Verification and Compliance in Collaborative Processes

Oyepeju Oyekola, Lai Xu

Computing and Informatics, Bournemouth University,
Poole BH12 5BB, Bournemouth, United Kingdom
{ooyekola,lxu}@bournemouth.ac.uk

Abstract. Evidently, COVID-19 has changed our lives and is likely to make a lasting impact on our economic development and our industry and services. In the ongoing process of digital transformation in industry and services, Collaborative Networks (CNs) is required to be more efficient, productive, flexible, resilient and sustainable according to change of situations and related rules applied afterwards. Although the CN area is relatively young, it requires the previous research to be extended, i.e. business process management from dealing with processes within a single organization into processes across different organizations. In this paper, we review current business process verification and compliance research. Different tools approaches and limitations of them are compared. The further research issues and potential solutions of business process verification and compliance check are discussed in the context of CNs.

Keywords: Collaborative Networks, Collaborative Business Process, Business process verification, Compliance, Change

1 Introduction

The advancement in technology and the development of commercial business models has brought about intensified collaborative network (CN), which presents businesses that operate in a global context. Such collaborative networks bring about growing interconnectivity of all processes in the value chain. During their process life cycle, business processes are subject to change as a result of the emergence of new market needs and ever-changing requirement due to the implementation of new laws, policies and regulations. For instance, the on-going BREXIT in the UK, once finalized can bring about new laws and regulation, which might have a knock-on effect on Collaborative Business Process (CBP) across Europe. Consequently, collaborative business partners are faced with a high level of complexity dealing with these changes and continuously verifying the compliant behaviour of their business processes with regulations in place or any changes in the regulatory requirements.

So far, business process verification and compliance have received substantial research attention over the last two decades focusing on checking the complaint behaviour of business processes against several policies and regulations. Most of the reviewed studies mostly focus on the business process within one single organization using different approaches [1]. Compared to the compliance checking of a single business process, achieving compliance of CBP is a daunting task as compliance must be achieved not only with the internal regulations but also with different applicable external laws and regulations in place for all partners involved. It, therefore, becomes imperative for organizations to check and verify their process and review internal and external business policies fast enough to match the regulatory demands to avoid fines or litigation. Thus, a knowledge gap exists in automatically verifying the compliance of CBP with existing business processes against amended regulations to avoid starting

from scratch, wasting time and resources in creating new processes each time policies or regulations changes.

2 Process Verification vs. Compliance for Collaborative Business Processes

Fig 1 presents a general relationship between collaborative process verification and collaborative process compliance checking. While the process verification is done at the process design stage, the process compliance check is applied for both process design and process running stages. At the process design time, a business process model is designed to comply with different rules, during process running time; the process compliance is monitored and related according to the changed rules.
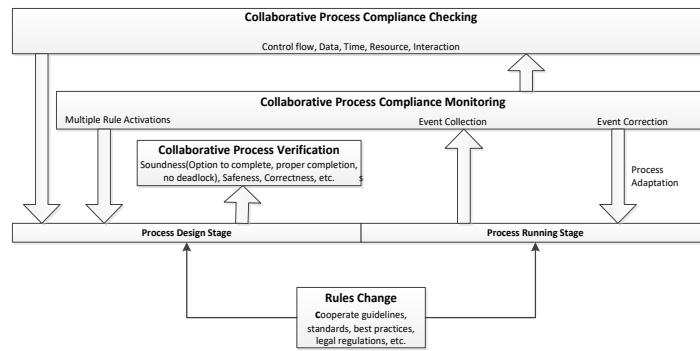
Fig. 1. The relation between verification and compliance

Naturally, process models may exhibit undesired properties in form of error which can prevent successful execution. For instance, in a collaborative business Process involving multiple process partners (i.e. private and public model). If a partner private model is changed uncontrollably, it can bring about the erroneous model to other process partners. It, therefore, becomes crucial to verify the correctness of the collaborative model before implementation as an erroneous model can result in behavioural anomalies within the entire process. The author in [2] describes three levels of correctness in-process model i.e. (i) syntactical correctness – checking the correct use of element (such as tasks, gateways, swim lanes, events), (ii) behavioural correctness (i.e. business process verification) – are the correctness of a model with regards to a set of properties such as deadlock, livelock, or dataflow errors, and (iii) semantics correctness (i.e. Business Process Compliance) – checking whether a business process model complies with applicable standards, law and/or regulations. These levels of correctness interlinked with each other and must be considered to fully achieve error-free model.

