A Conceptual Framework of Security Requirements in Multi-cloud Environment

Hamad Witti[1(✉)], Chirine Ghedira Guegan[2], and Elhadj Benkhelifa[3]

[1] University of Lyon, University Jean Moulin Lyon 3,
IAE Lyon School of Management, Magellan, Lyon, France
moussa.hamad-witti@univ-lyon3.fr

[2] University of Lyon, University Jean Moulin Lyon 3,
IAE Lyon School of Management, LIRIS, UMR 5205, Lyon, France
chirine.ghedira-guegan@univ-lyon3.fr

[3] Staffordshire University, Stafford, UK
elhadj.benkhelifa@googlemail.com

Abstract. Nowadays, organizations are increasingly attracted by the benefit of multi-cloud offerings. However, they have to adapt their business processes for multi-cloud collaboration and especially to deal with a major security problem. Indeed, the complexity of security due to multiple cloud policies and a variety of security requirements does not guarantee compliance with the security requirements of their business processes. We present our initial research that aims to develop an effective security governance framework for a multi-cloud environment. Our approach is to shed light on the need to integrate security requirements into business processes and to provide a conceptual framework of security requirements including steps and processes for a multi-cloud environment.

1 Introduction

Nowadays, organizations move their IT to cloud computing because of its various advantages, including the reduction of costs and the accessibility of services and data from any site, on any support at any time. Indeed, cloud customers and organizations store and exchange sensitive information with cloud service providers often vulnerable [1]. However, regardless of its deployment structure as infrastructure (IaaS), platform (PaaS) or applications (SaaS), the nature of the cloud requires a revision of its security.

However, recent tendency is to resort to multi-cloud environments [2]. Such environment provides a number of advantages over traditional single-vendor strategies used by single cloud environments. The main among them is the ability to leverage the most appropriate unique cloud services from multiple different providers at need on demand at any given time. In order to be flexible and dynamic, organizations can adapt quickly to changes in their business market to select the best cloud services to meet their requirements. To take advantage

© Springer International Publishing AG, part of Springer Nature 2018

A. Yang et al. (Eds.): SERVICES 2018, LNCS 10975, pp. 3–17, 2018.
https://doi.org/10.1007/978-3-319-94472-2_1

of these benefits in this context, compagnies deploy their business process (BP) using their applications over different clouds [3].

Yet, multi-cloud introduces additional challenges in the management and the security that expose the business activities. Therefore, securing the business process of those organizations is becoming a great challenge. Various solutions [4–7] to secure business process are provided in the cloud context, but did not concerns multi-cloud environment.

In this paper, we propose a framework to integrate security requirements based on business process in the multi-cloud environment. This work is part of our on-going research effort to create a Multi-cloud Security Governance (MSG) Framework for modelling Security Governance as a Service (SGaaS), according to the XaaS model at the Governance as a service (GaaS) Level. The framework consists in modeling the security requirements using the BPMN extension, integrating them into business process and allowing the security business processes to achieve governance level in order to provide automated security governance in multi-cloud environment. Our work ensures for the organizations and cloud providers that are involved in the multi-cloud process, secure business activities based on the security business processes defined by the security requirements.

The remainder of this paper is organized as follows. Section 2 presents the related challenges on multi-cloud security. Section 3 focuses on multi-cloud security requirements related to some issues and challenges. Section 4 presents Related Work. Section 5 describes the conceptual security requirements framework for multi-cloud environment. Section 6 gives an overview of the framework by detailing its different steps and components. Section 7 illustrates an example for Business Security Process in a multi-cloud use-case. Finally, Sect. 8 concludes the paper and presents some future endeavors.

2 Multi-cloud Security Challenges

Researchers and industry specialists have highlighted several security issues in cloud computing. Figure 1 illustrates some of those issues that specially emerge during dynamic sharing and collaboration across multiple clouds. Indeed, the use of multi-cloud services from multiple providers adds a new dimension of complexity to an already complex cloud computing scenario. Some essential aspects deserve to be emphasized and must be considered in a multi-cloud environment.

