# Distributed and Biometric Signature-Based Identity Proofing System for the Maritime Sector

Taylan Akbas
*Dept. of Computer Engineering*
*School of Eng., Yasar University*
Izmir, Turkiye
taylanakbas@protonmail.com
0000-0003-1287-7147

Ahmet Koltuksuz
*Dept. of Computer Engineering*
*School of Eng. Yasar University*
Izmir, Turkiye
ahmet.koltuksuz@yasar.edu.tr
0000-0002-0710-2988

Cagatay Yucel
*Dept. of Computing and Informatics*
*Bournemouth University*
Fern Barrow, Poole BH12 5BB, UK
cyucel@bournemouth.ac.uk
0000-0002-4901-5954

2023 8th International Conference on Computer Science and Engineering (UBMK) | 979-8-3503-4081-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/UBMK59864.2023.10286659

***Abstract*—The maritime sector is an industry that faces significant and various challenges related to cyber security and data management, such as fraud and user authentication. Therefore, there is a need for a secure solution that can effectively manage data transactions while resolving digital identity. A biometric signature application in blockchain for fighting fraud and fake identities may provide a solution in the maritime sector. This research proposes a biometric signature and an IPFS network-blockchain framework to address these challenges. This paper also discusses the proposed framework's cyber security challenges that threaten behavioral biometric security.**

***Keywords—behavioral biometrics, biometric signature, blockchain, distributed ledger, hyper ledger, smart contract, private blockchain, maritime cyber security***

## I. INTRODUCTION

Delivering rapid and accurate identity verification becomes crucial as the world transforms into a gigantic digital country. Identity proofing verifies a subject's association with a real-world identity [1]. Regarding privacy and security, new requirements are emerging against the threats such as fake identities and AI-backed attacks.

Since the beginning of the contemporary digital society in the early sixties, the digital identity model and its verification methods have evolved to deliver more reliable solutions. Those efforts started with passwords. Passwords have been the most used method of online authentication. A subject creates a secret, simple password that no one else knows and uses it for digital authentication whenever and wherever it is needed. To generate a strong password has always been another issue; this is where cryptography has come into play. Although cryptography and authentication are different concepts, they have a close link. The Key Derivation Functions (KDF) are cryptographic algorithms that generate secret keys from an arcanum value, such as the master key or a password using either a hash function or a symmetrical cryptosystem. Robert Morris invented the first KDF algorithm, called crypt, in the 1970s [2]. While cryptographic needs evolved, other technologies emerged, such as Public Key Cryptography, Two-Factor Authentication (2FA), One-Time-Password (OTP), Multi-Factor Authentication, and Biometrics.

Biometric authentication dates back to a fingerprint record Chinese traders took during the 14th century for identification purposes. It has evolved into unique biological characteristics of individual-driven identity proofing [3]. These biological recognition methods branch into two types; physical and behavioral. A hardware system or a human can acquire physical biometric recognition by accepting a retinal pattern, voice, palm pattern, or fingerprint as input. On the other hand, behavioral biometric authentication identifies the pattern of any behavioral attribute generated uniquely and only in one-time, such as the movements of fingers while signing a name on a touch-sensitive screen. This property makes behavioral biometrics very practical and valuable. Thus, many banks, hospitals, and companies accept the biometric signature and various institutions worldwide since it is straightforward and traditional. The maritime sector is one of the vital institutions in which biometric systems are essential for identity proofing. The fraud-fighting for the Integrity of information in the maritime sector, along with the cyber security and efficiency of data management, thus has the utmost importance.