In this paper, we present the state of the art of CBP verification and business process compliance verification approaches. Complementarily, several open issues will be identified regarding the collaborative process. The rest of the paper is described as follows: section 3 reviewed the state of the art of different process verification approaches in the area of CBP. Section 4 discusses the general view of business process compliance and the different compliance verification approaches. In section 5, we highlight the work being carried out in collaborative process compliance as well as

compliance challenges in the context of CN. And lastly, we make conclusions and reveal our ongoing work in CBP in section 6.

3   Collaborative Business Process verification approaches

Business process verification is the act of proving the correctness of a model with regards to a set of properties. Presently, several powerful modelling languages have been used to model the workflow of CBP, such as UMM, UP-ColBPIP, IOWF, BPMN 2.0[3]. Formalizing the execution semantics of such languages enable the definition of formal methods and eliminate language ambiguities. At such, much effort has been devoted to the formalizing the execution semantics of BPMN with some works focusing on the transformation of BPMN elements using an intermediary formal model such as Petri net, process calculi etc. While some works used behavioural anti-patterns, others provide a direct formalization of BPMN semantics. To formally verify the correctness of a model, several verification approaches have been identified in the literature as well as different supporting tools. Preliminary works geared towards the verification of syntactical correctness and behavioural correctness i.e. soundness and weak soundness constraints [4].

The general approaches of the process verification are based on Petri Net or its variables. Initially, a process model is mapped onto a reset net, and then determines the correctness of the model by analyzing its state-space performances to generate all possible reachable states of a process model [5]. The weak soundness property and the irreducible cancellation regions property have also been determined with the use of backwards coverability notion in reset nets [6].

Aalst [7] described an approach to analyze and model inter-organizational workflows based on synchronous and asynchronous communication. The approach was used to obtain a global workflow modelled using Inter-Organizational Workflow (IOWF), which was then transform into a WF-net and verify its soundness property. Similarly, Jorge Roa et al. [8] propose a verification method - Global Interaction Net (GI-Net) based on Hierarchical and Coloured Petri Net (HCP-Net) to formalize CBP model in UP-ColBPIP, then use CPN tools (Coloured Petri Nets) to verify the Global Interaction soundness property. Their approach was able to support advanced control flow issues like advanced synchronisations, exemption management and cancellation regions, which was not supported in [7]. Roa et al. [8] proposed method is independent of the semantics and can be used with any modelling language for CBP. Though, the model must be structured (i.e. for any other modelling language such as BPMN in a non-structured model, it needs to be converted into a structured model before deriving its corresponding GI-Net). The method is limited to detecting an error in the global view of the interaction of CBPs without considering the private aspects of the collaborative partners. And most importantly the methods rely on state-space exploration, which may harm performance due to the state space explosion problem.

To improve the performance of their verification method, Roa et al. [9] further propose a new approach to verify the control flow of CBPs using behavioural anti-patterns and enable the detection of deadlocks in the control flow of CBPs. The approach supports the verification of advanced elements such as exception management, advanced synchronization and multiple instances. Their study reveals that the use of anti-patterns is as accurate as of the use of formal methods, but the latter improves the performance of the verification method [10].