The heterogeneity of services offered by different providers generates a lack of interoperability [3]. A heterogeneous environment with various interfaces in different clouds represents a serious risk to be considered at design time, since it will influence the capacity of an application architect to decide between one service or another. In terms of quality, and security requirements a service will be highly interoperable with other systems if it can be combined in collaboration with many other services, from the same or other cloud service providers. Portability refers to the ability to move and reuse applications and data from one cloud provider to another regardless of the differences that may exist among their systems [8]. Thus, the multi-cloud portability is highly related to the business process and security requirements regarding applications and cloud services.

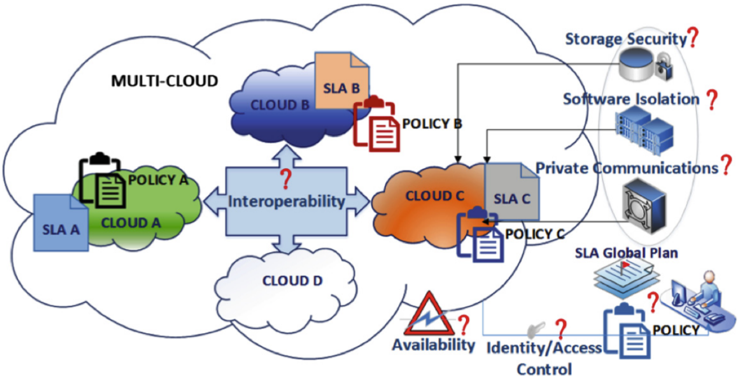


Fig. 1. Multi-cloud security challenges

Moreover, the transaction of data between services in different clouds and cloud providers collaboration may be unsecure (see Fig. 1). Thus, it increases the overall vulnerability due to the complexity of management, loss of client control, which is moved to brokers, exposed interfaces due to public domain, and the possibility of breaches in data storage and data privacy due to multi-tenancy. Therefore, for a secure multi-cloud collaboration, trust relationships among participants have to be reliably elicited, aggregated, and propagated [9]. However, in addition to the traditional security requirements illustrated in Fig. 1 such as data storage security, data security, data privacy and availability, the additional security requirements have to manage on multiple clouds the business security efficiently on the different clouds.

Besides, issues pertaining heterogeneous policy and conflict management are serious concerns in multi-cloud computing environment [10]. Indeed, interconnecting different models of cloud brings great agility and rich functionality covering all IT Systems needs with many benefits. However, Fig. 1 shows that the complexity due to the heterogeneity of the offers and services, raises major challenges in terms of security, interoperability, portability, and governance. Indeed, different clouds with different SLA involve different security policies that controlled access to the protected resources, specified security rules and based on the users policies, can be the source of policy conflicts.

Moreover, the coordination between services that are offered by different providers performs the capacity to replace a service by another one and increases security services coordination to achieve security governance. Multi-cloud collaboration, involving heterogeneous security policies can be the source of policy conflicts that result in security breaches [11]. Therefore, protecting the privacy and securing the exchanges between clouds, policy and conflicts management are critical and important challenges. Among the aforementioned multi-cloud security challenges, we focus on security requirements issues which we analyze in the next section.

3 Multi-cloud Security Requirements

The critical security challenges discussed above have gained significance and need to be carefully addressed. Thus, cloud service customers to be faced with those challenges of selecting cloud service providers and evaluate security implementations based on their security requirements. Multi-cloud security requirements refer to the security and privacy requirements for cloud services as a guide for assessing the level of security and identifying the security requirements needed to protect the multi-cloud environment. According to [12], a security requirement is the refinement of a risk treatment decision (e.g., avoidance, reduction, retention, or transfer) to treat and mitigate the identified risks. Moreover, authors define Security Requirement in [13], as a quality requirement that specifies a required amount of security (actually a quality subfactor of security) in terms of a system-specific criterion and a minimum level of an associated quality measure that is necessary to meet one or more security policies. In [10], Labda et al. analyzed *Confidentiality, Integrity, Availability and Accountability* as part of the security requirements. The most investigated security requirements are *confidentiality, integrity, availability, trust, audit*, and *compliance*. Besides, in the literature, cloud security requirements are addressed in terms of the fundamental security issues in a shared environment. Firesmith [13] listed seven key concepts at the highest level including access control, *attack/harm detection, integrity, non-repudiation, privacy, security auditing* and physical protection. As a foundation of the created structure by Firesmith [13], authors deduced in [14], six distinguishable classes of security requirements such as access control, attack/harm detection and prevention, integrity, accountability, privacy, and availability. Moreover, [15] identified that the following security requirements have been addressed: *Attack/Harm Detection, Non-Repudiation, Security Auditing, Privacy & Confidentiality, Access Control* and *Integrity.*