The maritime industry has cast specific requirements over the communication channels of the domain where centralized applications became the bottlenecks. Consider the case of a ship excursing through diverse ports where each central authority requires complex and disparate communication regulations and data specifications for authentication. In addition to the requirements, the state-of-the-art systems for IT network systems of ports are not designed with security in mind [4]. A modular encapsulating architecture providing flexibility through smart contracts gains significance in such a case. No one can adequately stress the importance of the maritime sector for worldwide trade. Simply put, there would almost be no worldwide trade without naval trade. Therefore, simple or complicated, any cyber threat is a significant threat in this sector. Some organizations like International Maritime Organization (IMO) and The Baltic and International Maritime Council (BIMCO) have declared the vulnerable systems in shipping as "bridge systems, cargo handling and management systems, propulsion and machinery management and power control systems, access control systems, passenger servicing, and management systems, passenger facing public networks, administrative and crew welfare systems, and communication systems" [5] [6]. The port is one of the main compounds of any digitalized maritime shipping system. The port is a critical infrastructure without which all the docking operations would cease. A cyber-attack on the electrical system that powers everything in the port may mean direct service and financial loss. Many computers, operating systems, and application software constitute the pier's superstructure for managerial functions. As such, there are numerous vulnerabilities, especially when all those systems are interconnected and, thus, have access to the Internet. European Union Agency for Cybersecurity (ENISA) analyzed the cybersecurity in the maritime sector [7] and came forward with the "Good practices for cybersecurity in the maritime sector" in port cybersecurity [8]. The cyber threats target the triad of Confidentiality, Integrity, and and Availability of information by different attack vectors in maritime systems. In another way of defining the situation, along with the advances in digitalization, the maritime sector has been having its share of cyber-attacks in terms of integrity

breaches leading to fraud, fake identification creating authentication issues, malware, ransomware, and unauthorized access, to name a few. This paper's biometric approach is a new defense tool that will be a powerful agent in fighting fraud and fake identification in the maritime sector. While the proposed architecture could efficiently be utilized for other sectors, the requirements, threats, and vulnerabilities specified for the maritime sector render this application a right fit for the industry. Therefore, this proposed distributed biometric authenticity framework, which encompasses the biometric signatures for identity proofing on blockchain methodology, will directly contribute to the Integrity of information in the maritime sector.

The rationale of this paper is as follows: Section two underlines our motivation and contributions. Section three summarizes the early works. While section four discusses the anatomy of biometric signatures as the methodology employed for this research, section five covers the ledgers from the confidentiality perspective by enumerating the distributed ledger technology. Section six presents the heart and soul of this research by proposing a new cyber security framework based on biometric signature and blockchain on the IPFS Network for the maritime sector. Section seven evaluates the framework from a counter angle to delineate the vulnerabilities and weaknesses in the proposed architecture. The results are presented in section eight. Finally, section nine is the conclusion section, and future work is also defined here.

## II. MOTIVATION AND CONTRIBUTION

The main objective of this study is to provide a new framework model for fighting fraud and maintaining safe and cyber-secure authentication in the maritime sector through biometric signature systems. Towards that end, our proposed model is a distributed and biometric signature-based identity proofing system. As such, these frameworks may be classified as authenticity enforcer systems, directly contributing to the Integrity of the information. However, our contribution is not limited to the Integrity of information. Standard blockchain technology would ensure the security and immutability of data, and biometric signatures would provide a secure and unique method of verifying identities. Moreover, since our proposed system utilizes the IPFS network, the IPFS networking would enable decentralized and efficient data storage and sharing. Therefore, the proposed framework will also contribute to information security and data management in the maritime sector. Thus, the two main pillars of cybersecurity, Confidentiality and the Integrity of information, would be maintained hard by the contributions of this study.

## III. SUMMARY OF THE RELATED WORKS

Beyond finding widespread use, a biometric signature is also studied extensively in academia. There are many publications over which, some critical of them summarized here. Miguel-Hortado [9] worked on the attributes of the biometric signatures, and Paez et al. [10] proposed an electronic identification document system on the blockchain due to increased security measures. Furthermore, the use of blockchain to store data on biometric templates has been discussed by Delgado-Mohatar et al. [11]. Tolasana et al. [12] recommend the application of the biometric signature with a finger instead of a stylus on smartphones. On the other hand, Bibi et al. [13] propose online and offline biometric signature verification systems using taxonomic classification models. Since the structure of the signature changes very quickly because of its fluid, dynamic nature and modality, ISO has standardized the biometric signature creation as standards of ISO/IEC 19794/7 and ISO/IEC 19794/11 [14] [15]. Koltuksuz [16] extensively studied the application of these standards of biometric signature creation on touch-sensitive screens.