Zhang et al [11] mapped two formal methods i.e. Petri nets (representing local flow model) and Pi calculus (represent the interaction between model) to model and generate the state graph of CBP using a collaborative reduction tool, then verify the structural soundness of the unified model. In [12], the author models a cross-organisational workflow using Interaction-Oriented Petri Nets (IOPN) then verifies the correctness (soundness and relaxed soundness) of the model based on the invariant analysis. Kheldoun et al [13] proposed a formal semantics of BPMN using ECARTNets to describe collaborative process then, verify its soundness property using Maude LTL model checker. Their proposed method can formalize a large set of BPMN features such as multiple instantiations of subprocesses, cancellation, exception handling while considering the data flow aspect.

In [14], the author proposed a direct formalization for a relevant subset of BPMN for mapping the CBP model in terms of Labeled Transition System (LTS). Then, automatically verify some properties (soundness and safeness) using LTL model checker. Their approach mainly focuses on the control-flow perspective and communication aspects of business processes. Another interesting work is described in [15], they provide a direct formalism of a subset of BPMN semantics using First-Order Logic (FOL) and further develop a verification tool (fbpmn tool) which was implemented in TLA+ using TLC model checker. Their approach was able to automatically verify some properties (soundness and safeness).

Overall, most of these studies fail to fully extend the formalism of tricky issues like multiple instances, subprocesses, error handling, loops and data object representation for a CBP. Studies that do not abstract data in verification are either required to state-bound domains which are subject to state-explosion [15] or rely on animation than a complete verification[16], making it difficult to verify a model for any possible initial value of the data [15].

Approach	Transformation					Anti-patterns		Direct Formalization		
Reference	[10]	[8]	[11]	[12]	[13]	[9]	[10]	[14]	[15]	[37]
Formalism	WF-NET	GI-NET	Petri Net & Pi Calculus	Invariant analysis	ECATNets	Behavioural anti-patterns	Anti-patterns	LTS	FOL	LTS
Tools		CPN				Eclipse plug-in		BProve	fBPMN	-
Model language	IOWF	UP-ColBPIP	Petri Net & Pi Calculus	IOPN	BPMN	UP-ColBPIP	UP-ColBPIP	BPMN 2.0	BPMN	BPMN
Techniques	-	-	-	-	Maude LTL model checker	-	-	LTL Model checker	TLC Model checker	-
Property verified	Soundness Property	Global soundness	Soundness property	soundness and relaxed soundness	Soundness property	Soundness Property: Deadlock in the control flow of CBP	Soundness Property: Deadlock in the control flow of CBP	Soundness and safeness	Soundness Property	well-structuredness, safeness, and soundness
Sub processes	-	-	-	-	Yes	-	-	-	Yes	Yes
Data	-	-	-	-		-	-	-	-	-
Loop		-			Yes	-	-	-	-	-
Multi instance	-	-	-	-	Yes	Yes	Yes	-	-	-
Cancellation regions	-	Yes	-	-	Yes	-	Yes	-	-	-
advanced synchronisations	-	Yes	-	-		Yes	Yes	-	-	-
exemption management	-	Yes	-	-	Yes	Yes	Yes	-	-	-

(Rows "Sub processes" through "exemption management" are grouped under the vertical label "Advance supported elements".)

Table 1: Comparison of verification approaches in CBP

Hence, there is still a need to define a formal semantics which will cover a comprehensive semantics that captures data objects, multi instances, looping and error handling for collaborative business processes. Besides, existing verification approaches for CBPs as review earlier mostly focus on control flow perspectives and communication aspects of business processes, whereby other process perspectives such as data, thermal and resources are abstracted.

Table 1 summaries different collaborative business process verification approaches. In general, there are three general types of verification approaches, namely transformation, anti-patterns, and direct formalization which are specified at the top row of the table. Different process verification approaches are also looking at from different aspects, such as which formalism used; properties verified and supported advanced elements of process characteristics, such as supporting sub-process, data flow, etc., which are shown in the first column of the table.