However, Iankoulova and Daneva argued in [16], that security requirements and solutions vary in terms of cloud layers being covered, technology types involved, and whether they reside on the Cloud Service Provider's or Cloud Service User's sides. Thus, multi-cloud security requirements are derived from these cloud computing security requirements and also encompassed the security needs at the interaction time between clouds of the multi-cloud environment to achieve the business security objectives. Furthermore, the report [17] provides a checklist of security and privacy requirements for cloud computing services, gathered from established industry standards and best practices, supplemented with requirements from European data protection legislation, and taking into account security issues identified in recent research on Cloud security. Based on these aforementioned works, we deduced ten relevant security requirements that concern the multi-cloud environment, namely **Availability, Access Control, Attack/Harm Detection and Prevention, Integrity, Accountability, Privacy, Binding of duties, Separation of duties** and **Delegation**.

In the following section, we discuss how these requirements can be modeled and enforced for business-process-driven systems. We also develop our approach based on those security requirements in order to enhance security governance in multi-cloud environment.

4 Related Work

Security is an essential aspect of all information processing activities and all organizations have to develop actively mechanisms and tools to maintain and ensure the security and integrity of their information resources. Rodríguez et al. [18], introduce a comprehensive BPMN-security extensions. They presented a BPMN metamodel with core element and extension that incorporate security requirements into Business Process Diagrams. They proposed an extension included *nonrepudiation, attack/harm detection, integrity, privacy, access control, security role* and *security permissions.* They also added two subcomponents namely privacy and access control. However, They don't explain the absence of *availability.* Given the importance of *availability* for business processes and the fact it is a core component of cyber security [14], it is a necessary requirement that should have been included.

Moreover, Mülle et al. provided in [19] a security extension to support the business process lifecycle from modeling to runtime. They develop security concepts including *authorisation, authentication, auditing, confidentiality* and *integrity.* Thus, they subdivide some of these based on the concept interacts such as *assignment mechanism, delegation, separation of duty, binding of duty, user consent and trust policy.* However, there are not included concepts which are widely consider a priority for any security extension, such as *non-repudiation, attack/harm detection* and *privacy.*

Brucker et al. presented an extension called SecureBPMN in [20]. Authors discuss how security requirements should be modeled at design-time and propose a tool which can both model the security requirements for business process-driven systems and enforce them at runtime. The proposed extension covered in SecureBPMN are comprised *access control, separation of duty, binding of duty* and *need to know.* Authors focuses their extension on access control as SecureUML [21], but also provides support for the other mentioned concepts. Despite, several concepts included in their extension, authors provide support for three core concepts namely *confidentiality, availability* and *integrity.* However, *need to know* is an interesting extension, but not seem placed at the adequate level i.e. at the same level of *access control.* Besides, Cherdantseva was developed in his thesis 'Secure*BPMN' [22], a graphical security modeling extension for industry standard business process modeling language BPMN 2.0.1. Secure*BPMN introduces comprehensive semantics based on a Reference Model of Information Assurance & Security (RMIAS) [23]. The BPMN metamodel was extended with security elements in particularly security goal that regroup *Confidentiality, Integrity, Availability, Authenticity & Trustworthiness, Non-repudiation, Accountability, Auditability* and *Privacy.*

Salnitri et al. propose in [24], a framework which aims to both model and verify security policies within a business process. The concepts they chose were derived from the Reference Model of Information Assurance and Security (RMIAS) [23]: *accountability, auditability, authenticity, availability, confidentiality, integrity, non-repudiation* and *privacy*.

Furthermore, the increase of cloud computing involves to consider business security extension in cloud computing. The literature shows that few approaches consider security requirements as a primary part in cloud context. Despite, some works relating approach integrating security requirements into Business Process Management in cloud computing cases [3,4,6,7]. None of them addresses the multi-cloud approach based on business processes and security requirements of all participants.