## IV. METHODOLOGY: THE NATURE OF BIOMETRIC SIGNATURES

A signature is the person's writing the name, surname, or pseudonym on the paper with a hand to prove and to bind the person to a document in whole or in part. Traditionally, the signature, signed by handwriting, not only provides a unique identification of the signer but also serves as direct proof of the permanent link between the signer and the document. In a digital world, however, the signature has wholly changed in structure, if not for functionality. The digital signature, introduced in the 21st century by cryptography, has emerged as the most striking form of this change. The biometric signature has also come to the fore due to the digitization of the signature environment. A biometric signature is used for behavioral biometric recognition by placing the subject's handwriting signature on any touch-sensitive screen. From an image processing view, each biometric signature, depending on its length, comprises nearly 400 points. Each point, in turn, may have 20 specific features which, when extracted and combined with the other same type of 20 features extracted from other 400 points, completes the biometric signature. Some of the unique features extracted from each of those 400 points can be listed as "The pressure of the pen," "The altitude angle of the pen," "The velocity of the pen in the x and y coordinates," and "The absolute speed and the acceleration of the pen." Those unique feature values are obtained from each point of the biometric signature simultaneously by the computing system as the signee performs the signature on the touch-sensitive screen. This complex data structure makes the biometric signature easy to change by the owner but impossible to forge. Furthermore, when cryptographic protections are added, even the signee cannot deny their hand-created biometric signature, let alone forgery attempts by outsiders.

## V. THE LEDGERS FOR CONFIDENTIALITY

Since earlier civilizations, ledgers have been used to record various items, particularly assets such as money and property. Even though we know distributed ledgers from Satoshi's Bitcoin, they can be traced back to the Roman Empire and are primarily involved in all contemporary banking procedures. A distributed ledger is a database storing information or transaction records across a secure network through multiple locations. Each ledger within the network has an identical copy of the documents. According to the network policies, a registered and validated person or anyone within the organization can modify the ledger entries. However, any changes on the ledger cause modification on every database instance. Such transactions can be completed in seconds or hours according to the physical and logical properties of the components of the distributed ledger. The security and validity of the assets in the ledger are maintained cryptographically through keys and digital signatures. The

terms distributed ledger technology (DLT) and blockchain are frequently misused.

Contrary to general belief, blockchain is another sub-category of distributed ledgers. A blockchain ledger has a specific architecture for its data. Blocks organize a blockchain in a consecutive order according to the time points at which the network's validators approve transactions. Consensus algorithms allow validators to agree on prudent decisions like putting off legal transactions. The rapid developments on the World Wide Web have created the necessity of distributing ledgers, hence the DLT. The third generation of the World Wide Web is not just meant for people to people and people to software, but also software to software. Blockchain-based Web 3.0 offers practical solutions to preserving the security and reliability of the Internet and constructing the infrastructure for data interchange, storage, and transactions. It also brings actual ownership and verifiability. The varied applications of DLTs may be grouped into three as follows.

### *A. Smart Contract*

Szabo introduced the 'Smart contract' concept in 1996 [17]. Unlike a traditional contract, a smart contract exists in a digital format, and it defines complex protocols and rules around an agreement and automatically enforces those obligations. However, making transactions on a smart contract with an authentic biometric signature brings the problem of storing all that sensitive biometric information. In this case, decentralized infrastructure and capabilities can become a haven for sensitive data. In 2014, Buterin, the inventor of Ethereum, defined 'scriptable smart contracts' technology. These contracts, defined as 'cryptographic "boxes" that contain value and only unlock it if certain conditions are met, can also be built on top of the Ethereum platform [18]. With the rise of smart contracts, decentralized applications, abbreviated as Dapps, have emerged. Despite several other blockchains publicly generated to serve Dapps, Ethereum is the most powerful platform for developing and executing smart contracts, allowing the developer to build decentralized solutions for exceptional cases. While the demand for blockchain applications from public and private organizations increased, several solutions have emerged to ensure block data privacy. Privacy is a vital concern of blockchain technology because of premising validation of each transaction between all the participants. This sharing should be done in an agreement process called consensus. However, delivering information to various parties for them to validate transactions creates an issue if that data must also be kept private.