4   Business Process Compliance

While early works focused on the process verification of syntactical correctness and behavioural correctness (soundness constraints) mentioned in Section 2, recent work dealt with issues related to semantic correctness (processes compliance). Business process compliance denotes checking the compliant behaviour of business processes with applicable corporate guidelines, standards, best practices, legal regulations etc. The regulatory requirements are elicited from the general regulatory document and form constraints that restrict the impermissible behaviour of an organization business process. Though, elicitation of relevant requirement from the source document is not sufficient, as the requirements need to be transformed and translated into a formal form i.e. compliance rules to enable compliance verification over business process models.

It is worth noting that business processes compliance relates to conformance to different process perspective that is different phases of the process life cycles such as control flow, data, time and resources perspectives. The different process perspectives help to establish a relationship which facilitates derivation and categorization of compliance rules from the general policies and regulations. Compliance rules must be comprehensible and at the same time should have a precise semantics to enable automated processing and avoid ambiguities. Hence, several researchers have placed their focus on enabling the specification of compliance rules using different approaches with differences in the level of formalism.

Exiting approaches used in formalizing compliance rules are mostly based on temporal logic and Deontic Logic. Approaches based on temporal logic uses logical language like Computational Tree Logic-CTL [18] and Linear Temporal Logic-LTL [17] to express compliance rules. While approaches based on Deontic logic use languages such as PENELOPE (Process Entailment from the Elicitation of Obligation and Permission)[20] and Formal Contract language (FCL) [19]. As the logic-based approaches are complex and difficult to comprehend for users, and mainly consider the control flow perspectives. Researchers propose a comprehensible pattern and visual-based approaches. The pattern-based approach hides formal details behind the textual description and is limited to a set of predefined compliance rules patterns [21]. The approach addresses control flow, data, thermal and resource perspectives. While the visual languages provide an intuitive way to model compliance rule and hide formal details but are not limited to a predefined set of patterns [22].

4.1   Compliance Verification Approaches

Business Process Compliance involves using different compliance management strategy that is design time and run-time compliance strategy to ensure process compliance [1]. A Design-time strategy is a preventive approach that aims at managing and ensuring the compliance of business processes at the design phase or before execution time [23]. To check business process compliance at design time several approaches have been

proposed as well as different verification techniques. In [24], the approaches are categorized based on logic-based, static-based, pattern-based, and query-based approaches. These approaches often propose different languages to support checking in terms of structural behaviour, contractual obligations and security and privacy [25] and address different phases of the process life cycle

These categorized approaches are based on different underlying techniques in which the common techniques used is model checking. Studies like [18] have reported the use of model checking to verify the compliance of business process addressing different process perspectives. Though model checking techniques can identify the source of error but has its drawback. For instance, since the techniques rely on the exploration of the state space of process model then it can result in a state-space explosion which is a big challenge for practical implementation. Though, the challenges can be mitigated with the application of abstraction methods and techniques [26]. To address these issues, studies like [27], [28] proposed other techniques like graph reduction and sequentialization of parallel workflow and predicate abstractions [29]. While most of these approaches consider the control-flow perspective only, few studied also consider data perspectives and time perspectives.

Furthermore, Business process compliance checking and verification have been well addressed in literature from different angles in terms of privacy and security based on RBAC (Role-Based Access Control model) for access control and authorization based on roles [30], TBAC (Task-Based Access Control) for access control and authorization policies based on task executed in the process [31], ABAC (Attribute-Based Access Control) [32], SecBPMN [33] and STS-ml [34].

