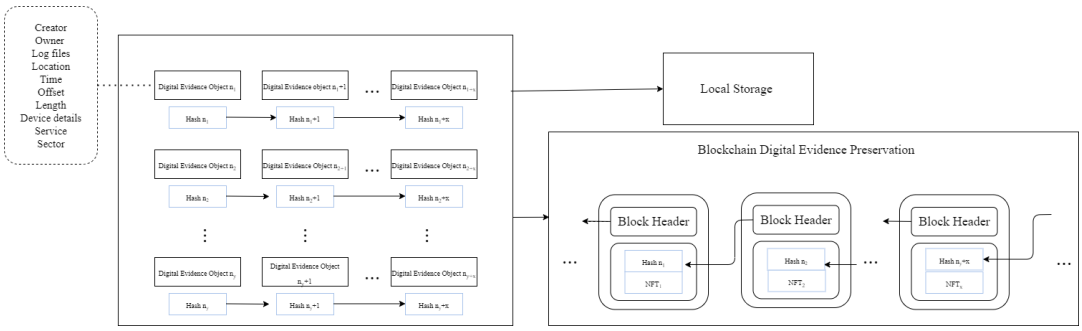

FIGURE 8.13: Digital Evidence Preservation

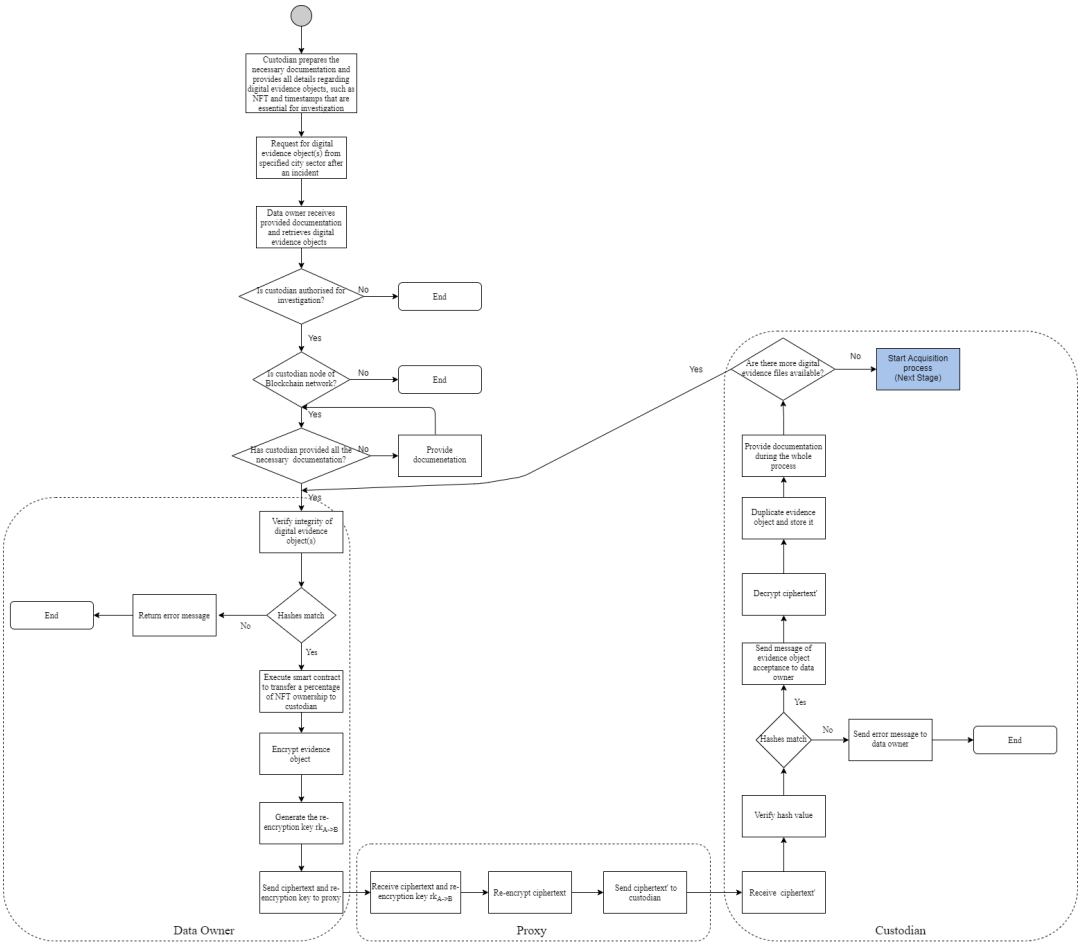

FIGURE 8.14: Post-incident digital forensic readiness phase

the framework obtains a lightweight fragmented ledger for forensic participants, who may preserve forensic data with limited access. This proposed framework does not take into consideration the ISO/IEC 27043 standard or any other approved readiness framework.

Moreover, in Brotsis et al. (2019), authors introduce a digital forensic evidence collection and preservation Blockchain-based solution. Authors describe a private, permissioned Blockchain network, where available evidence is stored, addressing security services, such as integrity, non-repudiation, availability, authentication, etc., in order for the Chain of Custody to be preserved and the evidence to be used within the context of a digital forensic investigation. The presented solution focuses on the realm of smart homes domain. Also, smart contracts have been employed in order to facilitate the communication of different entities that are involved in the investigation processes, including Internet service providers, law enforcement agencies and prosecutors.

The above presented research indicates the need for a digital forensic readiness framework and the need for improvement of the existing processes that should be followed by the respective frameworks. Also, the employment of the Blockchain technologies has been introduces as solution for the preservation of the security and integrity of the frameworks and in particular of the available digital evidence. For the needs of this research, the deployment of a DFRF and a DFRP facilitates a *forensic-by-design* approach, where digital evidence will be collected and stored before an incident takes place.

On the other hand, the introduced frameworks and models may not be able to facilitate the adoption of a digital forensic readiness framework within the realm of a smart city, due to the heterogeneity and complexity of this particular domain. In addition, this research focuses on smart cities, taking into consideration their achieved maturity level and introduces a crowdsourced approach, where various members and parties are involved to the collection and preservation of digital evidence.

All the participants, such as local authorities, stakeholders and service providers of a city environment should comply with the stages of the proposed playbook and adopt it as a plan of digital forensic readiness. The employment of the same DFRP provides a level of consistency between authorities, providers, and stakeholders, not only within the same city environment, but also enables the interconnectivity and communication between peer cities authorities with similar vulnerability exposure and profile. Furthermore, the maturity level of a city must be taken into consideration during the whole process, as it may indicate important details with regards to the frequency of digital evidence object possession and maintenance until the post-incident phase.

The proposed digital forensic readiness framework-playbook includes two phases, the pre-incident and the post-incident.

The pre-incident phase of the DFRP starts with determining the core team and by assign roles to its members. This stage of the process is critical, since teams, roles, and responsibilities must be defined from the outset. In addition, external teams and roles must be defined as well such as partners of service providers and their CSIRTs, which are responsible for the adoption and implementation of DFRP and the maintenance of digital evidence objects. Also, the escalation plan should be defined in advance. This stage of the playbook is presented in Figure 8.9.

During the pre-incident phase, the local authorities, service providers and critical sectors CSIRTs have to be able to identify the level of service business continuity, taking into consideration the maturity level, and potential risk factors that may disrupt the availability and impact the performance of the underlying systems and services, as well as the consequences of this disruption. All sectors and service providers should initially perform a risk assessment, depending on their criticality in order to identify the risk factors that may interrupt their operations, always having the city's maturity level in mind. As risk factors have been identified and evaluated, identification of digital evidence sources is the second most important step of the readiness playbook since all the necessary information for a digital forensic investigation comes from stored files within the network, devices, and service providers, such as Cloud and Edge Computing, application, Operating Systems, servers, databases, and so forth. Figure 8.10 presents the identification of digital evidence sources and the definition of risk factors stage.

As mentioned above, a crowdsourced approach should be adopted following the high heterogeneity and interconnectivity, especially on higher maturity levels. Crowdsourced approaches include coordination of peer authorities and CSIRTs, employed by the smart city's service providers. These teams of public and private sectors service providers are responsible for the identification of data sources within a city environment, the definition of criticality of the identified data sources and prioritisation of data collection, following the DFRP defined by local authorities and city level CSIRTs.

Digital and physical assets should be identified, and information related to these assets is essential for digital forensic readiness purposes. In the case of a physical asset, such as smart devices and sensors, information that facilitates readiness purposes may include log files, location details, contact details, if a device has been

placed in a public or residential place, details regarding the physical asset, such as manufacture, model, version, firmware, updates, MAC, IP, service provider and sector it facilitates. For digital assets, the same information may include metadata of data files of interest, data from various sources, such as network, applications, and operating systems, pcap files, collected data from monitoring tools, like implemented SIEMs, firewalls, and access control systems, timestamps, storage location, volatility, sector that facilitates, and so forth, as presented in Figure 8.11.

In addition, the identification of digital evidence types may facilitate the categorisation of digital evidence that should be maintained and it may indicate the frequency of digital evidence retrieval. For instance, in the case of a responsive city and volatile digital evidence type, the frequency of digital evidence retrieval may be increased, depending on the criticality of service as well (see Figure 8.11).

8.6.6 Digital Evidence Object Collection

The proposed Blockchain-based DFRP defines two entities, data owner, and custodian.

- Data owner or evidence owner refers to the respective core and extended team, the roles within this team as well those responsible for the detection, and collection of digital evidence, the generation and assignment of hash values and NFTs over the collected evidence objects, and the safe preservation of evidence and its integrity, until the beginning of an investigation. A digital evidence owner is a node of a private, permissioned Blockchain network, which has been employed as a means of implementing a Chain of Custody and ensuring the integrity of the contained information, based on its built in features, such as non-repudiation, integrity assurance, traceability and transparency. Being a node of the employed private Blockchain, the digital evidence owner obtains a pair of private and public keys, which is used in order to sign and verify transactions on the Blockchain network. These transactions include the computed hash values, the generated and assigned NFT and a timestamp for each of the digital evidence objects. All the data owners-service providers (CSIRT teams) within a city, are members of this private, permissioned Blockchain, along with city's authorities, stakeholders, and potential custodians, who are responsible for digital forensics investigations after an incident has been identified. These teams are considered to be a part of the city's critical infrastructures, such as energy and water provision, transportation, and public safety, and their goal is to collect and preserve as much digital evidence as possible in order to fulfil the requirements of digital forensic readiness framework adoption and facilitate future digital forensics investigations.

- Custodian or custodians are those members of the city's or jurisdiction's authorities or external investigators, who take over duties after a security incident has taken place. Custodians are members of the private, permissioned Blockchain network, obtaining a pair of keys, as the data owners do. Since their duties start after an incident, they are part of the post-incident phase. Their responsibilities include the identification of potential digital evidence objects that have been already collected and preserved by critical service providers, request for accessing these objects, verification of their integrity and analysis them for digital forensics investigation purposes, until they present their documentation to a court of law. Custodians may be considered as honest but curious, which means that the processes of transferring and receiving digital

evidence objects must be regulated by integrity and validity verification. This is achieved trough the usage of cryptographic techniques, such as computation and assignment of hashes and employment of encryption schemes. In addition, the access right over digital evidence objects and the computational capacity of custodian(s) should be defined (in advance) as well.

As discussed above, it is assumed that custodian is honest but curious. This means custodian is considered as honest, but curious, for verifying the correctness of digital evidence, the proper preservation regarding its integrity and validity and the time that it was captured. In addition, the deployment of a digital forensic readiness framework based on Blockchain provides various essential features, facilitating traceability, transparency and non-repudiation. Furthermore, data owner may be considered as "semi-honest", which means that he might have complied with the rules of the aforementioned presented playbook or the rules regarding the preservation of digital evidence objects before the beginning of an investigation, affecting their integrity and validity. Employing this framework, we aim to achieve the following security goals:

- Provable digital evidence objects possession for ensuring that data owner preserves them intact. Evidence objects must be created and stored in a predefined way that is able to reveal if they have been changed, facilitating custodian to accept them for acquisition and analysis or not.
- Provable digital evidence transmission for ensuring the successful transfer of digital evidence objects from data owner's local storage to custodian and their appropriateness for an investigation.
- Provable digital evidence deletion for ensuring the deletion of evidence objects after the completion of digital forensics investigation.

The pre-incident digital evidence objects collection process that is described below involves only digital assets, since a physical asset, like a hard disk of a computer, should not be removed without an incident has happened. The evidence collection process for a physical asset starts after an incident and includes the same steps as for a digital asset. The evidence object that will be created for a physical asset must include all the necessary information as presented above, the accompanying hash value that ensures the integrity, the NFT token and a timestamp, as presented in Figure 8.13. This data is preserved as records on a Blockchain network that facilitates a digital forensic readiness framework.

After the identification of digital evidence sources, the collection process begins. Before the collection process, the service provider must be compliant with privacy policies, since digital evidence may include personal information. In addition, the service provider, and particularly peer CSIRT must be a node of a private, permissioned Blockchain network that facilities the digital forensic readiness framework and is employed for the integrity of the Chain of Custody to be preserved. Furthermore, the data owner-service provider obtains a pair of cryptographic keys, a public and a private one, which is used for the needs of Blockchain processes. If the service provider is compliant with privacy policies, and member-node of the private city digital forensic readiness Blockchain, CSIRT validates the forensic hardware and software and creates the system configuration as needed. After the end of this step, extraction of the necessary data starts, while at the same time CSIRT computes the necessary hash value that will be assigned on the digital evidence object for

integrity purposes. After the completion of extraction and hash value computation processes, NFT generation takes place. NFT is used as a unique identifier assigned on a digital evidence object that can be used for ownership purposes regarding the transmission of it between authorities after an incident for investigation purposes. NFT is generated and the ownership is kept by the CSIRT of the data owner-service provider. This information along with NFT and all the changes of ownership are kept as stored records in token metadata. After the generation of NFT, the CSIRT of the service provider creates a new Blockchain transaction that includes the computed hash value of digital evidence data, the NFT of that specific digital evidence object and a timestamp that indicates the date and time, when digital evidence object has been created and stored. The new block of the chain is generated and includes the public key of the transaction creator, and transaction data, as described above. Because of the immutability, non-repudiation, transparency and traceability features of Blockchain, all the members-nodes of the network can keep a copy of the ledger, which includes all the new transactions that have been verified, the digital evidence objects details that every CSIRT of service providers within a city obtain for future investigations, the identity of every CSIRT and authorities, which add new transactions on the ledger regarding new identified digital evidence objects, by using their public and private keys for creating, signing and verifying new transactions. After transaction validation and generation of the new block of the chain, the CSIRT chooses the storage location of the digital evidence object or objects along with the computed hash value, which is used for verifying the integrity of data, and the NFT. Furthermore, duplication of digital evidence objects is necessary.

If there are more data sources for digital evidence collection, the CSIRT starts the same process again, otherwise, the collection process ends. The frequency of collection depends on the criticality of services that is provided to a city, the importance of its business continuity, and the maturity level of city, where the service is provided.

Algorithm 1: Evidence Object Creation

```
Input: Evidence Object, Hash Value, NFT
Result: Create new digital evidence object
if evidence object exists then
    return Evidence Object;
else
    compute and assign hash value ;
    execute smart contract for NFT generation ;
    assign generated NFT to digital evidence object ;
    sign transaction and generate the new block of the chain, including hash
     of evidence object, NFT and timestamp ;
```

8.6.7 Digital Evidence Objects Preservation

In Figure 8.13, the digital evidence preservation is presented. In order for a digital evidence object to be able to facilitate a future digital forensics investigation, it is necessary to include specific information.