### *B. Private Blockchain*

There are four types of blockchain technology: public, private, consortium, and hybrid. In our case, private blockchains are owned by a single organization and can be defined as partially decentralized networks. It saves the usage of many resources while the network only allows specific subject-engaged transactions. In addition, its isolated architecture lowers transaction fees, and the organization's regulatory system restricts reviewing and auditing rights. Use cases of private blockchain include different implementations of a 'smart contract' to serve decentralized infrastructure for financial services, governmental services, healthcare, and insurance. Hyperledger Fabric is a private blockchain technology that provides a flexible and modular framework for building enterprise-grade distributed ledger applications. It is an open-source platform that allows organizations to create and deploy their blockchain networks with custom consensus mechanisms, membership services, and smart contract logic. In addition, It is designed to support private and confidential transactions, making it well-suited for use cases where privacy, security, and scalability are essential. One of the critical features of Hyperledger Fabric is its modular architecture, which enables users to choose and customize different components of the framework to suit their specific needs. For example, Fabric supports pluggable consensus mechanisms, allowing users to select between different algorithms such as Raft or Kafka. It also supports smart contracts written in various programming languages like Go, Java, and Node.js. This flexibility enables organizations to build blockchain applications tailored to their unique requirements, whether for supply chain management, identity management, or financial services.

### *C. Inter Planetary File Storage System (IPFS)*

IPFS is a peer-to-peer hypermedia protocol that aims to store and access data and applications invented by Bennet [19]. IPFS uses a unique content identifier (CID) to identify the content address and retrieve this content from several peers and nodes. IPFS and other distributed content delivery networks (CDNs) use distributed hash tables (DHT). Under IPFS, the files and directories between different nodes are managed through directed acyclic graphs (DAG), specifically, Merkle-DAGs, which have distinct properties like Content Addressing, Tamper Resistance, and Deduplication [19]. To build a Merkle- DAG representation of a file's content, IPFS first splits this file into blocks. Then, different file parts can come from various sources or nodes and can be authenticated quickly [20]. Although IPFS is a low-latency network that can distribute data and applications, it seriously prohibits its utilization due to its requirement of sharing private data on a distributed network, thus allowing public access to those sensitive data.

## VI. A PROPOSED CYBER SECURITY FRAMEWORK FOR THE MARITIME SECTOR

The maritime sector is an industry that faces significant challenges related to security and data management. Abdallah et al. [21] delineate how the blockchain may improve performance in the maritime sector. One of the study's critical findings is that employing blockchain for fighting fraud is essential. Our below-proposed framework involves using a biometric signature and a blockchain on the IPFS network to address the many-faced challenges of fraud and authentication. While blockchain technology would ensure the security and immutability of data, biometric signatures would provide a secure and unique method of verifying identities. In addition, the IPFS network would enable decentralized and efficient data storage and sharing. Therefore, the proposed solution has the potential to significantly enhance information security and data management in the maritime sector, leading to increased efficiency and reduced costs. The proposed model has different components for different tasks. This model is just a high-level architecture design and does not have all the actors

and their functions to be implemented in the system environment. Details of each component are discussed below.

### A. Blockchain Network

A ship visiting various ports could be requested to fulfill necessary forms *en route*. Central authorities can have different and complex regulations applied for those ports. Each organization on the network must keep ownership rights of its data while transacting on a shared channel. We choose Hyperledger Fabric (HLF) as a private and permissioned blockchain infrastructure that offers a modular architecture delineating roles between infrastructure nodes, execution of Smart Contracts, and configurable consensus and membership services [22]. The network is divided into two main types of nodes: Peers and orderers. Peers maintain a copy of the ledger and execute transactions, while orderers manage the ordering of transactions and ensure consistency across all peers. It is designed to be permissioned, meaning participants must be authenticated and authorized to join the network. Participants can join channels, which are sub-networks within the main network, to conduct private and confidential transactions with other authorized participants. It also uses a modular architecture that allows users to customize different network components, including the consensus mechanism, membership services, and smart contract logic. The framework also supports pluggable consensus mechanisms, enabling users to choose the most appropriate algorithm for their use case. Despite many distributed blockchains, such as Bitcoin and Ethereum, relying on probabilistic consensus algorithms, the HLF network relies on a deterministic consensus algorithm. Thus, any block the peer validates is guaranteed to be final and correct. Organizations own their Certificate Authority (CA) for managing user certificates. Participants in a workflow use the CA to sign every request. Each CA component is configured as an intermediate CA and signed by an offline CA to protect the root of trust. This offline CA is configured to store private keys in an HSM via the PKCS11 interface.