5 A Conceptual Security Requirements Framework for Multi-cloud Environment

A multi-cloud environment that is stable and capable of delivering a very high level of security and privacy cannot be achieved without considering involved security requirements. These security requirements encompass both security requirements from cloud users and cloud providers that are involved in multi-cloud interaction.

Moreover, multi-cloud service users have business objectives that require to secure their business processes in this heterogeneous environment to achieve security and privacy. This is cannot be achieved without integrating security requirements into business process. However, multi-cloud environement implies to take also into account the security requirements of each involved clouds. We propose an approach that integrates cloud users security requirements into business process deployed on each cloud. Some works have treated on Business Process deployment in multi-cloud [6,25,26]. We assume that the business process was designed and modeled at the *enterprise domain* and splited into different clouds at the multi-cloud environement as illustrated in Fig. 5. We focus on security aspect in order to pilot security from security requirements and business process model. Moreover, our approach brings a novelty regarding the works carried out around this topic:

- The process owner knows the whole process and the security objectives to achieve business process execution in a secure way.
- The process owner knows the security requirements of each cloud that will run the process or part of the process at the multi-cloud collaboration phase.
- Each cloud executes the parts of the process while respecting the security requirements of the process owner according its own security needs. In addition, each cloud must also satisfy the security requirements of cloud with which it interacts at the collaboration phase.

6 Framework Overview

The proposed framework of security requirements in multi-cloud environment as depicted in the Fig. 2, is composed of:

- **Security Requirements Selection Module:** This module is in charge of the selection of overall security requirements from users side and cloud service providers side.
- **Multi-cloud Security Requirements Integration Module:** This module is in charge of the security requirements integration into the Business Process.
- **Business Security Process:** The Business Security Process is the result of Previous module (Multi-cloud Security Requirements Integration Module).
- **Business Security registry:** All Business Security was registered for monitoring and security governance process
- **Security Requirements Monitoring:** This module is in charge of security requirement monitoring.

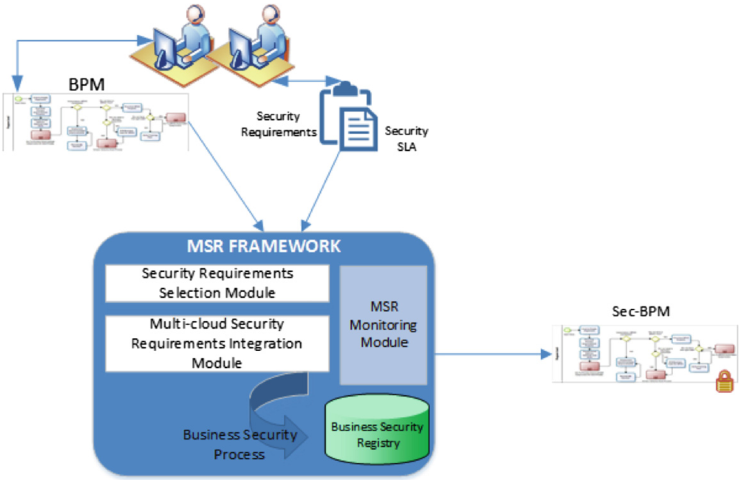

BPM
Security Requirements
Security SLA
MSR FRAMEWORK
Security Requirements Selection Module
Multi-cloud Security Requirements Integration Module
MSR Monitoring Module
Business Security Process
Business Security Registry
Sec-BPM

Fig. 2. Multi-cloud security requirements framework

The proposed framework integrates security requirements into business process in multi-cloud environment. Therefore, to tacking account our framework objectives, modeling language and new concepts of security requirements are both necessary. For this, the language of the proposed framework is based on BPMN regarding the concepts that have been defined in [18], combined with concepts from the security requirements engineering literature, and in particular SecureBPMN, and enhanced with concepts from security engineering and privacy engineering, and in particular Secure*BPMN.

The main objective of this framework is to create secure business process designs using as input the high-level security requirements of Multi-cloud system stakeholders as illustrated in Fig. 3 that shows the different components of the framework and their interconnections. Besides, Fig. 3 describes the steps for the application of our framework.