This information involves:

- evidence ID is assigned to each digital evidence object through the usage of NFTs and the execution of smart contacts;
- creator of digital evidence object, which indicates the authority and particular team member who created evidence object;

- owner of digital evidence object, referring to the owners of data retrieved as evidence;
- log files, all the necessary artifacts for supporting a future digital forensics investigation;
- location, where log files have been retrieved from;
- details related to time, such as offset, TTL, etc.;
- length of the digital evidence object;
- details regarding the service provider, the sector that it facilitates and the device from where digital evidence object has been retrieved from.

8.6.8 Post-Incident Phase and Transmission of Digital Evidence Objects

A digital forensics investigation is triggered upon detection of the security incident. The post-incident phase is presented in Figure 8.14. The city-level custodian Z starts the investigation, after having identified how the incident happened, when, which the systems of a city have been compromised and where evidence regarding the incident can be collected from. After having answered all these questions, custodian Z gathers all the necessary details regarding the evidence that is essential for that particular investigation. Before the investigation starts and after answering questions regarding the incident, custodian Z checks if the damaged by the incident service provider has already collected digital evidence from specific data sources. In this case, Z documents the incident details along with the details of digital evidence objects that are stored on the Blockchain network and sends it to service provider(s). It should be mentioned that custodian Z must be compliant with privacy policies, such as all the members and parties of the city, taking into to consideration the existence of personal information within digital evidence objects. Custodian Z provides all the necessary documentation to service provider or providers - data owner, who preserve the stored collected digital evidence objects, along with their assigned NFTs, which are used as unique identifiers of digital evidence objects. When the former receives the documentation and NFTs from custodian Z, they have to go through the control process of validating the authenticity of documentation and the transmission process of digital evidence objects or physical asset that is involved in the incident. The transmission process starts with the service provider retrieving all the necessary information for a particular digital evidence object from Blockchain and verifying the integrity of the former by verifying the assigned hash value. If the verification is successful, the data owner prepares digital evidence object or objects for transmission. One more action that has to be taken is the transmission of the ownership of the NFT token from its owner, the service provider-data owner, to custodian or custodians who require access to it. For the needs of this step, a smart contract must be executed by data owner, where the public key of custodian must be used as the address of the new owner of the token. The change of ownership of NFT and the transmission of digital evidence objects are preserved as records on the Blockchain network. This process employs a Proxy Re-Encryption scheme cryptosystem to address the secure delivery of the digital evidence object(s).

When the ownership of NFT is transferred from service provider-data owner to custodian Z, the first encrypts digital evidence object $\mathcal{E}$ with his/her public key p (under encryption primitive $e(\cdot)$), and generates a new re-encryption key, $r_{A \to B}$ sending both, $\mathcal{C} = e_p(\mathcal{E})$ and re-encryption key to proxy. The proxy receives the

encrypted digital evidence object, re-encryption key $r_{A \to B}$, and re-encrypts the first with the new key. After the digital evidence object has been encrypted with the new key, the proxy transmits the newly re-encrypted object $\mathcal{C}'$, to custodian Z.

When the custodian receives $\mathcal{C}'$, integrity verification must be performed for validating the assigned hash value. If integrity verification is successful, custodian Z decrypts the $\mathcal{C}'$, using his/her private key sk_B, duplicates the digital evidence object and the acquisition and analysis processes begin. Otherwise, custodian returns error message to data owner, informing that he/she cannot proceed to the investigation with the provided evidence object(s), since integrity has been compromised. It is important to mention that digital evidence objects may have to be shared among more than one custodians for an investigation to begin and be performed. Even NFT being an innovative approach that supports proof of ownership for digital assets, there is a constrain regarding this ownership and the number of entities that token have to be shared between at the same time. According to our research, it was realised that traditional NFTs schemes are not compatible with the needs of this proposal, since digital forensics investigation processes may be done in a parallel manner by more than one incident response teams and custodian. As such, there is a need for a different NFT scheme that supports ownership by multiple entities. In order for this challenge to be addressed, a distributed ownership of the NFT tokens standard should be adopted. As such, Distributed NFT scheme can support multiple ownerships by more than one member of the Blockchain network and digital forensic readiness framework (Singh (2019)). In Figure 8.15, dNFTs generation and ownership expressed by a percentage for digital and physical evidence objects are presented. The creation and maintenance of digital evidence objects is part of the pre-incident phase, which is facilitated by the application of the dNFTs scheme concept. As mentioned above, for the needs of a digital forensics investigation, digital evidence objects may be essential to be shared among more than one custodian and/or authorities. The distributed ownership scheme, introduced in Singh (2019), allows more than one authorities to have access to a digital evidence object, working simultaneously on a particular one, by sharing its ownership. During all the stages of the digital forensic investigation process, documentation of all the actions that are taken must be kept. When an investigation finishes and the final report is presented in a court of law, the ownership of NFT must return to its creator. This final step indicates the end of digital forensic investigation and the preservation of no data by authorities responsible for an investigation and custodians.

Algorithm 2: Evidence Object Transmission-Data Owner

Input: Evidence Object, Hash Value, NFT
Result: Transmission Status
if *NFT exists & custodian provides the essential documentation* **then**
  verify the evidence object assigned hash value ;
  recompute hash value ;
  if *hashes match* **then**
    execute smart contract to transfer a percentage of NFT ownership to custodian ;
    encrypt evidence object with your public key;
    generate the re-encryption key $rk_A \rightarrow B$;
    send ciphertext and re-encryption key to proxy;
  else
    return evidence object integrity has been compromised;
else
  return evidence object does not exist ;

Algorithm 3: Evidence Object Transmission, Proxy

Input: ciphertext, re-encryption key
Result: ciphertext'
receive ciphertext and re-encryption key $rk_A \rightarrow B$;
re-encrypt ciphertext;
send ciphertext' to custodian;
end;

Algorithm 4: Evidence Object Transmission, Custodian

Input: ciphertext', Hash value
Result: evidence object transmission status
receive ciphertext';
verify hash value ;
if *hash values match* **then**
  integrity check is successful;
  send message of evidence object acceptance to data owner;
  decrypt ciphertext';
  duplicate evidence object and store it;
  start investigation;
else
  decline evidence object;
  send error message to data owner;

8.6.9 Digital Evidence Deletion

The evidence object deletion process is the final stage after the completion of a digital forensics investigation. In this research, two types of deletion were defined, soft and hard deletion. The type of deletion that will be followed each time depends on the maturity level that a city has achieved, having the technological integration and the need for advanced security and privacy solutions, especially on higher maturity city

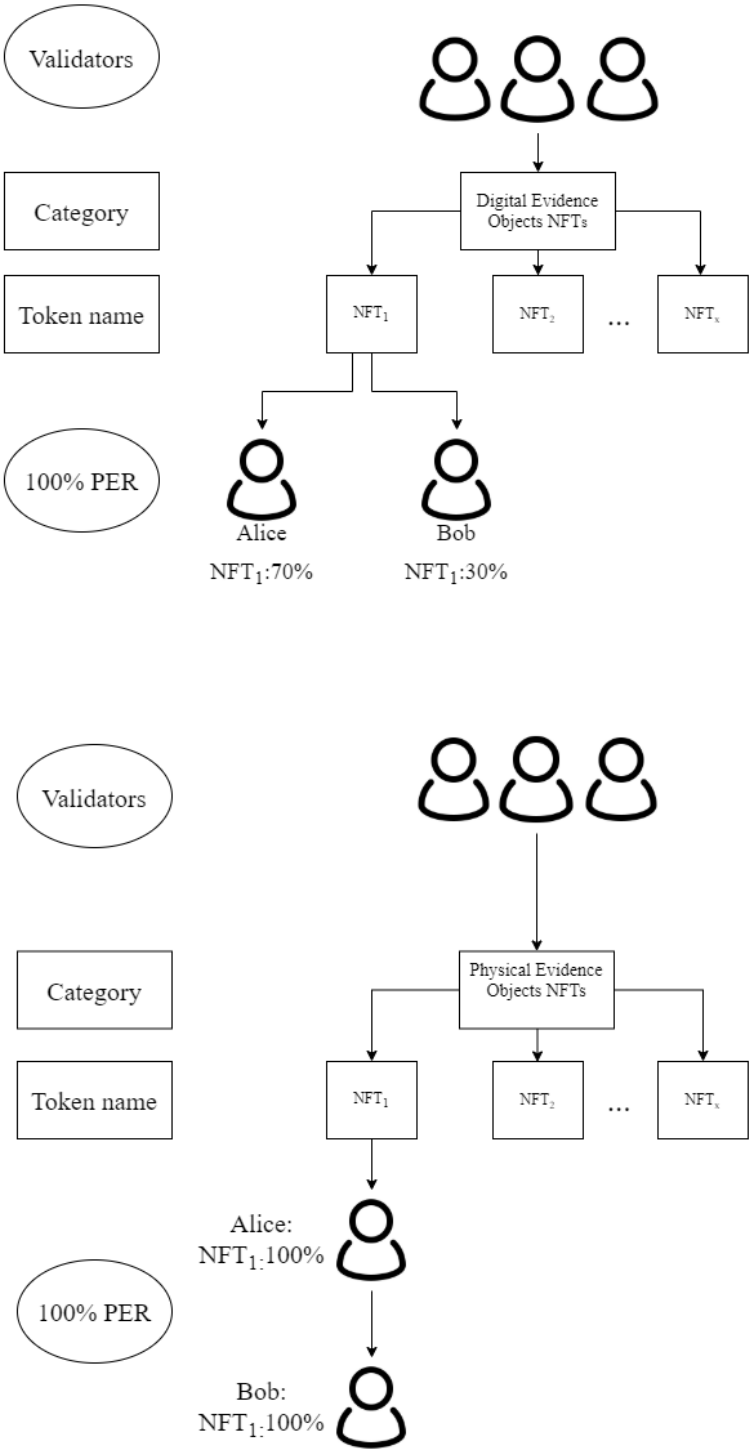

FIGURE 8.15: dNFT ownership transmission for digital and physical evidence objects (adapted from Singh (2019))

levels in mind. The two types of evidence objects deletion include specified steps that should be followed by both sides, data owners and custodians.

In addition, the hard deletion scheme involves the adoption of Merkle trees for preserving a hash chain and verification of proof of deletion, as described in Yang, Chen, and Xiang (2018). In addition, smart contacts for transferring the NFT ownership back to the data owner are employed for both deletion types.

In this research it is assumed that custodian should not preserve evidence objects after the end of an investigation, ensuring the protection and preservation of evidence privacy. After transferring the evidence objects to custodians and performing the necessary digital forensics investigation, the former needs to "return" evidence to its owner. It is assumed that the custodian and owner are honest, and the communication channels are secured. The aim of this model includes the correct deletion of evidence objects after the completion of an investigation, the preservation of evidence objects privacy, and the prevention of custodians misbehavior.

Soft deletion

The soft deletion involves the data owners and custodians, without the involvement of a Third Trusted Party (TTP) for addressing trust issues between both parties. The soft deletion scheme may be employed as a solution in lower maturity levels cities, and includes the return of NFT ownership to evidence object owner, after the completion of an investigation, the generation of a deletion request, and its verification. Verifying and signing a deletion request that the data owner has generated for particular evidence objects, facilitates the deletion process in lower maturity levels.

The soft deletion process is described by the following steps:

- The data owner generates and sends an evidence object deletion request to the custodian. The soft deletion process starts with the deletion request generation.
- The data owner computes $Sig_{Del} = Sig_{(sk_O)}(\text{"}deleteobject\text{"}, NFT_x, t_s)$ and generates the following deletion request: $DelReq = (\text{"}deleteobject\text{"}, Sig_{Del}, NFT_x, t_s)$, where NFT_x is the NFT assigned to a particular evidence object which will be deleted by custodian, and t_s is a timestamp. After the generation of the deletion request, the data owner sends it to the custodian.
- When the custodian receives the deletion request from the data owner, it is essential to go through the request verification process. The custodian verifies the signature Sig_{Del} using the public key of the data owner pk_O. If Sig_{Del} is valid, the custodial performs the deletion of the evidence object, otherwise, he returns an error message to the data owner.
- Upon successful deletion, the custodian executes the smart contract for returning NFT ownership percentage that he was assigned to the data owner.

Algorithm 5: Evidence Object Soft Deletion, Data Owner

```
Input: Evidence Object, Hash Value, NFT
Result: Deletion request
for <all evidence objects> do
    generate and send deletion request ;
return deletion request
```

Algorithm 6: Evidence Object Soft Deletion, Custodian

```
Input: Evidence Object, Hash Value, NFT
Result: Proof of evidence object deletion
while preserve evidence objects and the investigation is over do
    if deletion request is valid then
        verify deletion request ;
        delete evidence object ;
        execute smart contact for NFT ownership percentage return ;
    else
        return error message to data owner
return proof of deletion;
```

Hard Deletion

The hard evidence deletion model involves the data owner and the custodian, without the involvement of a TTP for addressing the potential trust issues between both sides. The deletion operation starts and its validity gets verified by the data owner. If the custodian does not delete the evidence objects, the data owner is able to detect it. After the completion of a digital forensics investigation, the data owner signs a deletion request, using his private key and transmit it to the custodian. The custodian verifies the deletion request and deletes the respective evidence objects, if the request is valid. After the deletion of the evidence object, the custodian generates a proof for the data owner to verify the results. In addition, he executes a smart contract for returning the percentage of NFT ownership that he obtains to the data owner.

The hard deletion process includes the following steps executed by both, the data owner and the custodians:

- `Delete`: The data owner generates and sends a deletion request to the custodian to delete the evidence objects that he preserves for the needs of an investigation, after its completion. When custodian receives the request, he goes through the verification process.

- `DelReqGen`: The data owner generates a deletion request for deleting evidence objects, and transfers it to custodian. The data owner computes a signature $sig_{DEL} = sig_{sk_O}(\text{"}deleteobject\text{"}, NFT_x, h_i, t_s)$, where NFT_x and h_i the assigned NFT token and hash value of the evidence object during its creation. The data owner generates the request $DelReq = (\text{"}deleteobject\text{"}, Sig_{DEL}, NFT_x, h_i, t_s)$, and sends it to custodian.

- Deletion process: the custodian receives the deletion request $DelReq$, and validates it. The custodian verifies the signature with data owner's the public key pk_O. If it is valid, the custodian deletes the evidence object and triggers the execution of NFT ownership smart contracts.

- `ProofGen`: After deleting the evidence object, the custodian generates the proof, which is provided for the data owner to verify the outcome of the deletion. $GenProof(Sig_{Del}, Sig_C, NFT_x, t_s)$ is the generated proof of deletion. The custodian computes $proof_i = (\text{"}deleteobject\text{"}, Sig_{Del}, Sig_C, NFT_x, t_s)$, where $Sig_C = Sig_{skC}(\text{"}deleteobject\text{"}, NFT_x, ts)$. The custodian transmits $proof_i$ to the data owner and he builds a Merkle hash tree preserving all the generated proofs. For the needs of the Merkle hash tree, the custodian computes a new hash value h_i for the new $proof_i$, as $h_i = H_i(h_{i-1}, t_s, root_i)$, where h_{i-1} is the previous value of the hash chain. After the hash value computation, the data owner receives the final deletion proof evidence $ep = (proof_i, root_i, h_i)$.