### B. Private IPFS Network

We need a private network for our maritime workflow to store contracts with biometric signatures and other additional proofs such as ISO 19794-7 complying with biometric signatures, the image of the biometric signature, and the contract itself. When adding a file to public IPFS, it gives back a hash. With this hash information, users and organizations can access the related file. These hashes can be considered private links as long as keeping the hash information confidential. Due to technical and legal limitations, this level of privacy is not appropriate for organizations. On the other hand, a private IPFS network allows only connecting to other peers with a private key. As a result, each peer determines which other peer it will join. Nodes in that network do not respond to interactions from nodes in different networks. A high-tech Web3 concept, the IPFS cluster is highly recommended for easier management of multiple nodes on the network [19]. This structure gives the capability of smart pinning prioritization and balanced allocation. In this way, peers can track pin lifetime. Also, it has built-in permissions set to support peers. Since the IPFS network is designed as a P2P network, all participants must run their own IPFS nodes. Nevertheless, this transaction causes a decrease in usability and an increase in operating costs. For this reason, another concept, IPFS Gateway, is coming into action. The primary usage of IPFS gateways is to allow users to access IPFS content without installing any additional software or using command-line interfaces. By using an IPFS gateway, users can access content stored on the IPFS network.

### C. Cryptographic Key Management Service (CKMS)

The key management follows a lifecycle of operations on API keys, encryption keys, passwords, and certificates. A cryptographic key follows a lifecycle that involves the generation, distribution, usage, storage, rotation, backup and recovery, revocation, and destruction. CKMS provides encryption, authentication, and authorization methods. Secrets and other sensitive data can be tightly controlled and securely managed using HTTP API; thus, all are auditable. By integrating CKMS, organizations can improve the security of their system.

### D. Client Application

The Client Application service is a crucial component of the proposed model for enhancing security and data management in the maritime sector. As the maritime industry is subject to various security challenges, such as piracy, terrorism, and cyber-attacks, there is a need for a robust and secure solution that can effectively manage data and transactions. The service is designed to provide a secure and efficient means of interacting with the blockchain and accessing maritime sector services. The blockchain, a distributed and decentralized database, provides a secure and transparent means of managing data and transactions, ensuring data integrity, and preventing unauthorized access. The Client App would interact with the blockchain to access, store, and update data related to the maritime sector, such as shipping information, cargo manifests, and port operations. In addition, the Client App service would utilize biometric authentication to ensure secure access to the application and its services. Biometric signatures are used for verifying identities and would provide a robust means of preventing unauthorized access to the application and the blockchain. Furthermore, the Client App service would utilize the IPFS network to store and share data decentralized and efficiently. The Client App service would also have a user-friendly interface allowing clients to easily access and manage their data, view transaction history, and perform other necessary functions. The interface would be designed to be intuitive and easy to use, allowing clients to access the information quickly and efficiently they need.

## VII. THE VULNERABILITY ANALYSES OF THE PROPOSED FRAMEWORK

We have utilized the MITRE Common Vulnerabilities and Exposures (CVE) database [23], MITRE Common Weakness Enumeration (CWE) database [24], and NIST National Vulnerability Database (NVD) [25] to explore the nature of the cyber-attacks affecting our proposed system. Table 1 below shows the already-identified vulnerabilities by those databases.

TABLE I. THE KNOWN VULNERABILITIES OF THE PROPOSED FRAMEWORK.

| # | CVE Number | Software | Description |
|---|---|---|---|
| 1 | CVE-2022-31121<br>CVE-2022-36023<br>CVE-2021-43669<br>CVE-2021-43667 | Hyperledger Fabric | Malformed input – yielding to the crash of the system. |
| 2 | CVE-2022-45196 | Hyperledger Fabric | By leveraging this vulnerability, a DDoS attack is possible. |
| 3 | CVE-2022-47933<br>CVE-2020-10937<br>CVE-2020-26279<br>CVE-2020-26283 | IPFS | Potential name takeover, overwriting, and downgrading for the CID entries. |
| 4 | CVE-2022-23495<br>CVE-2023-23631<br>CVE-2023-23626<br>CVE-2023-23625 | Go-merkledag<br>Go-unixfsnode | By leveraging manually crafted inputs to the implementations, an attacker can cause the system to go into a panic state – which might end up with memory leaks or potential attacks on availability. |

## VIII. RESULTS AND DISCUSSION

The above-defined vulnerabilities in the proposed model have all been mitigated with the current stable versions. Nevertheless, these vulnerabilities unveil potential attacks and attack vectors over the orchestrated system. We have patched four vulnerability groups that were detected in our proposed approach with risk mitigation measures as suggested by MITRE's CVE, CWE, and NIST's NVD:

*1) Malformed input:* We have utilized an automated input validation software as a code writing practice encapsulating all the open-source software we have integrated into our system. The software checks for the missing consensus messages and returns an error if the message is missing.