1. **Step 1:** At the Enterprise Level, Business Process is generated after analysis of internal process to achieve business Objectives. This process is modeled with BPMN. In the Enterprise Level the generated Business Process was validated after simulations operations. Otherwise, an analysis of the threat and security breach of the Business Process, provides Security Requirements in the Enterprise Level. These security requirements are identified and modeled in XML format.
2. **Setp 2:** At the Multi-cloud Security Requirements Level, the Security Requirements from Enterprise Level was associated with the Cloud Service Provider Security requirements by the Security Requirements System.
3. **Setp 3:** At this step Security Requirements of cloud Service Provider is selected and the Security Requirements was contactualized in the Security SLA.
4. **Setp 4:** SOA based Modeler provides a transformation rules for integrating Security Requirements into Business Process according the security extension of BPMN that described in the next section.
5. **Setp 5:** The Multi-cloud Security Requirements Integration System and Multi-cloud Business Security Construction System are working together to integrate the selected Multi-cloud Security Requirements into Business Process. Indeed, the mapping of the Security Requirements and the Business Process provides Security Process. Therefore, the generated Security Process was used by the Multi-cloud Business Security Construction System to create Secure Business Process.
6. **Setp 6:** The generated Secure Business Process by the Business Security Extension Process was stored in the registry.

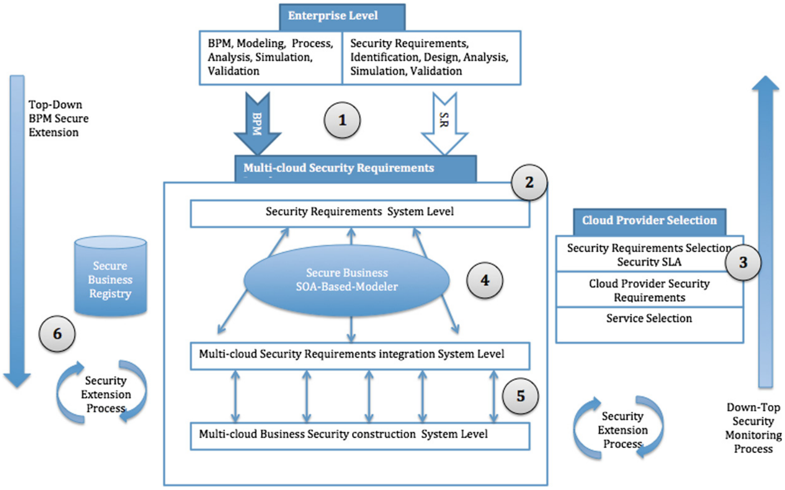

Enterprise Level
BPM, Modeling, Process, Analysis, Simulation, Validation
Security Requirements, Identification, Design, Analysis, Simulation, Validation
BPM
1
S.R
Top-Down BPM Secure Extension
Multi-cloud Security Requirements
2
Security Requirements System Level
Secure Business SOA-Based-Modeler
4
Multi-cloud Security Requirements integration System Level
5
Multi-cloud Business Security construction System Level
Secure Business Registry
6
Security Extension Process
Cloud Provider Selection
Security Requirements Selection
Security SLA
3
Cloud Provider Security Requirements
Service Selection
Security Extension Process
Down-Top Security Monitoring Process

Fig. 3. Components and process of Multi-cloud secure business process design

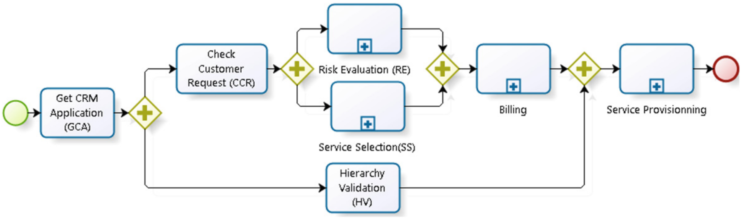

Get CRM Application (GCA)
Check Customer Request (CCR)
Risk Evaluation (RE)
Service Selection(SS)
Hierarchy Validation (HV)
Billing
Service Provisionning

Fig. 4. A simple business process for CRM customers requesting and service provisioning

7 Illustration Example

To illustrate the goal of our proposal, we define a simple business process model for CRM provisioning services from customers requests using BPMN notation (depicted in Fig. 4). In this business scenario, an enterprise user (front-office user) initiates the CRM application and checks customer requests. First, to handle the customer requests, front-office user directly sends to the risk evaluation application and service selection service to select the requested service. Once the risk related to the customer's requested service is evaluated, the second step is the billing process. Third, service provisioning needs hierarchy validation by the back-office user from the proposed billing. Finally, after the service provisioning process, the customer's request is finalized.