Hard deletion is feasible only in higher maturity levels, where Cloud service is involved, as Platform as a Service (PaaS) model.

Algorithm 7: Evidence Object Hard Deletion, Data Owner

Input: Evidence Object, Hash Value, NFT
Result: Deletion request
for *<all evidence objects>* **do**
    generate and send deletion request ;
return deletion request

Algorithm 8: Evidence Object Hard Deletion, Custodian

Input: Evidence Object, Hash Value, NFT
Result: Proof of evidence object deletion
while *preserve evidence objects and the investigation is over* **do**
    if *deletion request is valid* **then**
        verify deletion request;
        delete evidence object ;
        execute smart contact for NFT ownership percentage return ;
        generate the deletion proof;
        sign and return the deletion proof to data owner;
    else
        return error message to data owner

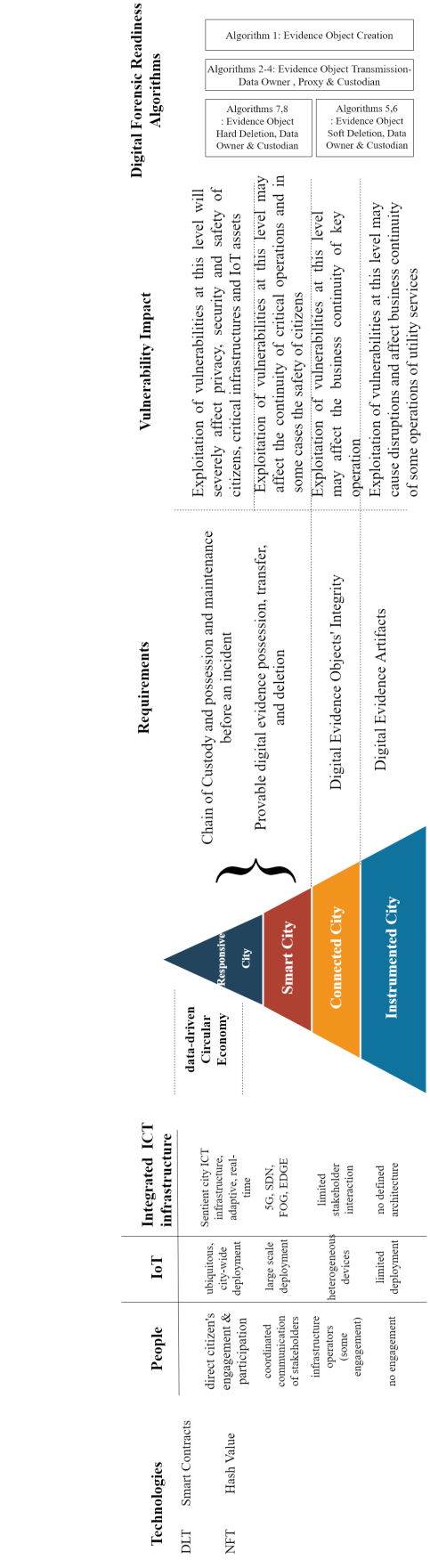

FIGURE 8.16: Deployed Digital Forensic Readiness algorithms and their employment based on the city's maturity level

8.7 Evaluation

As digital forensic readiness is considered to be part of Incident Response (IR), the following analysis considers the IR technologies a city is expected to adopt. In order to observe the equilibria of the impact of IR technologies in a smart city ecosystem, two sets of assumptions have been developed as follows:

1. Incident response technologies demand. We first explore how the impact and consequently risk of vulnerabilities affects the demand of IR technologies.

    - There exists a positive relationship between the maturity level (M) of a city and the impact (I) contributed by a vulnerability, $I = f(M)$. This is supported by the observation that the more advanced (i.e. mature) a city is, the higher the Socio-Technical integration would be. In essence, it is accepted that the environment affects the impact of a certain vulnerability. Such an approach has also been adopted in the widely accepted by the CVSS scoring method, where the base score can be further adjusted by specifying the environmental variables.
    - In agreement with the prevalent definition of quantitative risk (i.e. risk = probability * impact), we accept the positive relationship between impact and risk, R=g(I).
    - In cybersecurity, the demand for security controls is risk-driven. That is, the higher the risk, the more security controls will need to be implemented in order to mitigate the (unaccepted) risk. After the application of the security controls, what remains is the residual (or acceptable) risk. As such, there exists a positive relationship between risk and IR controls IR=h(R): the higher the risk, the higher the demand for IR technologies, and conversely, the lower the risk, the lower the IR technologies demand.

    Figure 8.17 presents the positive relationship between the maturity level and the impact, the impact and risk and the incident response and risk.

2. The IR technologies supply. In this case we consider the overall investment of technologies that contribute to the increase of the maturity level of a smart city, along with the (necessary) investment of IR technologies.

    - The target or aspired maturity level determines the level of investment of the smart city enabling technologies. The stakeholders and decision makers consider the smart city initiatives and projects a city would need to implement and seek for the associated budget approvals. This suggests a positive relationship between the maturity level (M) and smart city investment (S): $S = u(M)$.
    - As with any ICT investment, there also needs to be a budget consideration for non-functional elements, such as the security controls investment. In this analysis, we single out the IR technologies to be the additional investment needed to protect the smart city infrastructure against threat actors targeting vulnerabilities. The total investment is fixed to the budget line $SI^* = u(M) + IRS$.
    - Economists suggest that market forces and economic laws, if left alone, will eventually push IR technologies supply to equilibrium with IR technologies demand, regardless of their initial allocation. This is represented by the identity function $IR = IRS$.

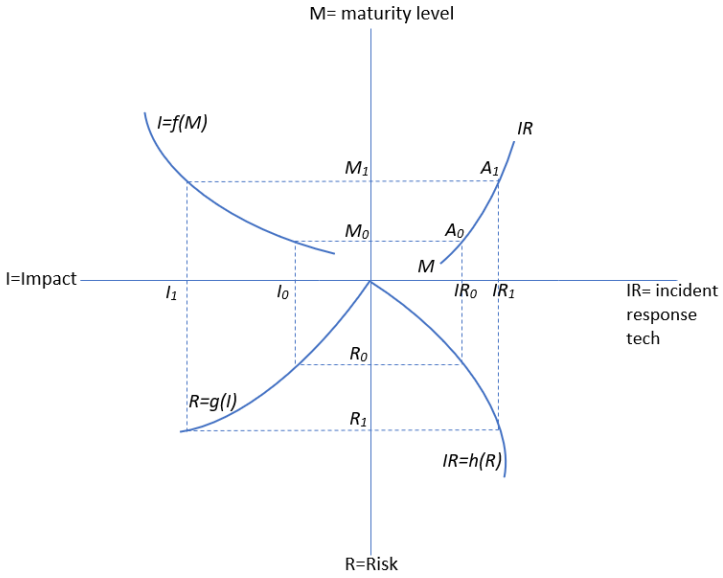

FIGURE 8.17: Demand of Incident Response technologies

Figure 8.18 shows the results of the cross method. Interestingly, the supply of IR technologies drops as the maturity level increases. This is in agreement with the findings presented in Chapter 7, where it was shown that in more mature cities the human capital compensates and contributes to the level of security. Moreover, a higher maturity level suggests that the technological investment is loaded on the enabling technologies, which, if combined with a circular economy agenda, security will also be offered through the exploitation of such technologies.

By superimposing the two diagrams of the first quadrants, the overall equilibrium E of the relationship between the maturity level and the IR technologies is obtained (Figure 8.19)

Throughout this thesis the adoption of the CE paradigm is advocated, which dictates that the existing, finite resources should reach their highest utilisation potential. In what follows the introduction of the proposed approaches is examined, which leverage existing infrastructures (logfile retention performed by data owners, that include local authorities, service providers, and stakeholders, and utilisation of Blockchain to crowdsource forensic functions in order to improve forensic readiness).

The main assumption of crowdsourcing is the "*spontaneous*" introduction of resources in order to solve a problem (primarily a computational one, but serving a business requirement). A representative recent example is the implementation of COVID19 digital certificates where the citizens use their own existing computing resources (i.e. smart phones) with a relatively minimum investment (i.e. a lookup app to verify their vaccination or infection status (Angelopoulos, Damianou, and Katos (2020))). Such straightforward and relatively simple approach capitalised on the collective, distributed computing capabilities and has allowed the resume of pre-covid activities, to an extent.

From the cross methodology's perspective, the "*pulling*" of citizen's computational power would result into the increase of the available budget, which is depicted by a parallel movement of the budget line (SI*) away from the beginning of the axes, say SI**. By repeating the methodology again, the new M'-IR' equilibrium

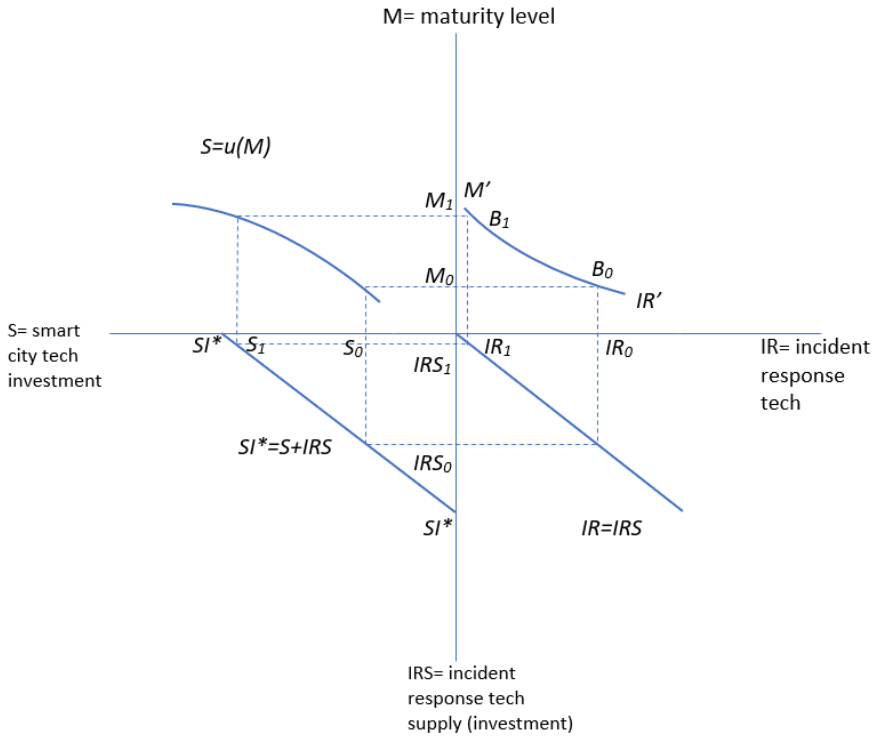

FIGURE 8.18: Supply of IR technologies

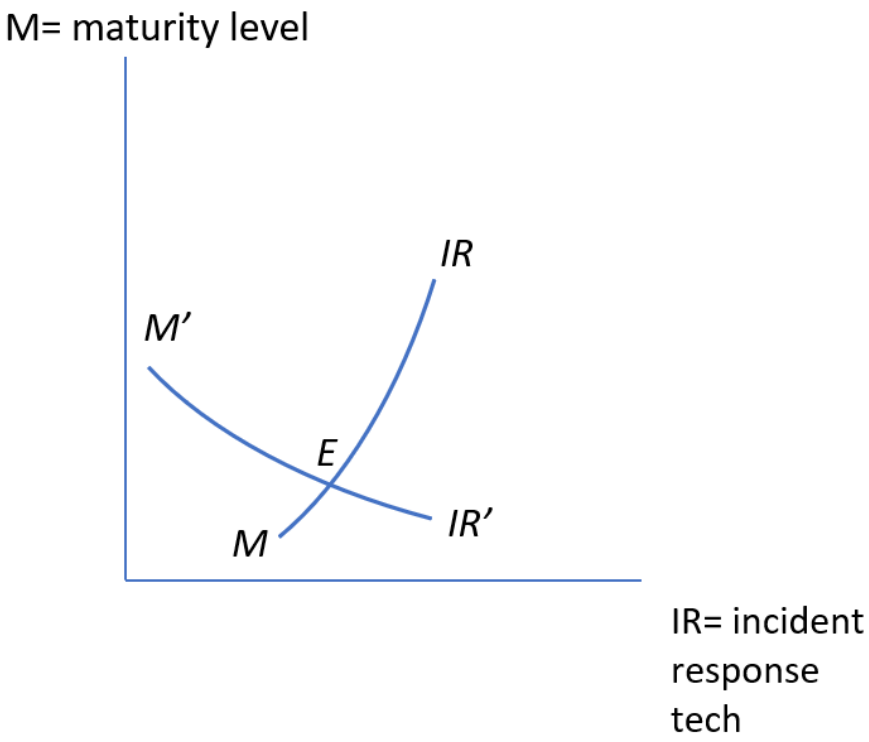

FIGURE 8.19: The overall equilibrium

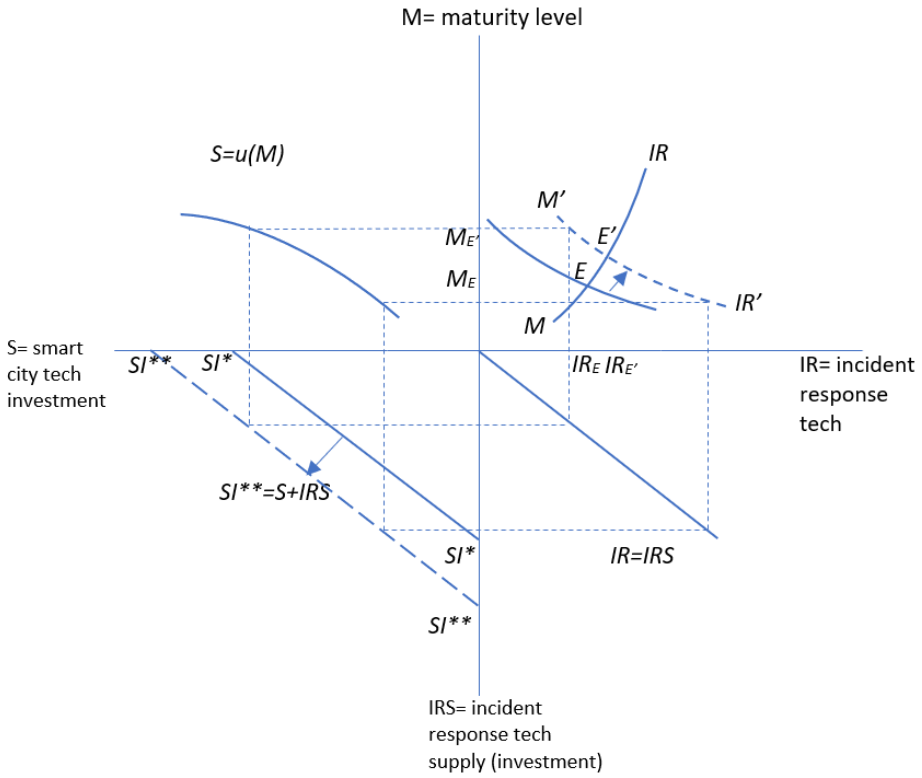

FIGURE 8.20: The effect of crowdsourcing

line and the new overall equilibrium E′ are obtained.