*2) Distributed Denial of Service Attacks*: This vulnerability is caused by Hyperledger Fabric, through which a denial of service or orderer crash attack is possible. We have implemented a locking mechanism and a check for existing names to ensure availability.

*3) Attacks towards the Integrity of the IPFS systems*: As the IPFS system requires dynamic naming conventions for when the file has changed, or a new entry has been issued, we have implemented a dynamic naming structure.

*4) Manuel Crafted Input Leveraging:* All the inputs by the users for setting a new 'CidBuilder' are sanitized through a software mechanism. A similar sanitization protocol was applied to 'Tsize' as well.

## IX. CONCLUSION AND FUTURE WORK

A distributed and biometric signature-based identity proofing system is proposed for fighting fraud and maintaining safe and cyber-secure authentication in the maritime sector. Based on an IPFS network, this proposed framework will create and maintain decentralized data storage and sharing, contributing to information security and efficient data management in the maritime sector.

Along with this contribution, a biometric signature application in blockchain, coupled with enhanced cryptographic security measures, may pave the way for the Confidentiality and Integrity of information, which are critical issues in the maritime sector.

The proposed system integrates different software subsystems and, thus, needs meticulous orchestration for efficiency and cyber security. Towards that end, the whole system has undergone scrutiny of performance and vulnerability analysis. The found vulnerabilities patched, and the new security testing phase, driven by complete new test cases and scenarios before the actual deployment, is what we consider very near future work.

## ACKNOWLEDGMENT

The authors thank the anonymous referees for their valuable contributions in making this research paper precise and presented in superior quality.

This work was supported within the scope of the scientific research project, which was accepted by the Project Evaluation Commission of Yasar University under the project number and title of "BAP104_ Yaşar Üniversitesi Lisansüstü Eğitim Enstitüsü (LEE) İçin Geliştirilmiş, Kriptografik Güvenlik Mimarisiyle Korunan, Yapay Zekâ Destekli, Biyometrik İmzalı, Blok Zinciri Yapılı Evrak Arşiv Sistemi (BIOSEC)."

## REFERENCES

[1] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines: revision 3, NIST Special Publication 800-63-3," Gaithersburg, MD, Jun. 2017. doi: 10.6028/NIST.SP.800-63-3.

[2] R. Morris and K. Thompson, "Password Security: A Case History," Commun ACM, vol. 22, no. 11, pp. 594–597, 1979, Accessed: Mar. 22, 2023. [Online]. Available: https://www.yumpu.com/en/document/view/25513412/password-security-a-case-history-acm-digital-library

[3] D. Bhattacharyya, R. Ranjan, F. Alisherov, and M. Choi, "Biometric Authentication: A Review," International Journal of u- and e- Service, Science and Technology, vol. 2, no. 3, pp. 13–28, 2009, Accessed: Mar. 22, 2023. [Online]. Available: https://www.researchgate.net/publication/46189709

[4] F. Alpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity Challenges in the F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity hallenges in the Maritime Sector," Network, vol. 2, pp. 123–138, 2022, https:// doi.org/10.3390/network2010009.

[5] International Maritime Organization (IMO), "Guidelines on Maritime Cyber Risk Management," London, Jul. 2017.

[6] The Baltic and International Maritime Council (BIMCO), "The Guidelines on Cyber Security Onboard Ships - Version 4," 2021. Accessed: Jun. 07, 2023. [Online]. Available: https://www.bimco.org/

[7] European Network and Information Security Agency (ENISA), "Analysis of Cyber Security Aspects in the Maritime Sector," Nov. 2011.

[8] European Union Agency for Cybersecurity (ENISA), "Port Cybersecurity, Good Practices for Cybersecurity in the Maritime Sector," Nov. 2019. doi: 10.2824/328515.