Formalism		Approach	Applications	Control flow	Data	Resources	Time
Model	CR						
Logic based Approaches							
BCL		Deontic	Design time	x			
FCL		Deontic	Design time	x			x
		Model checking	Design time	x			
PCL		Deontic	Design time	x			
PENELOPE		Deontic	Design time	x			x
NTL-ALC		Model checking	Design time	x			
CRL		Temporal	Design time	x			
Static based compliance approach							
BPEL -> π–calculus ->FSM	BPSL -LTL	Model checking	Design time	x	x		x
Timed automata	CTL	Model checking	Design time	x			
Pattern/graph based approaches							
PROPOLS - FSA		Pattern-based	Design time	x			x
BPMN-> automata	LTL	Model checking & bi-simulation	Design time	x			
BPEL-> LTS->TDFA	Ontology language	compliance verification approach	Design time	x			
LTL	CRL-LTL	Pattern-based	Design time	x			
Query based Approaches							
		Graph reduction technique and model checking	*Design time*	x	x		
BPMN-Q							
Approaches based on compliance with security and privacy							
RBAC		Temporal logic	Design time				
TBAC		Temporal logic	Design time		x	x	x
ABAC		Temporal logic	Design time		x	x	x
SecBPMN		Temporal logic	Design time	x	x		
STS-ml		-	Design time	x	x		

Table 2: Summary of Compliance Verification Approaches

Table 2 summarizes some of the state-of-the-art approaches for design-time compliance checking and verification. The approaches are classified based on their underlying techniques that are logic-based, static based, query-based, pattern-based approaches [24] and approaches based on compliance with privacy and security.

Compared to design-time checking (see Fig.1), run-time compliance strategy involves checking business process compliance during its execution [23]. The reality is that even if a business process has been checked during design-time, there is no certainty that the corresponding running process instance will be compliant as a result of human and machine-related errors. This implies that after designing a process model and the actual execution of a process is initiated, the running process instances need to be constantly monitored to detect any inconsistencies or violations [24]. The run-time approach has been well addressed in the literature and is categorized based on run-time compliance monitoring approach and run-time compliance detection [24].   Both approaches are further classified into monitoring–based approaches, logic-based approaches, and model-based approaches. While the runtime compliance approach is perceived to be flexible and having the ability to handle compliance violations beyond design time; the design time is preferable for being pre-emptive in detecting compliance violations and allowing corrections at an earlier stage during process design.

5   Compliance in Collaborative Networks

Collaborative Network (CN) has been the topic of discussion in the literature involving a diverse range of forms i.e. from stable collaborative networks to dynamic networks such as Virtual Organisations, Virtual Enterprise, chain or enterprise networks. CN involves business integration and collaboration between geographically distributed and heterogeneous organizations to achieve common goals. Such integration and collaboration among the organizations are established and carried out through Collaborative Business Processes (CBP) enabled by advancement in technology. These intelligent technologies come along with intensified collaborative network CN, which gives rise to the growing interconnectivity of all processes in the entire value chain such as human and machine. Though, it is accompanied by a high level of complexity in regards to legal and compliance challenges.

By nature, achieving compliance of CBP in the context of CN is complex and requires unique characteristics and requirements due to its design principles for decentralized decision making. For instance, in a CN environment, different partners combine resources and skills to design and execute a business opportunity and at the same time act independently from each other. The fact that each partner is geographically distributed makes them distinct from partners in the same location. In particular, besides the internal policies and external regulations regulating each partner process, their process is also governed by contractual obligations as well as international regulations guiding their overall process operations. Achieving compliance in such a network environment will be challenging and especially when one partner changes its process structure in an uncontrolled manner, or when policy or regulations changes.

Realistically, potential changes in process or policies and regulations are inevitable and should be expected either through market expectations and needs, amendment of existing laws or implementation of new laws, policies and regulations. A great example is with the COVID-19, which has made the government around the world to revise and amends regulations in response to the virus outbreak. Most organizations must change

and comply with their businesses and services according to the strategies published by the governments of different countries. Collaborative business partners will need to assess and deal with different changes in regulatory requirements around the world. These changes might have a direct effect on the entire business collaboration and its existing processes resulting in heavy cost as well as causing an organization to modify its entire process or part of it to achieve compliance. Not only does the change will affect the structure of the CBP model but also their accompanying rules as well as the running instances. Falling to manage or constantly monitor these changes can lead to penalties and potential legal issues.