By comparing E and E′ is observed that the introduction of crowdsourcing will seamlessly increase the maturity level of a city (as more resources will be integrated and used), requiring also a corresponding increase in IR technologies.

8.8 Chapter Summary

In this Chapter, incident response and digital forensics terms are introduced, and the digital forensic readiness requirements, based on ISO/IEC 27043:2015 is defined. In addition, the necessity for the employment of a DFRP by smart cities, the collection of digital evidence, before an incident, and the maintenance of evidence integrity, during its whole lifecycle, from its collection until the final presentation to a court of law, through a digital forensics investigation are highlighted. In order for the identified digital forensic readiness requirements to be addressed, the deployment and the implementation of a DFRP, adopted by a city's local authorities, stakeholders, and service providers are proposed. The adoption of the playbook provides guidance to the former parts and members of a city to identify potential digital evidence sources and types, define the teams and roles that will conduct the identification and collection of digital evidence processes, potential risk factors that may affect the provided services, as well as critical infrastructures and services that may be affected, always taking into consideration the maturity level that a city has achieved.

Furthermore, we point out the need for digital evidence integrity during all the phases of the digital forensic readiness, from the possession, until the final deletion after the completion of a digital forensic investigation and the documentation presentation to a court of law.

In order to facilitate the maintenance of the integrity of digital evidence objects, we propose the use of Blockchain, smart contracts, and NFT technologies. Through the employment of these technologies, all participating entities may be able to preserve transparency throughout the digital forensic readiness processes that have been followed, the possession of digital evidence objects by data owners and custodians, during the pre-incident and post-incident phase, the digital evidence object sharing for digital forensic investigation purposes, and the final deletion of these objects after the completion of the investigation.

Finally, the proposed approach has been evaluated by adopting a qualitative macroeconomics approach in order to assess the support of the CE paradigm by the proposed DFRP.

Chapter 9

Conclusions

In this Chapter, the findings of this research are summarised. The thesis is successfully assessed in answering the research question, as well as the success in meeting the research aims. In addition, the challenges and limitations of this research are presented, as well as the discussion regarding the future work.

9.0.1 Novel aspects of the thesis

This section summarises the novel aspects of this thesis.

The main idea of this research is the vulnerability exposure of a city that has adopted advanced technological solutions, based on various dimensions and the deployment of a Digital Forensic Readiness Framework (DFRF), taking into consideration the maturity level that the city has achieved.

In order for the the goals of this research to be facilitated, an empirical analysis of the current smart cities and their technological assets' exposure based on existing vulnerabilities has been performed and factors that may increase and decrease the vulnerability exposure of cities, especially on higher maturity levels have been identified.

In addition, a digital forensic readiness framework is introduced and a DFRP, describing both pre-incident and post-incident phases was deployed, for facilitating local authorities, service providers and stakeholders to adopt it and comply.

Also, a Blockchain approach on the digital forensics domain in order to address the preservation of integrity of the Chain of Custody challenges was adopted and the differences between Ethereum and EOS, the advantages and the limitations of each DLT network and the adoption of EOS DLT scheme have been critically evaluated. Moreover, a suite of algorithms have been introduced for handling on-chain digital evidence related data, providing details about the digital evidence possession and the creation of digital evidence objects, the digital evidence objects transmission, as well as the digital evidence objects deletion after the completion of the digital forensics investigation.

Finally, a decision making and evaluation tool based on a macroeconomics methodology in order to evaluate and validate the compatibility of the aforementioned playbook and algorithms against the CE paradigm has been presented.

9.1 Evaluation

9.1.1 Aim 1

- Provide a suitable definition of a smart city, what sustainability entails, and investigate the technological enablers adopted by smart cities, as well as their contribution of Circular Economy model.

The research aim was motivated by the rapid evolution of cities during the last decades and the complexity that smart cities ecosystems obtain. In addition, technological enablers have been investigated and studied, as well their security and privacy challenges that obtain have been discussed. In addition, the novel Circular Economy model is studied, as it is considered as a key contributor regarding the maintenance of smart cities sustainability. In addition, the maturity model presented in *IDEAL CITIES* was adopted (Ideal-Cities (2018)) project, for mapping the technological integration and the implementation of a CE agenda of cities (**Objective 1.1**). This aim is addressed in Chapter 3.

Furthermore, in Chapter 4, four use cases related to some of the sectors of a city, such as transportation and healthcare have been developed and presented. Through the introduced use cases it can be described city sectors that have achieved different levels of maturity and how potential vulnerabilities impact may differ among these levels (**Objective 1.1**). The presented use cases introduce the exploitation of vulnerabilities and risks within the realm of smart cities, compromising critical infrastructures and causing serious issues and putting in danger citizens safety and life. The use cases take into consideration various cities that have achieved different maturity levels, designating the interconnectivity and interdependency among the adopted technological enablers and systems, as well as the interconnectivity and interdependency among critical sectors and infrastructures within the same ecosystem. The introduction of the use cases in this Chapter informs the vulnerability management and the dimensions that affects the vulnerability exposure profile of a city, presented in the Chapter 7. In addition, the Digital Forensic Readiness Framework (DFRF) and Digital Forensic Readiness Playbook, presented in Chapter 8 are informed by the presented use cases, dependent of the maturity level that a city has achieved.

9.1.2 Aim 2

- Identify the common ground between the technological integration and the increase of the vulnerability exposure of smart cities.

Aim 2 was motivated by the increase of the technological integration and the investment of effort, resources and budget, as well as the extensive increase of cyber attacks as a consequence of the substantial growth of smart cities. There are many different cases that indicate the increase of vulnerabilities and risks exploitation and systems tampering within smart urban environments. For this claim to be investigated, a quantitative vulnerability assessment was conducted, adopting the Common Vulnerability Scoring System (CVSS) (FIRST (2020), Chandramoull et al. ("Common Vulnerability Scoring System")). The severity of the identified vulnerabilities is assessed against, not only the calculated CVSS base score, but against the so-called environmental variable. Urban governance and business models for sustainability have been revised or redesigned to meet the expectations of citizens through the introduction of ICT infrastructure.

In order for the quantitative research to be conducted, both primary and secondary data were collected. The available datasets for this research belong to two main and orthogonal domains, a "*smartness*" metrics and factors conducted by business type of research groups, such as the Cities in Motion research (Berrone and Ricart (2019)) and domain refers to cybersecurity research, adopting the ENISA vulnerabilities 2018-2019 dataset (Rostami (2020), ENISA (2019)), which includes contextualised vulnerability data from various open sources. The second dataset has

been extended and enriched with geolocation, on a country and a city level, and device exposure data from the online Shodan datasets. In addition, for executing the hypothesis testing on a country level, the Global Cybersecurity Index has been also included (Bruggemann et al. (2021)).

The quantitative research includes statistical analysis using Python / Jupyter notebooks. The analysis tests a set of statistical hypotheses to illustrate the potential risks that may affect a the city based on a set of factors included in the Cities in Motion survey (Berrone and Ricart (2019)), dependent on the presented maturity model.

This analysis focused on cities cases that have employed a (data-driven) Circular Economy agenda, which we believe may increase the potential vulnerability exposure of a city (**Objective 2.1**). Nonetheless, findings designate that the more technologically advanced urban environments obtain higher vulnerability exposure (**Objective 2.1**).

On the other hand, the investment on technological enablers and human capital enables the moderation of this exposure, enabling it to be minimised, however not at the desirable level in order for high exposure city profiles to be addressed. From a cybersecurity perspective, attacks against smart city's services and infrastructures, may deter citizens of using the provided by the city services. Since there is a wide range of technological domains and themes, we assert that vulnerabilities involve a horizontal theme, *expanding* and infecting many other domains.

9.1.3 Aim 3

- Propose and deploy a DFRP for local authorities, service providers and stakeholders in general and introduce a Blockchain and smart contracts based approach for digital evidence integrity preservation, dependent on the smart city maturity level.

Aim 3 was motivated by the employment of ICT infrastructures and devices on a massive scale and the definition of cyber situational awareness and incident response capabilities from the outset. Thus, identifying a point of convergence between cybersecurity and local government is critical.

In addition, the high heterogeneity and interconnections among service providers, local authorities and stakeholders increase the exposure surface, allowing more systems to be compromised and infected by exploitation of vulnerabilities.

Also, the lack of standardised digital forensic investigation processes within the realm of smart cities highlights the significance of well-defined incident response protocols and the presence of a digital forensic ready framework. As such, a DFRP, based on a crowdsourced approach was introduced, that may be employed by a city's local authorities, stakeholders and service providers, in order for future investigation to be facilitated (**Objective 3.2**). The aim of the proposed playbook is to enhance the incident response plan of a smart city, to preserve digital evidence until an incident takes place and ensure the integrity of the collected evidence, from its collection until the final presentation in a court of law, satisfying all the essential criteria, until the prism of the maturity level that a city has achieved.

The goal of the proposed digital DFRP is to designate the teams and roles that are responsible for the identification, collection and preservation of digital evidence, before an incident takes place, the critical infrastructures within a smart city and the processes that should be followed from the data owners side before a digital forensic investigation starts.

TABLE 9.1: Employed technologies for addressing digital forensics investigation requirements

Digital Forensics Requirements	NFT	DLT	Smart Contracts	Hash Value
Chain of Custody Integrity				✓
Evidence Object Integrity				✓
Transparency		✓	✓	
Traceability		✓	✓	
Non-repudiation	✓		✓	
Provable evidence possession, transfer, deletion	✓		✓	

In addition, the technologies that have been adopted for this proposal and the digital forensic readiness requirements that each of them addresses have been presented (**Objective 3.1**). The Table 9.1 depicts the requirements regarding digital forensic readiness at each of the presented maturity levels, including the technologies that have been adopted for facilitating them. From the Figure 9.1, it is obvious that the adopted technologies have been employed for facilitating the digital forensic readiness framework only on the higher level of maturity, on Smart and Responsive levels. In the context of this research, it has been apparent that the increasing technological integration comes along with the increase of the vulnerability exposure of a city. Thus, we believe that since lower maturity level cities employ technological enablers for specified and constrained purposes may not require the adoption of a digital forensic readiness framework and the employment of addition technologies that may facilitate constrains aims.

On the other hand, we believe that cities, which have achieved Smart and/or Responsive maturity level, may have already employed the proposed technologies for addressing various challenges. Thus, the deployment of a digital forensic readiness framework and the adoption of a DFRP, based on existing technological enablers within an urban environment may be an efficient solution. In the Table 9.1, the employed technologies for the needs of this research have been presented and their contribution to particular digital forensic readiness requirements as well. In addition, as it has been discussed in (Bada et al. (2021)), the decision for the adoption of Blockchain technology should be taken based on the energy consumption of consensus mechanisms. The proposed framework of this research provides to the decision making of stakeholders for choosing the ideal consensus mechanism and the Blockchain environment based on their current needs.

Since there is need for reducing the energy consumption and addressing the climate changes challenges, the deployment of a novel Blockchain based solution for facilitating only the needs of a digital forensic readiness framework, especially on lower maturity levels, where Blockchain is not already adopted, may rise additional challenges and add unnecessary complexity to an Instrumented or a Connected city.

Finally, we evaluated the proposed digital forensic readiness framework has been evaluated adopting a qualitative macroeconomics approach in order to assess the compatibility of our playbook against the CE paradigm (**Objective 3.3**).

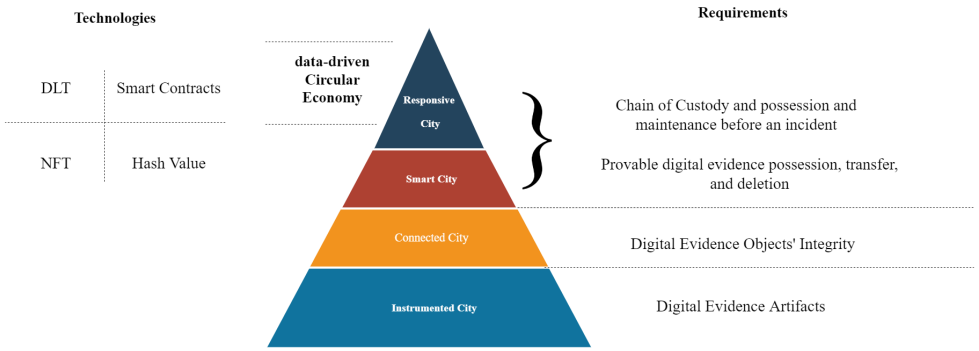

FIGURE 9.1: Requirements and Proposed Technologies for the deployment of a digital forensic readiness framework

9.2 Challenges and Limitations

The research presented in this thesis, such as any other scientific study, has limitations.

Some of the critical challenges of this research have been already presented and discussed in Chapter 7.

First of all, the fact that there is no information related to the type of service or ownership of a vulnerable device is considered as limitation of this research. Thus, a city is considered only as one entity, without distinguishing various services, sectors and devices within the same city ecosystem (critical infrastructures, different sectors, devices of public and private domain and so forth). Furthermore, the available datasets do not include IPv6. This fact excludes a considerable number of IoT devices, may affecting the results of this research, especially for cities that have achieved higher maturity levels and those that have already adopted 5G. As such,

regarding the lack of information related of the type of services or ownership of vulnerable devices, the fact that the current dataset does not cover IPv6, without taking into consideration a considerable number of IoT devices and the volatility of the results due to the live vulnerability exposure data nature, since recorded data from Shodan designate a snapshot of a specified time period. Therefore, it can be recognised that the results of our current research represent the best scenarios and the lower bounds of the attack surface. Also, the scope would be limited to more *traditional* and core services, due to the exclusion of IPv6. Nonetheless, this limitation, along with the geolocation method, designate the necessity for a city's NOC/SOC equivalent to invest in asset detection and a register, which is a non-trivial effort in practise. In addition, IP addresses exposing devices over VPN or TOR networks were not excluded because no significant bias was expected in the analysis.

The second identified limitation is related to the results volatility due to the live vulnerability exposure data nature. The Shodan data that this research considers, indicate a snapshot of a specified time period. For the purpose of this research, it is considered that vulnerability data are used for revealing if there are relationships between them and other types of data, related to different dimensions, such as behavioural and economic variables. Finally, the exposure metrics related to CVE

attribution to devices and services were performed by Shodan, so the results and accuracy of the results depend on Shodan's implicit vulnerability disclaimer.

Another challenge, emerging from this research, is related to the CVSS scoring system for performing identified vulnerabilities assessment. Although CVSS approach may be considered as trustworthy, various applications introduce conflicts regarding the assigning values process and its validity. Even the CVSS scoring system may be considered as established, it has received criticism regarding its validity. The CVSS may be considered as *incomplete*, since it only takes into consideration the base score, which is not the only metric that indicates the severity of an identified threat or vulnerability. Temporal and environmental scores, that are provided by the CVSSv3.0 must be included as well.

In addition, various CVEs with identical base score are grouped together. As such, it is difficult to prioritise particular CVEs taking into consideration only the calculated CVSS base score. Furthermore, the calculation of the base score in the CVSS includes limited variables, *low*, *medium*, *high* and *critical*. These values provide a finite number of possible scores and groups of threats with the same score. Also, the CVSS does not consider the age of a vulnerability, making it not concrete over the time. Finally, threats and risks base scores are publicly available and accessed by cybersecurity teams through a massive number of databases. Relying on these databases may not be considered as a good practice, since this data does not provide key risk context and does not reflect the true severity level of a real world exploit.