[9] O. Hurtada-Miguel, "Online Signature Verification Algorithms and Development of Signature International Standards," Universitad Carlos III de Madrid, Madrid, 2011.

[10] R. Páez, M. Pérez, G. Ramírez, J. Montes, and L. Bouvarel, "An Architecture for Biometric Electronic Identification Document System Based on Blockchain †," Future Internet, vol. 12, no. 1, p. 10, Jan. 2020, doi: 10.3390/fi12010010.

[11] O. Delgado-Mohatar, J. Fierrez, R. Tolosana, and R. Vera-Rodriguez, "Blockchain meets Biometrics: Concepts, Application to Template Protection, and Trends," ArXiv, vol. 2003.09262v1[cs.CV], Mar. 2020, doi: https://doi.org/10.48550/arXiv.2003.09262.

[12] R. Tolosana, R. Vera-Rodriguez, R. Guest, J. Fierrez, and Ortega-Garcia J., "Exploiting complexity in pen and touch-based signature biometrics.," International Journal on Document Analysis and Recognition (IJDAR), vol. 23, pp. 129–141, 2020, doi: https://doi.org/10.1007/s10032-020-00351-3.

[13] K. Bibi, S. Naz, and A. Rehman, "Biometric signature authentication using machine learning techniques: Current trends, challenges, and opportunities.," Multimed Tools Appl, vol. 79, pp. 289–340, 2020, doi: 10.1007/s11042-019-08022-0.

[14] "ISO/IEC 19794-7:2021 Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data," 2021 Accessed: Mar. 22, 2023. [Online]. Available: https://www.iso.org/standard/77910.html

[15] "ISO/IEC 19794-11:2013 Information technology — Biometric data interchange formats — Part 11: Signature/sign processed dynamic data," Feb. 2013 Accessed: Mar. 22, 2023. [Online]. Available: https://www.iso.org/standard/51824.html

[16] A. H. Koltuksuz, "The Biometric Signature as a Blockchain Application," in Blockchain Applications in IoT Ecosystem, T. Choudhury, A. Khanna, T. T. Toe, M. Khurana, and N. G. Nhu, Eds., Switzerland AG: Springer Nature, 2021, pp. 167–176. doi: https://doi.org/10.1007/978-3-030-65691-1_11.

[17] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets.," 1996. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (accessed Mar. 22, 2023).

[18] V. Buterin, "A Next Generation Smart Contract & Decentralized Application Platform," 2014. Accessed: Mar. 22, 2023. [Online]. Available: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[19] H. Benet, "IPFS - Content Addressed, Versioned, P2P File System (Draft 3)," ArXiv, Jul. 2014, doi: https://doi.org/10.48550/arXiv.1407.3561.

[20] P. Kubiak, M. Kutylowski, A. Lauks-Dutka, and M. Tabor, "Mediated Signatures - Towards Undeniability of Digital Data in Technical and Legal Framework," in Business Information Systems Workshops (LNBIP 57), W. Abramowicz, R. Tolksdorf, and K. Wecel, Eds., Berlin: Springer, May 2010, pp. 298–309.

[21] R. Abdallah, C. Bertelle, C. Duvallet, J. Besancenot, and F. Gilletta, "Blockchain Potentials in the Maritime Sector: A Survey," in Proceedings of the ICR'22 International Conference on Innovations in Computing Research, K. Daimi and A. Al Sadoon, Eds., Switzerland, AG: Springer Nature, 2022, pp. 293–309. doi: 10.1007/978-3-031-14054-9_28.

[22] E. Androulaki et al., "Hyperledger fabric," in Proceedings of the Thirteenth EuroSys Conference, New York, NY, USA: ACM, Apr. 2018, pp. 1–15. doi: 10.1145/3190508.3190538.

[23] MITRE of USA, "Common Vulnerabilities and Exposures (CVE)," 2023. https://cve.mitre.org (accessed Jun. 10, 2023).

[24] MITRE of USA, "Common Weakness Enumeration (CWE)," 2023. https://cwe.mitre.org (accessed Jun. 10, 2023).

[25] NIST of USA, "National Vulnerabilities Database (NVD)," 2023. https://nvd.nist.gov (accessed Jun. 10, 2023).