In reality, compliance can be fulfilled before a change in CBP but this might not remain satisfied after any change occurs. Therefore, after a change has been applied to a process or compliance rules, it is imperative to identify changes in the policy, follow a formal method to re-evaluate the compliance rules, identify the components of the process that are affected by the amendments, and recheck all the three correctness level specifically checking if the existing or redesigned collaborative process still complies with all compliance rules. Though, few works have been done in the literature addressing the impact of change on the compliance of CBP. For instance, the work of [35], analyses how compliance rule and process changes impact on each other, then, further propose an algorithm that deals with the change propagation in CBP. And of recent, Kasse [36], propose a simulation technique to assess the impact of regulatory variations over existing or redesign collaborative business process. Compliance of CBP, however, is yet to be fully investigated or checked after any changes in process or compliance rule.

It is worth noting that despite the overwhelming body of literature addressing the compliance-related problem from a variety of perspectives, it is hard to oversee, compare and make a decision on which of the existing approaches could be utilized to check the compliance of CBP after any changes. Hence we justify the need to optimize different compliance verification approaches and provide an efficient algorithm that will support compliance verification of CBP after any change to keep the CBP model behaviourally and semantically correct both at design time and runtime.

6 Conclusion and Future Research

The paper first provides a clear picture of the relationship between collaborative process verification and collaborative process compliance. Different approaches for collaborative process verification in Section 3 and process compliance in Section 4 and 5 are summarized. The paper also reviews the different techniques used in the verification and compliance check, i.e. formal methods, model checkers, graph reduction, sequentialization of parallel workflow, and predicate abstractions, etc.

More recently using process traces and process simulation are used to check collaborative process compliance due to the complex nature of collaboration. Traditionally, the properties for process verification or checking are limited. Today collaborative networks are often subject to restrictions that stem from laws, regulations or guidelines which are not just impacting the control flows of the processes, but also data flow, resource flow, and process exceptional handling. The compliance properties thus need to be largely extended not only to cover traditional process properties, but also security and time, etc. COVID-19 has changed our lives and is likely to make a lasting impact on our economic development. All existing CNs are facing some levels' changes. The paper provides the first step forward to the solutions of compliance checking of CNs in dynamic environments.

References

1. El Gammal, A.F.S.A.: Towards a comprehensive framework for business process compliance. Tilburg University, School of Economics and Management (2012).
2. Knuplesch, D., et al.: Towards compliance of cross-organizational processes and their changes. In International Conference on Business Process Management. Springer, (2012).
3. von Rosing, M., et al.: Business Process Model and Notation-BPMN (2015).
4. Knuplesch, D., Reichert, M. and Kumar, A.: A framework for visually monitoring business process compliance. Information Systems, 64: p. 381-409 (2017).
5. Wynn, M.T., et al.: Business process verification–finally a reality! Business Process Management Journal (2009).
6. Finkel, A. and Schnoebelen, P.: Well-structured transition systems everywhere! Theoretical Computer Science. 256(1-2) p. 63-92 (2001).
7. Van Der Aalst, M.: Modeling and analyzing Interorganizational workflows. In Proceedings 1998 International Conference on Application of Concurrency to System Design. IEEE (1998).
8. Roa, J., O. Chiotti, and Villarreal, P.: A verification method for collaborative business processes. In International Conference on Business Process Management. Springer (2011).
9. Roa, J., O.J.A. Chiotti, and Villarreal, P.D.: Detection of anti-patterns in the control flow of collaborative business processes. In Simposio Argentino de Ingeniería de Software (ASSE 2015)-JAIIO 44, Rosario (2015).
10. Roa, J., et al.: Specification of behavioural anti-patterns for the verification of block-structured collaborative business processes. 75: p. 148-170 (2016).
11. Zhang, L., Lu, Y. and Xu, F.: Unified modelling and analysis of the collaboration business process based on Petri nets and Pi calculus. 4(5): p. 303-317 (2010).
12. Ge, J. and Hu, H.: A Decomposition Approach with Invariant Analysis for Workflow Coordination. In International Conference on Database Systems for Advanced Applications. Springer (2009).
13. Kheldoun, A., Barkaoui, K. and Ioualalen, M.: Formal verification of complex business processes based on high-level Petri nets. Journal of Information Science. 385: p. 39-54 (2017).
14. Corradini, F., et al.: BProVe: a formal verification framework for business process models. In32nd IEEE/ACM International Conference on Automated Software Engineering (ASE). IEEE (2017).
15. Houhou, S., et al.: A First-Order Logic Semantics for Communication-Parametric BPMN Collaborations. In International Conference on Business Process Management. Springer (2019).
16. Corradini, F., et al.: Animating multiple instances in BPMN collaborations: from formal semantics to tool support. In International Conference on Business Process Management. Springer (2018).
17. Ghose, A. and Koliadis, G.: Auditing business process compliance. In International Conference on Service-Oriented Computing. Springer (2007).
18. Nishizaki, S.-y. and Ohata, T.: Real-time model checking for regulatory compliance. In International Conference on Advances in Information Technology and Mobile Communication. Springer (2012).