Also, the lack of standardised digital forensic investigation approaches within the realm of smart cities, especially related to the IoT paradigm, in order for our proposal to be critically assessed is a limitation for this research, since our proposal could not be evaluated in accordance to existing and established approaches. There are various digital forensic investigation approaches related to some of the presented technological enablers of this research, however, none of these approaches are established, especially those related to the IoT paradigm. Due to the heterogeneity of a smart city ecosystem, and the existence of various services, sectors and technological enablers, a *universal* approach that tries to address every entity and part of a city may not be efficient in this case.

As such, this research presents a proactive digital forensic approach for identifying and collecting digital evidence before an incident takes place, by the respective service provider or the sector administrator. A future digital forensic investigation process will be conducted considering the technological paradigm and the experts recommendations for a particular incident. On the other hand, it is not possible to assess the proposed approach taking into consideration existing approaches, since none of them are considered as established and *"official"*.

An additional limitation or challenge is the lack of a cryptosystem scheme that may facilitate custodians to verify the integrity preservation and the correctness of a hash value for one or more particular digital evidence objects, before they access these objects, during the receipt/ delivery. During the post incident phase, data owner needs to transmit the available digital evidence objects to the custodian or custodians, who will conduct the digital forensic investigation. In order for custodians to identify if there are alterations regarding the provided digital evidence objects, and verify the integrity of these objects, before they access the available data, the adoption of a cryptosystem may facilitate this stage of the process. Through the study process in order to address this part of this research, the lack of a cryptosystem with these operations and features has been identified. As such, this research adopts other cryptosystem schemes with similar features that might facilitate this stage of

the process, identifying the lack and the need for a cryptosystem scheme developing as well.

A final limitation of this thesis is that the proposed approach has not been evaluated by the researcher. As a future work, one of the main aims related to this research is the development and the implementation of the proposed digital forensic readiness framework, based on the adoption of the Blockchain and smart contracts technologies, employing EOS Blockchain platform, which facilitates a Blockchain network maintenance, and the execution of smart contracts in order for NFT values to be generated. In addition, the employment of the EOS Blockchain platform provides the dNFT scheme, which allow the distribution of the ownership among more than one custodians, after the beginning of a digital forensic investigation.

9.3 Future Work

This section proposes directions for future work based on the findings of this research.

9.3.1 A vulnerability integrated model development in smart, circular cities

Future work related to the research presented in the Chapter 7, involves the deployment of a vulnerabilities integrated model in the context of smart, circular cities by performing structured equation modelling (SEM) on the indicators of the non-vulnerability related data, such as those presented in Cities in Motion research and the IMD world digital competitiveness data that include the citizens' perceptions and adoption of smart city technologies.

From the vulnerabilities perspective, the available datasets enrichment with standardised Customer Type Indicators (CTIs), such as ATT &CK's techniques and tactics and CAPEC, may provide additional insights on the exposure of a city and facilitate decision making more efficiently.

A medium term research direction involves the introduction of sector specific device information to further enrich the vulnerabilities using theory and approaches from the interdependent network domain.

9.3.2 Introduction of Environmental Score for the assessment of identified vulnerabilities

For the needs of this research, a vulnerability scoring system, and more precisely the CVSS scoring system has been adopted. In order to perform all the necessary analysis, only the base scores of the identified vulnerabilities were taking into consideration. Since one of the main aspects of this research is related to the differences between the level of the technological integration and the adoption of the CE paradigm among cities, future work should include the evaluation of the identified vulnerabilities, depending on the environmental factors, such as the maturity level and the interconnectivity of infrastructures, devices and sectors.

Environmental score of an identified vulnerability must be taken into consideration, due to the different impact that it may have on a lower or higher maturity level.

9.3.3 Deployment and implementation of the Proposed Digital Forensic Readiness Framework

Future work, related to the proposed framework introduced in Chapter 8, involves the deployment and the implementation of a Blockchain, smart contracts and NFT based digital forensic readiness, employing EOS Distributed Ledger platform and developing a private and permissioned Blockchain network, with local authorities, service providers and stakeholders being nodes of this network for incident response plan and digital forensic readiness to be facilitated within a Smart and/or a Responsive city environment.

In addition, the implementation of our proposed DFRF in accordance with the regulation of local authorities and service providers of actual smart cities, should be addressed for facilitating a real incident response plan.

9.3.4 Formal validation of proposed Readiness Framework algorithms

Furthermore, future work involves the formal validation of the proposed Digital Forensic Framework algorithms, presented in Chapter 8. These algorithms indicate the steps and the processes that should be followed by both sides, data owners and custodians during the pre-incident and post-incident phases regarding the identification, collection, preservation, transmission and deletion of digital evidence objects that may facilitate a digital forensic investigation. In order for these algorithms to be validated, it is necessary to be expressed as a program for assuring that they facilitate their purposes. The programming language that is employed for validating these algorithms is the Python.

9.3.5 Empirical estimation of supply and demand curves

For the proposed digital forensic readiness framework to be evaluated a *cross methodology* approach from the domain of macroeconomics has been adopted to assess whether the proposed playbook would support the CE paradigm. The macroeconomics analysis that is presented in Chapter 8 is a qualitative analysis. As future work, it is essential to perform a quantitative analysis, conducting an empirical estimation of the presented curves.

9.3.6 How acceptable would be a playbook by stakeholders - user/human acceptance

For the needs of this research, a crowdsourced approach has been proposed related to the deployment of an incident response plan, dependent of the maturity model, adopted by the *IDEAL CITIES* project (Ideal-Cities (2018)), and the implementation of a digital forensic readiness framework through the use of a playbook. The proposed approach involves all the members and parties of a smart city environment. Part of our future work should include the consensus achievement among local authorities, stakeholders and service providers, citizens as well, who indicate the human factors elements of the forensic readiness framework. The consensus among all these members and parties plays a key role for the success deployment and implementation of a crowdsourced incident response and a digital forensic readiness framework.

9.4 Concluding Summary

This research was motivated by the evolution of smart cities, which are considered as complex and with high heterogeneity ecosystems, to preserve balance and sustainability, but at the same time to address potential challenges from the increase of people and facilitate citizens needs. In addition, the increase of technological integration rise various security and privacy challenges related to the increase of vulnerability exposure of a city.

While perfect security and privacy techniques adoption may not be efficient-effective-optimal enough to address the upcoming challenges that novel and innovate technological paradigms bring, the deployment of an effective/efficient incident response plan and a digital forensic readiness framework based on a crowd-sourced approach should be defined from the outset.

The deployed incident response plan and the proposed digital forensic readiness framework should be employed by local authorities, service providers and stakeholders, allowing them the collection and preservation of digital evidence objects during the pre-incident phase, and the transmission and processing of evidence by custodians for performing data acquisition, analysis and presentation within the context of a digital forensics investigation, during the post-incident phase.

In order for the integrity of the Chain of Custody to be preserved during both pre-incident and post-incident phases, the proposed approach based on Blockchain technologies has been introduced.

References

Ab Rahman, Nurul Hidayah, William Bradley Glisson, Yanjiang Yang, and Kim-Kwang Raymond Choo (2016). "Forensic-by-design framework for cyber-physical cloud systems". In: *IEEE Cloud Computing* 3.1, pp. 50–59.

Abreu, David Perez, Karima Velasquez, Marilia Curado, and Edmundo Monteiro (2017). "A resilient Internet of Things architecture for smart cities". In: *Annals of Telecommunications* 72.1-2, pp. 19–30.

Agencia de Ecología Urbana de Barcelona (2012). URL: http://www.bcnecologia.net/en.

Ahmad, Ijaz, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov (2018). "Overview of 5G security challenges and solutions". In: *IEEE Communications Standards Magazine* 2.1, pp. 36–43.

Al Nuaimi, Eiman, Hind Al Neyadi, Nader Mohamed, and Jameela Al-Jaroodi (2015). "Applications of big data to smart cities". In: *Journal of Internet Services and Applications* 6.1, pp. 1–15.

Al-Sultan, Saif, Moath M Al-Doori, Ali H Al-Bayatti, and Hussien Zedan (2014). "A comprehensive survey on vehicular ad hoc network". In: *Journal of network and computer applications* 37, pp. 380–392.

Alsultanny, Yas A (2014). "Evaluating Users Intention to Use E-overnment Services". In: *environment* 3.5.

Alur, Rajeev, Emery Berger, Ann W Drobnis, Limor Fix, Kevin Fu, Gregory D Hager, Daniel Lopresti, Klara Nahrstedt, Elizabeth Mynatt, and Shwetak Patel (2016). "Systems computing challenges in the internet of things". In: *arXiv preprint arXiv:1604.02980*.

Alvear, Oscar, Carlos T Calafate, Juan-Carlos Cano, and Pietro Manzoni (2018). " Crowdsensing in smart cities: Overview, platforms, and environment sensing issues". In: *Sensors* 18.2, p. 460.

Angelopoulos, Constantinos Marios, Amalia Damianou, and Vasilios Katos (2020). "DHP Framework: Digital Health Passports Using Blockchain–Use case on international tourism during the COVID-19 pandemic". In: *arXiv preprint arXiv:2005.08922*.

Anthopoulos, Leonidas G (2017). "The rise of the smart city". In: *Understanding smart cities: A tool for smart government or an industrial trick?* Springer, pp. 5–45. DOI: https://doi.org/10.1007/978-3-319-57015-0. URL: https://link.springer.com/book/10.1007\%2F978-3-319-57015-0.

Antikainen, Maria, Teuvo Uusitalo, and Päivi Kivikytö-Reponen (2018). "Digitalisation as an enabler of circular economy". In: *Procedia CIRP* 73. 10th CIRP Conference on Industrial Product-Service Systems, IPS2 2018, 29-31 May 2018, Linköping, Sweden, pp. 45–49. ISSN: 2212-8271. DOI: https://doi.org/10.1016/j.procir.2018.04.027. URL: http://www.sciencedirect.com/science/article/pii/S2212827118305432.

Ar, Sevinç (2021). *Circular Economy models for smart city assets*. URL: https://www.ideal-cities.eu/wp-content/uploads/2019/10/IDEAL-CITIES-D2.1.pdf.

Askoxylakis, Ioannis (2018). "A framework for pairing circular economy and the Internet of Things". In: *2018 IEEE International Conference on Communications (ICC)*. IEEE, pp. 1–6. DOI: 10.1109/ICC.2018.8422488.

Aufner, Peter (2020). "The IoT security gap: a look down into the valley between threat models and their implementation". In: *International Journal of Information Security* 19.1, pp. 3–14.

Babou, Cheikh Saliou Mbacke, Doudou Fall, Shigeru Kashihara, Ibrahima Niang, and Youki Kadobayashi (2018). "Home edge computing (HEC): Design of a new edge computing technology for achieving ultra-low latency". In: *International conference on edge computing*. Springer, pp. 3–17.

Bada, Abigael Okikijesu, Amalia Damianou, Constantinos Marios Angelopoulos, and Vasilios Katos (2021). "Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption". In: *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, pp. 503–511.

Baig, Zubair A, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, Paresh Kerai, Ahmed Ibrahim, and Krishnun Sansurooah (2017). "Future challenges for smart cities: Cyber-security and digital forensics". In: *Digital Investigation* 22, pp. 3–13.

Balbix (2019). *CVSS v2 vs CVSS v3*. URL: https://www.balbix.com/insights/cvss-v2-vs-cvss-v3/.

Barrionuevo, Juan M, Pascual Berrone, and Joan E Ricart (2012). "Smart cities, sustainable progress". In: *Iese Insight* 14.14, pp. 50–57.

Baru, Sanjaya (2018). "Blockchain: The next innovation to make our cities smarter". In: *en. In:(Jan. 2018)*, p. 48.

Basu, Srijita, Arjun Bardhan, Koyal Gupta, Payel Saha, Mahasweta Pal, Manjima Bose, Kaushik Basu, Saunak Chaudhury, and Pritika Sarkar (2018). "Cloud computing security challenges & solutions-A survey". In: *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, pp. 347–356.

Baxter, Gordon and Ian Sommerville (2011). "Socio-technical systems: From design methods to systems engineering". In: *Interacting with computers* 23.1, pp. 4–17.

Belchior, Rafael, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia (2020). "A survey on blockchain interoperability: Past, present, and future trends". In: *arXiv preprint arXiv:2005.14282*.

Belmonte Martin, A, L Marinos, E Rekleitis, G Spanoudakis, and NE Petroulakis (2015). "Threat landscape and good practice guide for software defined networks/5g". In:

Berkel, Antonie RR, Prince M Singh, and Marten J van Sinderen (2018). "An information security architecture for smart cities". In: *International Symposium on Business Modeling and Software Design*. Springer, pp. 167–184.

Berrone, Pascual and Joan Enric Ricart (2019). *IESE Cities in Motion Index*. URL: https://media.iese.edu/research/pdfs/ST-0509-E.pdf.

Bit_of_Hex (2019). *ATT&CKing the Singapore Health Data Breach*. URL: https://bitofhex.com/2019/01/attack-and-singapore-breach/.

Blockchain.com (2019). *Blockchain Size (MB)*. URL: https://www.blockchain.com/charts/blocks-size.

Bocek, Thomas, Bruno B Rodrigues, Tim Strasser, and Burkhard Stiller (2017). " Blockchains everywhere-a use-case of blockchains in the pharma supply-chain". In: *2017 IFIP/IEEE symposium on integrated network and service management (IM)*. IEEE, pp. 772–777.

Bocetta, Samuel (2020). *Following a wallet hack, the IOTA Foundation hits turbulence.* URL: https://bravenewcoin.com/insights/following-a-wallet-hack-the-iota-foundation-hits-turbulence.

Borgia, Eleonora (2014). "The Internet of Things vision: Key features, applications and open issues". In: *Computer Communications* 54, pp. 1–31.

Bris, Arturo and Christos Cabolis (2020). *IMD World Digital Competitiveness Ranking 2020*. URL: https://www.imd.org/globalassets/wcc/docs/release-2020/digital/digital_2020.pdf.

British-Standards-Institution (Aug. 2014). *The Role of Standards in Smart Cities*. URL: https://www.bsigroup.com/LocalFiles/en-GB/smart-cities/resources/The-Role-of-Standards-in-Smart-Cities-Issue-2-August-2014.pdf.

Brotsis, Sotirios, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Dimitris Kavallieros, Emanuele Bellini, and Clément Pavué (2019). "Blockchain solutions for forensic evidence preservation in IoT environments". In: *2019 IEEE Conference on Network Softwarization (NetSoft)*. IEEE, pp. 110–114.

Bruggemann, Rainer, Peter Koppatz, Margit Scholl, and Regina Schuktomow (2021). "Global Cybersecurity Index (GCI) and the Role of its 5 Pillars". In: *Social Indicators Research*, pp. 1–19.

Bruijn, Hans de and Marijn Janssen (2017). "Building cybersecurity awareness: The need for evidence-based framing strategies". In: *Government Information Quarterly* 34.1, pp. 1–7. DOI: https://doi.org/10.1016/j.giq.2017.02.007. URL: http://www.sciencedirect.com/science/article/pii/S0740624X17300540.

Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, and Bobby Filar (2018). "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation". In: *arXiv preprint arXiv:1802.07228*.

Buterin, Vitalik (2014). "A next-generation smart contract and decentralized application platform". In: *white paper* 3.37.

C40-Cities (2020). *Municipality-led circular economy case studies*. URL: https://www.c40.org/researches/municipality-led-circular-economy.

Cagnazzo, Matteo, Markus Hertlein, Thorsten Holz, and Norbert Pohlmann (2018). "Threat modeling for mobile health systems". In: *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, pp. 314–319.

Calderaro, Andrea and Anthony JS Craig (2020). "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building". In: *Third World Quarterly* 41, pp. 1–22. DOI: https://doi.org/10.1080/01436597.2020.1729729. URL: https://www.tandfonline.com/doi/epub/10.1080/01436597.2020.1729729?needAccess=true.

Caragliu, Andrea and Chiara Del Bo (2012). "Smartness and European urban performance: assessing the local impacts of smart urban attributes". In: *Innovation: The European Journal of Social Science Research* 25.2, pp. 97–113.

Carrier, Brian and Eugene Spafford (2004). "An event-based digital forensic investigation framework". In: *Digital Investigation*.

Case, Defense Use (2016). "Analysis of the cyber attack on the Ukrainian power grid". In: *Electricity Information Sharing and Analysis Center (E-ISAC)* 388.

Cebe, Mumin, Enes Erdin, Kemal Akkaya, Hidayet Aksu, and Selcuk Uluagac (2018). "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles". In: *IEEE Communications Magazine* 56.10, pp. 50–57.

Chakrabarty, Shaibal and Daniel W Engels (2016). "A secure IoT architecture for smart cities". In: *2016 13th IEEE annual consumer communications & networking conference (CCNC)*. IEEE, pp. 812–813.

Chandramoull, R, T Grance, R Kuhn, and S Landau. "Common Vulnerability Scoring System". In: *IEEE Computer Society* (), pp. 1540–7993.

Chaudhry, Natalia and Muhammad Murtaza Yousaf (2018). "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities". In: *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*. IEEE, pp. 54–63.

Cheng, Pengsu, Lingyu Wang, Sushil Jajodia, and Anoop Singhal (2012). "Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics". In: *2012 IEEE 31st Symposium on Reliable Distributed Systems*. IEEE, pp. 31–40. DOI: 10.1109/SRDS.2012.4.

Cheng, S, B Zeng, and YZ Huang (2017). "Research on application model of blockchain technology in distributed electricity market". In: *IOP Conference Series: Earth and Environmental Science*. Vol. 93. 1. IOP Publishing, p. 012065.

Chevet, Sylve (2018). "Blockchain technology and non-fungible tokens: Reshaping value chains in creative industries". In: *Available at SSRN 3212662*.

Chourabi, Hafedh, Taewoo Nam, Shawn Walker, J Ramon Gil-Garcia, Sehl Mellouli, Karine Nahon, Theresa A Pardo, and Hans Jochen Scholl (2012). "Understanding smart cities: An integrative framework". In: *2012 45th Hawaii international conference on system sciences*. IEEE, pp. 2289–2297.

Christidis, Konstantinos and Michael Devetsikiotis (2016). "Blockchains and smart contracts for the internet of things". In: *Ieee Access* 4, pp. 2292–2303.

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone (2012). "Computer security incident handling guide". In: *NIST Special Publication* 800.61, pp. 1–147.

Cimpanu, Catalin (2022). *UK government plans to release Nmap scripts for finding vulnerabilities*. URL: https://therecord.media/uk-government-plans-to-release-nmap-scripts-for-finding-vulnerabilities/amp/.

CISA (2020). *Critical Infrastructure Sectors*. URL: https://www.cisa.gov/critical-infrastructure-sectors.

Creese, Sadie, William H Dutton, Patricia Esteve-Gonzalez, and Ruth Shillair (2020). "Cybersecurity Capacity Building: Cross-National Benefits and International Divides". In: *Paper accepted for presentation at the TPRC48, Washington DC, February* 2021.

CWE (2020). *2020 CWE Top 25 Most Dangerous Software Weaknesses*. URL: https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html.

Damianou, Amalia (2017). *Anonymity on Cryptocurrencies. MSc thesis in Information Security. Royal Holloway, University of London.*

De Jong, Kenneth (1988). "Learning with genetic algorithms: An overview". In: *Machine learning* 3.2-3, pp. 121–138.

Dia, Hussein (2016). "The real-time city: Unlocking the potential of smart mobility". In: *Melbourne, Australia: Australasian Transport Research Forum 2016, Proceedings*, pp. 16–18.

Digiconomist (2021). *Bitcoin Energy Consumption Index*. URL: https://digiconomist.net/bitcoin-energy-consumption/.

Digital, DI (2018). *Copenhagen Smart City*. URL: https://www.danskindustri.dk/brancher/di-digital/.

Doan, Anhai, Raghu Ramakrishnan, and Alon Y Halevy (2011). "Crowdsourcing systems on the world-wide web". In: *Communications of the ACM* 54.4, pp. 86–96.

Dorri, Ali, Salil S Kanhere, and Raja Jurdak (2017). "Towards an optimized blockchain for IoT". In: *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, pp. 173–178.

Dorri, Ali, Marco Steger, Salil S Kanhere, and Raja Jurdak (2017). "Blockchain: A distributed solution to automotive security and privacy". In: *IEEE Communications Magazine* 55.12, pp. 119–125.

EC-Council (2020). *DREAD THREAT MODELING: AN INTRODUCTION TO QUALITATIVE AND QUANTITATIVE RISK ANALYSIS*. URL: https://blog.eccouncil.org/dread-threat-modeling-an-introduction-to-qualitative-and-quantitative-risk-analysis/.

Eger, John M (2009). "Smart growth, smart cities, and the crisis at the pump a worldwide phenomenon". In: *I-WAYS-The Journal of E-Government Policy and Regulation* 32.1, pp. 47–53.

Ekblaw, Ariel, Asaph Azaria, John D Halamka, and Andrew Lippman (2016). "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data". In: *Proceedings of IEEE open & big data conference*. Vol. 13, p. 13.

Ellen-MacArthur-Fundation. *Introdution to Circular Economy*. URL: https://www.ellenmacarthurfoundation.org/assets/downloads/sme/19_CE100-SME-booklet_print.pdf.

Energy, Nuclear (2019). *the Current Security Environment in the Era of Hybrid Threats*. Tech. rep. Research Report.

ENISA (Dec. 2019). *State of Vulnerabilities 2018/2019 - Analysis of Events in the life of Vulnerabilities*. URL: https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities/download/fullReport.

EOS (2018a). *Learn About Wallets, Keys, and Accounts With Cleos*. URL: https://developers.eos.io/eosionodeos/docs/learn-about-wallets-keys-and-accounts-with-cleos.

EOS Developer, Documenetation (2018b). *What is EOSIO*. URL: https://developers.eos.io/welcome/latest/index.

Esposito, Mark, Terence Tse, and Khaled Soufani (2018). "Introducing a circular economy: New thinking with new managerial and policy implications". In: *California Management Review* 60.3, pp. 5–19.

Ethdocs (2016). *Ethereum Homestead Documrntation- Ethereum Homestead 0.1 documentation.* URL: http://www.ethdocs.org/en/latest/.

Ethereum-Org. *Non-fungible tokens (NFT)*. URL: https://ethereum.org/en/nft.

European-Commission (2016). *5G for Europe: An Action Plan [online]. Available from:* URL: https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-588-EN-F1-1.PDF.

— (2019). *COMMISSION RECOMMENDATION of 26.3.2019 Cybersecurity of 5G networks*. URL: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks.

Evince-Development (2019). *Human to Machine Communication by Evince Development*. URL: https://evincedev.com/human-to-machine-communication/.

Fekete, Alexander (2011). "Common criteria for the assessment of critical infrastructures". In: *International Journal of Disaster Risk Science* 2.1, pp. 15–24.

Felten, Ed (2016). "Preparing for the future of artificial intelligence". In: *Washington DC: The White House, May* 3. URL: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

Fernández-Caramés, Tiago M and Paula Fraga-Lamas (2018). "A Review on the Use of Blockchain for the Internet of Things". In: *Ieee Access* 6, pp. 32979–33001.

FIRST (2020). *Common Vulnerability Scoring System*. URL: https://www.first.org/cvss/.

Fourtané, Susan (2018). *The Technologies Building The Smart Cities of The Future*. URL: https://interestingengineering.com/the-technologies-building-the-smart-cities-of-the-future.

Frazer, Jim (2018). *The Nine Critical Applications of a Smart City*. URL: https://www.arcweb.com/blog/nine-critical-applications-smart-city.

Galinec, Darko, William Steingartner, and Vinko Zebić (2019). "Cyber rapid response team: An option within hybrid threats". In: *2019 IEEE 15th International Scientific Conference on Informatics*. IEEE, pp. 000043–000050.

Gallon, L. (2010). "On the Impact of Environmental Metrics on CVSS Scores". In: *2010 IEEE Second International Conference on Social Computing*, pp. 987–992. DOI: 10.1109/SocialCom.2010.146.

Garcia, Flavio D, David Oswald, Timo Kasper, and Pierre Pavlidès (2016). "Lock it and still lose it—on the (in) security of automotive remote keyless entry systems". In: *25th {USENIX} Security Symposium ({USENIX} Security 16)*.

Gascó-Hernandez, Mila (2018). "Building a smart city: Lessons from Barcelona". In: *Communications of the ACM* 61.4, pp. 50–57.

Geissdoerfer, Martin, Paulo Savaget, Nancy MP Bocken, and Erik Jan Hultink (2017). "The Circular Economy–A new sustainability paradigm?" In: *Journal of cleaner production* 143, pp. 757–768.

Giffinger, Rudolf, Christian Fertner, Hans Kramar, Evert Meijers, et al. (2007). "City-ranking of European medium-sized cities". In: *Cent. Reg. Sci. Vienna UT*, pp. 1–12.

Giova, Giuliano (2011). "Improving chain of custody in forensic investigation of electronic digital systems". In: *International Journal of Computer Science and Network Security* 11.1, pp. 1–9.

Golubchikov, Oleg and Mary Thornbush (2020). "Artificial intelligence and robotics in smart city strategies and planned smart development". In: *Smart Cities* 3.4, pp. 1133–1144.

Goodfellow, Ian, Yoshua Bengio, and Aaron Courville (2016). *Deep learning*. MIT press.

GSMA (2018). *Opportunities and Use Cases for Distributed Ledger Technologies in IoT*.

Guthrie, Peter and Thalia Konaris (2012). *Infrastructure and Resilience. Commissioned Review*
. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/286993/12-1310-infrastructure-and-resilience.pdf.

Hall, Robert E, B Bowerman, J Braverman, J Taylor, H Todosow, and U Von Wimmersperg (2000). *The vision of a smart city*. Tech. rep. Brookhaven National Lab., Upton, NY (US).

Hasan, Monowar, Ekram Hossain, and Dusit Niyato (2013). "Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches". In: *IEEE communications Magazine* 51.6, pp. 86–93.

Hashem, Ibrahim Abaker Targio, Victor Chang, Nor Badrul Anuar, Kayode Adewole, Ibrar Yaqoob, Abdullah Gani, Ejaz Ahmed, and Haruna Chiroma (2016). "The role of big data in smart city". In: *International Journal of information management* 36.5, pp. 748–758.

Hashim, Nurul Akmal, Z Zainal Abidin, Nurul Azma Zakaria, Rabiah Ahmad, and AP Puvanasvaran (2018). "Risk assessment method for insider threats in cyber security: A review". In: *International Journal of Advanced Computer Science and Applications* 9.11.

Hellani, Hussein, Layth Sliman, Motaz Ben Hassine, Abed Ellatif Samhat, Ernesto Exposito, and Mourad Kmimech (2019). "Tangle The Blockchain: Toward IOTA and Blockchain integration for IoT Environment". In: *International Conference on Hybrid Intelligent Systems*. Springer, pp. 429–440.

Hollands, Robert G. (2008a). "Will the real smart city please stand up?" In: *City* 12.3, pp. 303–320. DOI: 10.1080/13604810802479126. eprint: https://doi.org/10.1080/13604810802479126. URL: https://doi.org/10.1080/13604810802479126.

Hollands, Robert G (2008b). "Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?" In: *City* 12.3, pp. 303–320.

Homeland Security, U.S. Department of (2019). *Information Sharing Specifications for Cybersecurity*
. URL: https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.

Hu, Yun Chao, Milan Patel, Dario Sabella, Nurit Sprecher, and Valerie Young (2015). "Mobile edge computing—A key technology towards 5G". In: *ETSI white paper* 11.11, pp. 1–16.

Huq, Numaan, Rainer Vosseler, and Morton Swimmer (2017). "Cyberattacks against intelligent transportation systems". In: *TrendLabs Research Paper*.

Ibba, Simona, Andrea Pinna, Matteo Seu, and Filippo Eros Pani (2017). "CitySense: blockchain-oriented smart cities". In: *Proceedings of the XP2017 Scientific Workshops*, pp. 1–5.

Ideal-Cities (2018). *IDEAL CITIES*. URL: https://www.ideal-cities.eu/.

International-Telecommunication-Union (2014). *Smart sustainable cities: An analysis of definitions*. URL: https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/Approved_Deliverables/TR-Definitions.docx.

IOTA. *IOTA-Nodes*. URL: https://docs.iota.org/docs/getting-started/0.1/network/nodes.

Ismagilova, Elvira, Laurie Hughes, Yogesh K Dwivedi, and K Ravi Raman (2019). "Smart cities: Advances in research—An information systems perspective". In: *International Journal of Information Management* 47, pp. 88–100. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.01.004. URL: http://www.sciencedirect.com/science/article/pii/S0268401218312738.

ISO/IEC-27043 (2015). "Information technology–Security techniques–Incident investigation principles and processes". In:

— (2015). *2015 International Standard, Information Technology – Security Techniques – Incident Investigation Principles and Processes, ISO.org*.

Johnson, Pontus, Robert Lagerström, Mathias Ekstedt, and Ulrik Franke (2016). "Can the common vulnerability scoring system be trusted? a bayesian analysis". In: *IEEE Transactions on Dependable and Secure Computing* 15.6, pp. 1002–1015. DOI: 10.1109/TDSC.2016.2644614. URL: https://www.tandfonline.com/doi/epub/10.1080/01436597.2020.1729729?needAccess=true.

Kaelbling, Leslie Pack, Michael L Littman, and Andrew W Moore (1996). "Reinforcement learning: A survey". In: *Journal of artificial intelligence research* 4, pp. 237–285.

Kaloudi, Nektaria and Jingyue Li (2020). "The AI-Based Cyber Threat Landscape: A Survey". In: *ACM Comput. Surv.* 53.1. ISSN: 0360-0300. DOI: 10.1145/3372823. URL: https://doi.org/10.1145/3372823.

Karlgaard, Rich (2005). *Ten laws of the modern world*.

Katos Vasilis, Rostami Shahin (2019). *STATE O F VULNERABILITIES 2018/2019. Analysis of Events in the life of Vulnerabilities*. URL: https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities.

Kebande, Victor R and Indrakshi Ray (2016). "A generic digital forensic investigation framework for internet of things (iot)". In: *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, pp. 356–362.