10

19. Governatori, G. and Rotolo, A.: Norm compliance in business process modelling. In International Workshop on Rules and Rule Markup Languages for the Semantic Web. Springer (2010).
20. Goedertier, S. and Vanthienen, J.: Designing compliant business processes with obligations and permissions. In International Conference on Business Process Management. 2006. Springer.
21. Turetken, O., et al.: Capturing compliance requirements: A pattern-based approach. In *IEEE Software*, vol. 29, no. 3, pp. 28-36, DOI: 10.1109/MS.2012.45. (2012).
22. Knuplesch, D., et al.: Visual modelling of business process compliance rules with the support of multiple perspectives. In International conference on conceptual modelling. Springer (2013).
23. Fdhila, W., et al.: Change and compliance in collaborative processes. In IEEE International Conference on Services Computing. IEEE (2015).
24. Hashmi, M., et al.: Are we done with business process compliance: state of the art and challenges ahead. 57(1): p. 79-133 (2018).
25. Kasse, J.P., et al.: The need for compliance verification in collaborative business processes. In Working Conference on Virtual Enterprises. Springer (2018).
26. Frederick, K. Frantz. A: taxonomy of model abstraction techniques". In: Proceedings of the 27th conference on winter simulation pp. 1413–1420. DOI: 10. 1145/224401.224834 (1995).
27. Awad, A. and Sakr, S.: Querying graph-based repositories of business process models. In International Conference on Database Systems for Advanced Applications. Springer (2010).
28. Barnawi, A., et al.: An anti-pattern-based runtime business process compliance monitoring framework. 7(2) (2016).
29. Knuplesch, D. and Reichert, M.: Ensuring business process compliance along the process life cycle. (2012).
30. Combi, C., L. Viganò, and M. Zavatteri.: Security constraints in temporal role-based access-controlled workflows. In Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. (2016).
31. Thomas, R.K. and Sandhu, R.S.: Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management, in Database security XI. Springer. p.166-181 (1998).
32. Gautam, M., et al. Poster: Constrained policy mining in attribute-based access control. In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies. (2017).
33. Salnitri, M., Dalpiaz, F. and Giorgini, P.: Modeling and verifying security policies in business processes, in Enterprise, business-process and information systems modelling. Springer. p. 200-214 (2014).
34. Robol, M., Salnitri, M and Giorgini, P.: Toward GDPR-compliant socio-technical systems: modelling language and reasoning framework. In IFIP Working Conference on the Practice of Enterprise Modeling. Springer (2017).
35. Knuplesch, D., et al.: Detecting the effects of changes on the compliance of cross-organizational business processes. In International Conference on Conceptual Modeling. Springer (2015).
36. Kasse, J.: Supporting compliance verification for collaborative business processes. Bournemouth University. (2019).
37. Corradini, F., et al., Well-structuredness, Safeness and Soundness: A Formal Classification of BPMN (Collaborations) (2020).