Kent, Karen, Suzanne Chevalier, Tim Grance, and Hung Dang (2006). "Guide to integrating forensic techniques into incident response". In: *NIST Special Publication* 10.14, pp. 800–86.

Kershner, Michael (2021). *Data Isn't The New Oil — Time Is*. URL: https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/.

Khan, Rafiullah, Kieran McLaughlin, David Laverty, and Sakir Sezer (2017). "STRIDE-based threat modeling for cyber-physical systems". In: *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, pp. 1–6.

Khoshgoftar, Mohammad and Omar Osman (2009). "Comparison of maturity models". In: *2009 2nd IEEE International Conference on Computer Science and Information Technology*. IEEE, pp. 297–301. DOI: 10.1109/ICCSIT.2009.5234402.

Ki-Aries, Duncan, Shamal Faily, Huseyin Dogan, and Christopher Williams (2018). "System of systems characterisation assisting security risk assessment". In: *2018 13th Annual Conference on System of Systems Engineering (SoSE)*. IEEE, pp. 485–492.

Klaper, David and Eduard Hovy (2014). "A taxonomy and a knowledge portal for cybersecurity". In: *Proceedings of the 15th annual international conference on digital government research*. New York, NY, USA: Association for Computing Machinery, pp. 79–85. ISBN: 9781450329019. DOI: 10.1145/2612733.2612759.

Kosba, Ahmed, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou (2016). "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts". In: *2016 IEEE symposium on security and privacy (SP)*. IEEE, pp. 839–858.

Kounelis, Ioannis, Gary Steri, Raimondo Giuliani, Dimitrios Geneiatakis, Ricardo Neisse, and Igor Nai-Fovino (2017). "Fostering consumers' energy market through smart contracts". In: *2017 International Conference in Energy and Sustainability in Small Developing Economies (ES2DE)*. IEEE, pp. 1–6.

Kourtit, Karima, Peter Nijkamp, and Daniel Arribas (2012). "Smart cities in perspective–a comparative European study by means of self-organizing maps". In: *Innovation: The European journal of social science research* 25.2, pp. 229–246.

Kure, Halima Ibrahim, Shareeful Islam, and Mohammad Abdur Razzaque (2018). "An integrated cyber security risk management approach for a cyber-physical system". In: *Applied Sciences* 8.6, p. 898.

Lacy, Peter and Jakob Rutqvist (2015). "Waste to Wealth: creating advantage in a circular economy". In: *Accenture Strategy* 293, pp. 1–288.

Lai, Chengzhe, Rongxing Lu, Dong Zheng, and Xuemin Shen (2020). "Security and privacy challenges in 5G-enabled vehicular networks". In: *IEEE Network* 34.2, pp. 37–45.

Langley, David J, Jenny van Doorn, Irene CL Ng, Stefan Stieglitz, Alexander Lazovik, and Albert Boonstra (2021a). "The Internet of Everything: Smart things and their impact on business models". In: *Journal of Business Research* 122, pp. 853–863.

— (2021b). "The Internet of Everything: Smart things and their impact on business models". In: *Journal of Business Research* 122, pp. 853 –863. ISSN: 0148-2963. DOI: "DOI:"https://doi.org/10.1016/j.jbusres.2019.12.035. URL: http://www.sciencedirect.com/science/article/pii/S014829631930801X.

LeBlanc, David and Michael Howard (2002). *Writing secure code*. Pearson Education.

Lei, Ao, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P Anyigor Ogah, and Zhili Sun (2017). "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems". In: *IEEE Internet of Things Journal* 4.6, pp. 1832–1843.

Li, Xiaoqi, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen (2020). "A survey on the security of blockchain systems". In: *Future Generation Computer Systems* 107, pp. 841–853.

Li, Zhen and Qi Liao (2018). "Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets". In: *Government Information Quarterly* 35.1, pp. 151–160. DOI: https://doi.org/10.1016/j.giq.2017.10.006. URL: http://www.sciencedirect.com/science/article/pii/S0740624X16302155.

Lone, Auqib Hamid and Roohie Naaz Mir (2019). "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer". In: *Digital Investigation* 28, pp. 44–55.

Lu, Qinghua and Xiwei Xu (2017). "Adaptable blockchain-based systems: A case study for product traceability". In: *Ieee Software* 34.6, pp. 21–27.

MacArthur, Ellen et al. (2013). "Towards the circular economy". In: *Journal of Industrial Ecology* 2, pp. 23–44.

Macrorie, Rachel, Simon Marvin, and Aidan While (2021). "Robotics and automation in the city: a research agenda". In: *Urban Geography* 42.2, pp. 197–217.

Maddinson, Paul and Deborah Petterson (2020). *CNI Hub. National Cyber Security Centre*. URL: https://www.ncsc.gov.uk/section/private-sector-cni/cni#section_1.

Mahdavinejad, Mohammad Saeid, Mohammadreza Rezvan, Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi, and Amit P Sheth (2018). "Machine learning for Internet of Things data analysis: A survey". In: *Digital Communications and Networks* 4.3, pp. 161–175.

Mahizhnan, Arun (1999). "Smart cities: the Singapore case". In: *Cities* 16.1, pp. 13–18.

Mahmoud, Rwan, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan (2015). "Internet of things (IoT) security: Current status, challenges and prospective measures". In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, pp. 336–341.

Manico, Jim (2015). *OWASP Application Security Verification Standard*. URL: https://owasp.org/www-project-application-security-verification-standard/.

Matias, Jon, Jokin Garay, Nerea Toledo, Juanjo Unzilla, and Eduardo Jacob (2015). "Toward an SDN-enabled NFV architecture". In: *IEEE Communications Magazine* 53.4, pp. 187–193.

Mearian, Lucas (2015). *With 15 Dollars in Radio Shack Parts, 14-Year-Old Hacks a Car*. URL: http://www.computerworld.com/article/2886830/with-15-in-radio-shackparts-14-year-old-hacks-a-car.html.

Mell, Peter, Tim Grance, et al. (2011). "The NIST definition of cloud computing". In:

Mell, Peter, Karen Scarfone, and Sasha Romanosky (2006). "Common vulnerability scoring system". In: *IEEE Security & Privacy* 4.6, pp. 85–89. DOI: 10.1109/MSP.2006.145. URL: https://ieeexplore.ieee.org/abstract/document/4042667.

Mettler, K (2019). "Somebody keeps hacking these Dallas road signs with messages about Donald Trump Bernie Sanders and Harambe the gorilla". In: *Washington, DC: WP Company*.

Miaoudakis, Andreas, Konstantinos Fysarakis, Nikolaos Petroulakis, Sofia Alexaki, George Alexandirs, Sotiris Ioannidis, George Spanoudakis, Vasilis Katos, and

Christos Verikoukis (2020). "Pairing a Circular Economy and the 5G-Enabled Internet of Things: Creating a Class of "Looping Smart Assets"". In: *IEEE Vehicular Technology Magazine* 15.3, pp. 20–31. DOI: 10.1109/MVT.2020.2991788.

Miller, Charlie and Chris Valasek (2015). "Remote exploitation of an unaltered passenger vehicle". In: *Black Hat USA* 2015.S 91.

Mitrou, Lilian (2018). "Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof'?" In: *Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR)'Artificial Intelligence-Proof*.

Mohammadi, Mehdi and Ala Al-Fuqaha (2018). "Enabling cognitive smart cities using big data and machine learning: Approaches and challenges". In: *IEEE Communications Magazine* 56.2, pp. 94–101.

Mohanty, Saraju P, Uma Choppali, and Elias Kougianos (2016). "Everything you wanted to know about smart cities: The internet of things is the backbone". In: *IEEE Consumer Electronics Magazine* 5.3, pp. 60–70. DOI: 10.1109/MCE.2016.2556879.

Mohurle, Savita and Manisha Patil (2017). "A brief study of wannacry threat: Ransomware attack 2017". In: *International Journal of Advanced Research in Computer Science* 8.5, pp. 1938–1940.

Morlet, Andrew, Jocelyn Blériot, Rob Opsomer, Mats Linder, Anina Henggeler, Alix Bluhm, and Andrea Carrera (2016a). "Intelligent assets: Unlocking the circular economy potential". In: *Ellen MacArthur Foundation*, pp. 1–25.

— (2016b). "Intelligent assets: Unlocking the circular economy potential". In: *Ellen MacArthur Foundation*, pp. 1–25.

Möser, Malte, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, et al. (2017). "An empirical analysis of traceability in the monero blockchain". In: *arXiv preprint arXiv:1704.04299*.

Nakamoto, Satoshi and A Bitcoin (2008). "A peer-to-peer electronic cash system". In: *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* 4.

Nam, Taewoo and Theresa A Pardo (2014). "The changing face of a city government: A case study of Philly311". In: *Government Information Quarterly* 31, S1–S9.

Narula, Neha (2017). *Cryptographic Vulnerabilities in IOTA*. URL: https://medium.com/@neha/cryptographic-vulnerabilities-in-iota-9a6a9ddc4367.

Neshenko, Nataliia, Christelle Nader, Elias Bou-Harb, and Borko Furht (2020). "A survey of methods supporting cyber situational awareness in the context of smart cities". In: *Journal of Big Data* 7.1, pp. 1–41.

Nessus (2022). *CVSS Scores vs. VPR*. URL: https://docs.tenable.com/nessus/Content/RiskMetrics.htm.

Ngobeni, Sipho, Hein Venter, and Ivan Burke (2010). "A forensic readiness model for wireless networks". In: *IFIP International Conference on Digital Forensics*. Springer, pp. 107–117.

Nicholls, RJ, S Hanson, C Herweijer, N Patmore, S Hallegatte, and J Corfee-Morlot. *& Muir-Wood, R.(2008). Ranking port cities with high exposure and vulnerability to climate extremes*. Tech. rep. OECD Environment Working Papers.

Nikitas, Alexandros, Ioannis Kougias, Elena Alyavina, and Eric Njoya Tchouamou (2017). "How can autonomous and connected vehicles, electromobility, BRT, hyperloop, shared use mobility and mobility-as-a-service shape transport futures for the context of smart cities?" In: *Urban Science* 1.4, p. 36.

Niras (2018). *Copenhagen Smart City*. URL: https://www.niras.dk/media/1585/kimspiegelbergsteltzer.pdf.

NIST (2020). *National Vulnerability Database*. URL: https://nvd.nist.gov.

NIST-SP – 800-150, Rev. 2. (2016). *Guide to Cyber Threat Information Sharing*. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

NIST-SP – 800 37, Rev. 2. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. URL: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

NIST-SP – 800-82, Rev. 2 (2015). *Guide to Industrial Control Systems (ICS) Security.* . URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

NIST Special Publication 800-53, Rev. 4. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. URL: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Novo, Oscar (2018). "Blockchain meets IoT: An architecture for scalable access management in IoT". In: *IEEE Internet of Things Journal* 5.2, pp. 1184–1195.

Nuñez, David, Isaac Agudo, and Javier Lopez (2017). "Proxy re-encryption: Analysis of constructions and its application to secure access delegation". In: *Journal of Network and Computer Applications* 87, pp. 193–209.

OECD (2019). *Business Models for the Circular Economy*, p. 112. DOI: https://doi.org/https://doi.org/10.1787/g2g9dd62-en. URL: https://www.oecd-ilibrary.org/content/publication/g2g9dd62-en.

Olowononi, Felix O, Danda B Rawat, and Chunmei Liu (2020). "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps". In: *IEEE Communications Surveys & Tutorials* 23.1, pp. 524–552.

Omotosho, Adebayo, Benjamin Ayemlo Haruna, and Olayemi Mikail Olaniyi (2019). "Threat modeling of internet of things health devices". In: *Journal of Applied Security Research* 14.1, pp. 106–121.

Oriwoh, Edewede, David Jazani, Gregory Epiphaniou, and Paul Sant (2013). "Internet of things forensics: Challenges and approaches". In: *9th IEEE International Conference on Collaborative computing: networking, Applications and Worksharing*. IEEE, pp. 608–615.

Pagliari, E. (2019). *Proof of Believability: the consensus algorithm of IOST. The Cryptonomist*. URL: https://en.cryptonomist.ch/2019/08/11/proof-of-believability-iost/.

Pan, Yunhe, Yun Tian, Xiaolong Liu, Dedao Gu, and Gang Hua (2016). "Urban big data and the development of city intelligence". In: *Engineering* 2.2, pp. 171–178.

Panarello, Alfonso, Nachiket Tapas, Giovanni Merlino, Francesco Longo, and Antonio Puliafito (2018). "Blockchain and iot integration: A systematic survey". In: *Sensors* 18.8, p. 2575.

Patzer, Florian, Ankush Meshram, and Maximilian Heß (2019). "Automated Incident Response for Industrial Control Systems Leveraging Software-defined Networking." In: *ICISSP*, pp. 319–327.

Petit, Jonathan, Bas Stottelaar, Michael Feiri, and Frank Kargl (2015). "Remote attacks on automated vehicles sensors: Experiments on camera and lidar". In: *Black Hat Europe* 11.2015, p. 995.

Philomin, Sebastien, Avinash Singh, Adeyemi Ikuesan, and Hein Venter (2020). "Digital forensic readiness framework for smart homes". In: *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited, pp. 627–XVIII.

Potteiger, Bradley, Goncalo Martins, and Xenofon Koutsoukos (2016). "Software and attack centric integrated threat modeling for quantitative risk assessment". In: *Proceedings of the Symposium and Bootcamp on the Science of Security*, pp. 99–108.

Pradhan, Ashis (2012). "Support vector machine-a survey". In: *International Journal of Emerging Technology and Advanced Engineering* 2.8, pp. 82–85.

Press Secretary, The White House Office of the (2013). *Presidential Policy Directive – Critical Infrastructure Security and Resilience*. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Profile, Smart (2021). *City Profile*. URL: https://www.smartcitiesworld.net/.

Pujol, F, C Manero, and T Jaffal (2018). "5G observatory—quarterly report 4". In: *Luxembourg: European Commission*.

Rajbahadur, Gopi Krishnan, Andrew J Malton, Andrew Walenstein, and Ahmed E Hassan (2018). "A survey of anomaly detection for connected vehicle cybersecurity and safety". In: *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, pp. 421–426.

Rajkumar, Ragunathan, Insup Lee, Lui Sha, and John Stankovic (2010). "Cyber-physical systems: the next computing revolution". In: *Design automation conference*. IEEE, pp. 731–736.

Rana, Nripendra P, Sunil Luthra, Sachin Kumar Mangla, Rubina Islam, Sian Roderick, and Yogesh K Dwivedi (2019). "Barriers to the development of smart cities in Indian context". In: *Information Systems Frontiers* 21.3, pp. 503–525.

Rappaport, Theodore S, Shu Sun, Rimma Mayzus, Hang Zhao, Yaniv Azar, Kevin Wang, George N Wong, Jocelyn K Schulz, Mathew Samimi, and Felix Gutierrez (2013). "Millimeter wave mobile communications for 5G cellular: It will work!" In: *IEEE access* 1, pp. 335–349.

Reyna, Ana, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz (2018). "On blockchain and its integration with IoT. Challenges and opportunities". In: *Future generation computer systems* 88, pp. 173–190.

Rinaldi, Steven M, James P Peerenboom, and Terrence K Kelly (2001). "Identifying, understanding, and analyzing critical infrastructure interdependencies". In: *IEEE control systems magazine* 21.6, pp. 11–25.

Rome, Erich, Norman Voß, A Connelly, J Carter, and J Handley (2015). *State of the Art Report (1) Urban Critical Infrastructure Systems*.

Rostami, Shahin (2020). *The 2018-2019 ENISA vulnerabilities dataset*. URL: https://github.com/enisaeu/vuln-report.

Rostami, Shahin, Agnieszka Kleszcz, Daniel Dimanov, and Vasilios Katos (2020). "A Machine Learning Approach to Dataset Imputation for Software Vulnerabilities". In: *International Conference on Multimedia Communications, Services and Security*. Springer, pp. 25–36.

Rueda, Salvador (2019). "Superblocks for the design of new cities and renovation of existing ones: Barcelona's case". In: *Integrating human health into urban and transport planning*. Springer, pp. 135–153.

Russell, Stuart and Peter Norvig (2002). "Artificial intelligence: a modern approach". In:

s5068096A (2021). *Source code of the IoTA-ITS testbed*. URL: https://github.com/s5068096-A/IoTA-ITS-testbed.

Sabella, Dario, Alessandro Vaillant, Pekka Kuure, Uwe Rauschenbach, and Fabio Giust (2016). "Mobile-edge computing architecture: The role of MEC in the Internet of Things". In: *IEEE Consumer Electronics Magazine* 5.4, pp. 84–91.

Scarfone, Karen and Peter Mell (2010). "The common configuration scoring system (ccss): Metrics for software security configuration vulnerabilities". In: *NIST interagency report* 7502.

Schuurman, Dimitri, Bastiaan Baccarne, Lieven De Marez, and Peter Mechant (2012). "Smart ideas for smart cities: Investigating crowdsourcing for generating and selecting ideas for ICT innovation in a city context". In: *Journal of theoretical and applied electronic commerce research* 7.3, pp. 49–62.

Shae, Zonyin and Jeffrey JP Tsai (2017). "On the design of a blockchain platform for clinical trial and precision medicine". In: *2017 IEEE 37th international conference on distributed computing systems (ICDCS)*. IEEE, pp. 1972–1980.

Sharma, Pradip Kumar, Seo Yeon Moon, and Jong Hyuk Park (2017). "Block-VN: A distributed blockchain based vehicular network architecture in smart city". In: *Journal of information processing systems* 13.1, pp. 184–195.

Sharma, Toshendra Kumar (2019). *EOS vs. Ethereum: A detailed Comparison*. URL: https://www.blockchain-council.org/blockchain/eos-vs-ethereum-a-detailed-comparison/.

Sicari, Sabrina, Alessandra Rizzardi, and Alberto Coen-Porisini (2020). "5G in the internet of things era: an overview on security and privacy challenges". In: *Computer Networks* 179, p. 107345.

Silva, Bhagya Nathali, Murad Khan, and Kijun Han (2018). "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities". In: *Sustainable Cities and Society* 38.1, pp. 697–713. DOI: 10.1016/j.scs.2018.01.053. URL: https://www.sciencedirect.com/science/article/pii/.

Simmons, Jake (2019). *IOTA network down for 15 hours – What happened?* URL: https://www.crypto-news-flash.com/iota-network-down-for-15-hours-what-happened/.

Singh, Ak Ashakumar and K Surchandra Singh (2012). "Network Threat Ratings in Conventional DREAD Model Using Fuzzy Logic". In: *International Journal of Computer Science Issues (IJCSI)* 9.1, p. 478.

Singh, Jaspreet (2019). *Distributed Non Fungible Tokens (DNFT)*. URL: https://github.com/Quillhash/dnfts.

Spanos, Georgios and Lefteris Angelis (2015). "Impact Metrics of Security Vulnerabilities: Analysis and Weighing". In: *Information Security Journal: A Global Perspective* 24.1-3, pp. 57–71. DOI: 10.1080/19393555.2015.1051675. URL: https://doi.org/10.1080/19393555.2015.1051675.

Statistics-How-To (2021). *Hierarchical Clustering / Dendrogram: Simple Definition, Examples*. URL: https://www.statisticshowto.com/hierarchical-clustering/#google_vignette.

Stellios, Ioannis, Panayiotis Kotzanikolaou, Mihalis Psarakis, Cristina Alcaraz, and Javier Lopez (2018). "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services". In: *IEEE Communications Surveys & Tutorials* 20.4, pp. 3453–3495.

Talari, Saber, Miadreza Shafie-Khah, Pierluigi Siano, Vincenzo Loia, Aurelio Tommasetti, and João PS Catalão (2017). "A review of smart cities based on the internet of things concept". In: *Energies* 10.4, p. 421.

Tanaka, Kenji, Kosuke Nagakubo, and Rikiya Abe (2017). "Blockchain-based electricity trading with Digitalgrid router". In: *2017 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*. IEEE, pp. 201–202.

Team, C (2015). "Common vulnerability scoring system v3. 0: Specification document". In: *First. org*.

Telecompaper (2021). *Cape Verde to set up computer security incident response team*. URL: https://www.telecompaper.com/news/cape-verde-to-set-up-computer-security-incident-response-team--1370871.

Teli, Maurizio, Silvia Bordin, María Menéndez Blanco, Giusi Orabona, and Antonella De Angeli (2015). "Public design of digital commons in urban places: a case study". In: *International Journal of Human-Computer Studies* 81, pp. 17–30.

Toyoda, Kentaroh, P Takis Mathiopoulos, Iwao Sasase, and Tomoaki Ohtsuki (2017). "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain". In: *IEEE access* 5, pp. 17465–17477.

Tripathi, Abhishek (2016). "Internet of Things: The key enabler of smart cities in India". In: *International Journal of Business Administration and Management Research* 2.2, pp. 15–19.

Tukker, Arnold (2004). "Eight types of product–service system: eight ways to sustainability? Experiences from SusProNet". In: *Business strategy and the environment* 13.4, pp. 246–260.

Vallance, Chris (2015). *Car Hack Uses Digital-Radio Broadcasts to Seize Control (BBC)*. URL: https://www.bbc.co.uk/news/technology-33622298.

Vayona, Anastasia and Giorgos Demetriou (2020). "Towards An Operating Model For Attribution In Circular Economy". In: *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, pp. 490–495.

Wachenfeld, Walther, Hermann Winner, J Chris Gerdes, Barbara Lenz, Markus Maurer, Sven Beiker, Eva Fraedrich, and Thomas Winkle (2016). "Use cases for autonomous driving". In: *Autonomous driving*. Springer, pp. 9–37.

Wang, Paul, Amjad Ali, and William Kelly (2015). "Data security and threat modeling for smart city infrastructure". In: *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. IEEE, pp. 1–6. DOI: 10.1109/SSIC.2015.7245322.

WCCD (2018). *Global Cities Registry for WCCD ISO 37120 Series*. URL: https://www.dataforcities.org/global-cities-registry.

Wei, Zhongxiang, Xu Zhu, Sumei Sun, Yi Huang, Ahmed Al-Tahmeesschi, and Yufei Jiang (2016). "Energy-efficiency of millimeter-wave full-duplex relaying systems: Challenges and solutions". In: *IEEE Access* 4, pp. 4848–4860.

Williams, J (2012). "ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evi-dence". In: *Groot-Brittanië: Association of Chief Police Officers*.

Williams-Shaw, Sydni (2019). *How to build an incident response playbook*. URL: https://swimlane.com/blog/incident-response-playbook.

Wüst, Karl and Arthur Gervais (2017). *Do you need a Blockchain?* Cryptology ePrint Archive, Report 2017/375. https://eprint.iacr.org/2017/375.

Xie, Junfeng, Helen Tang, Tao Huang, F Richard Yu, Renchao Xie, Jiang Liu, and Yunjie Liu (2019). "A survey of blockchain technology applied to smart cities: Research issues and challenges". In: *IEEE Communications Surveys & Tutorials* 21.3, pp. 2794–2830.

Xiong, Zehui, Yang Zhang, Dusit Niyato, Ping Wang, and Zhu Han (2017). "When mobile blockchain meets edge computing". In: *arXiv preprint arXiv:1711.05938*.

XM-CYBER. *What is Common Vulnerability Scoring System?* URL: https://www.xmcyber.com/common-vulnerability-scoring-system/.

Xu, Brent, Dhruv Luthra, Zak Cole, and Nate Blakely (2018). "Eos: An architectural, performance, and economic analysis". In: *Retrieved June* 11, p. 2019.

Yadron, Danny and Dan Tynan (2016). *Tesla Driver Dies in First Fatal Crash While Using Autopilot Mode (The Guardian)*. URL: https://www.theguardian.com/

technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk.

Yang, Changsong, Xiaofeng Chen, and Yang Xiang (2018). "Blockchain-based publicly verifiable data deletion scheme for cloud storage". In: *Journal of Network and Computer Applications* 103, pp. 185–193.

Yang, Fan, Wei Zhou, QingQing Wu, Rui Long, Neal N Xiong, and Meiqi Zhou (2019). "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism". In: *IEEE Access* 7, pp. 118541–118555.

Yavuz, Emre, Ali Kaan Koç, Umut Can Çabuk, and Gökhan Dalkılıç (2018). "Towards secure e-voting using ethereum blockchain". In: *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE, pp. 1–7.

Yeh, Hsiaoping (2017). "The effects of successful ICT-based smart city services: From citizens' perspectives". In: *Government Information Quarterly* 34.3, pp. 556–565.

York, Richard and Julius Alexander McGee (2016). "Understanding the Jevons paradox". In: *Environmental Sociology* 2.1, pp. 77–87.

Yuan, Yong and Fei-Yue Wang (2016). "Towards blockchain-based intelligent transportation systems". In: *2016 IEEE 19th international conference on intelligent transportation systems (ITSC)*. IEEE, pp. 2663–2668.

Yue, Xiao, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang (2016). "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control". In: *Journal of medical systems* 40.10, pp. 1–8.

Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang (2017). "An overview of blockchain technology: Architecture, consensus, and future trends". In: *2017 IEEE international congress on big data (BigData congress)*. IEEE, pp. 557–564.

Zygiaris, Sotiris (2013). "Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems". In: *Journal of the knowledge economy* 4.2, pp. 217–231.

Appendix A

Performance Evaluation of PoC

A.1 Performance Evaluation

The six connected nodes to the message broker are presented in Figure A.1. *smart-car* is an ESP-32 connected to the message broker. In addition, it publishes messages to the message broker at a rate of 10 bytes per second. *guest* is a VM that runs the script that reads from the broker and inserts transactions into the Tangles. Script receives 60 bytes per second, published by the smart car. There are five connected vehicles in total that are displayed in this overview.

Furthermore, the queue created by the incoming and outcoming MQTT messages are presented in Figure A.2. For the needs of this research, the message rates per queue is defined at 2.6 seconds for all the five ESP-32 "smart-cars". As such, all the messages are delivered to the script every 2.6 seconds, as well.

In Figure A.3, one hour time frame slot is presented. The yellow line indicates the published messages and the green line indicates the delivered ones.

There are periods of steady traffic when data is delivered and received at the same rate. However, there are times when data is not delivered by the devices, resulting in no messages being received in the subscription script's queue.

In addition, there are time slots, when published messages are more than the subscribed ones. Data communication issues, such as packet loss, may cause fluctuations in traffic. These issues may affect the data flow, plotted on a graph.

The messages that have not been received by the RabbitMQ may be stored by the devices locally, and re transmitted.

In a real world application, smart vehicles will not send messages based on a specific rate, but only when it is essential, for example, only when it is close to other vehicles or traffic furniture.

Overview			Details			Network		+/-
Name	**User name**	**State**	**SSL / TLS**	**Protocol**	**Channels**	**From client**	**To client**	
127.0.0.1:45112	guest	running	○	MQTT 3.1.1	1	0 B/s	60 B/s	
192.168.0.24:65326	smart-car	running	○	MQTT 3.1.1	1	10 iB/s	0 iB/s	
192.168.0.38:53361	smart-car2	running	○	MQTT 3.1.1	1	10 iB/s	0 iB/s	
192.168.0.39:60626	smart-car3	running	○	MQTT 3.1.1	1	10 B/s	0 B/s	
192.168.0.42:53338	smart-car4	running	○	MQTT 3.1.1	1	15 iB/s	0 iB/s	
192.168.0.44:59980	smart-car5	running	○	MQTT 3.1.1	1	15 iB/s	0 iB/s	

FIGURE A.1: Overview of connected devices

Overview				Messages			Message rates			+/-
Name	**Type**	Features	**State**	**Ready**	**Unacked**	**Total**	**incoming**	**deliver / get**	**ack**	
mqtt-subscription-mqttjs_baeb4296qos0	classic	AD	running	0	0	0	2.6/s	2.6/s	0.00/s	

FIGURE A.2: The MQTT messages queue that are published and subscribed

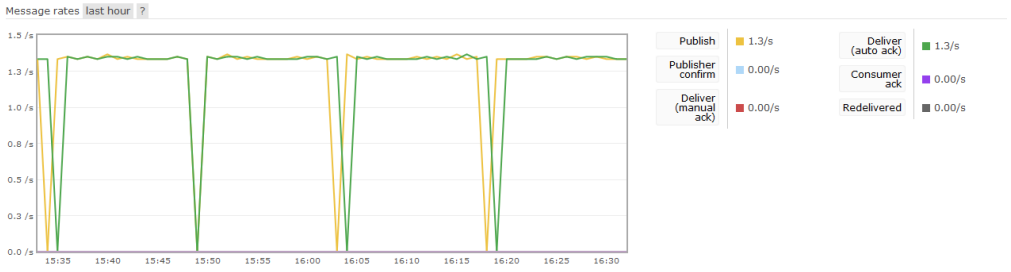

FIGURE A.3: 1 hour time slot capture of messages sent from IoT devices to Tangle

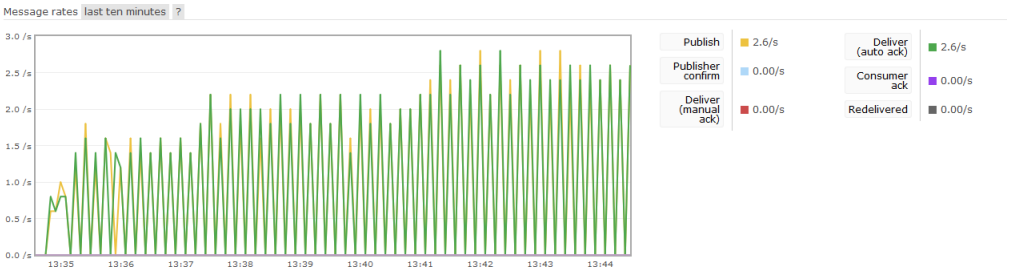

FIGURE A.4: A 10-minute time slot capture of a message sent from an IoT device to the Tangle

There may be situations where cars are in traffic, generating an influx of transactions at a higher rate. These messages will be queued until they are ready to be processed and delivered to the Tangle.

A view of ten minutes time slot is presented in Figure A.4, which depicts better the inconsistencies that exist when publishing and delivering messages. It is also important to note that the rate of data flow is measured in seconds, which could directly correlate to the current speed of travel on a particular route. The rate of reaching traffic structures by a vehicle depends on the travel in miles per hour.