Using a multi-cloud environment, company wishes to guarantee its security requirements along with the business objectives. Therefore company needs to connect freely and securely to the various external applications that are hosted on different clouds (Cloud 1, Cloud 2 and Cloud 3) and this in various forms of access.

Moreover, the business process execution of the CRM must respect the security requirements and the business processes must not be compromised by the multiples users in internal cloud and between clouds in multi-cloud mode (Fig. 5). In this context, securing business process became a challenge for the company.

The problem is on the one hand, that it is necessary to secure the business processes during the different phases taking into account the interactions between the users inside of clouds, but also between the differents clouds from the multi-cloud environment. On the other hand, it will be necessary to take into account in addition to the security requirements of the enterprise domain, the security requirements at the level of the different clouds that are involved in the execution of the multi-cloud process. This requires clarifying the relationships and responsibilities between the different actors and the roles of each cloud. Then, sharing the security requirements between different clouds and the enterprise users is an important step to be met. Finally, integrating security requirements into the business process (Fig. 5) in order to generate secure business processes will ensure security objectives.

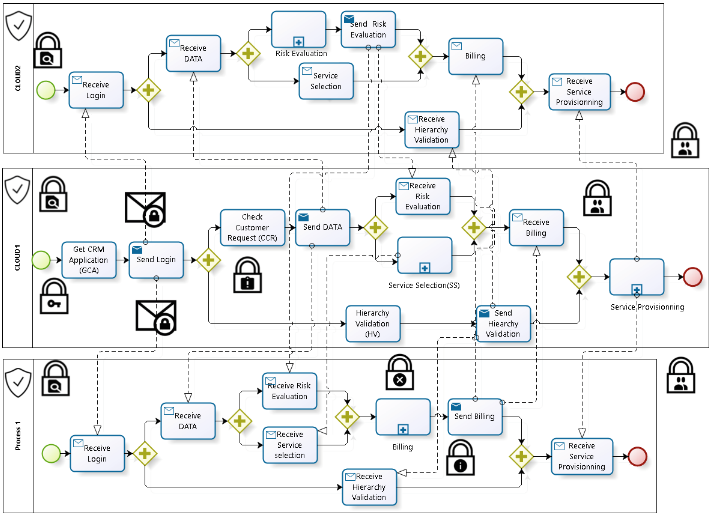


Fig. 5. Secured business process in multi-cloud collaboration

Each cloud must consider accountability as a mandatory security aspect in the multi-cloud environment. Moreover, each sending or receiving of messages between the different clouds must also be secured (Secure Association). However, the particularity of the Multi-cloud, is that SoD can be considered into the same cloud between several users, but also between the different clouds.

7.1 Business Security Process: Security Extension for BPMN

In order to integrate security requirements into business process models, it is necessary and useful to have a notation that must be supported by a set of graphical concepts that allows us represent the security semantics. As we have shown in the previous section, BPMN is widely used by researchers especially for its business orientation. However, BPMN does not explicitly consider mechanisms to represent security requirements.

In order to explain our proposal we remind initially our selected security elements in Sect. 3 according to the cyber security literature, that we have incorporated into the BPMN metamodel that we have created as shown in Fig. 6.

Furthermore, we have completed the extended metamodel (Fig. 6) with security requirements. In Table 1, we extensively show the relation between the Business Process Diagramm (BPD) elements and the new security elements. We show a BPD (core modeling elements) metamodel including the security requirements which have been represented in the specifications of our proposal (yellow-coloured). We have inherited from **BusinessProcessDiagram** the class **SecureBusinessProcessDiagram** that will be used to contain the specifications related to requirements, roles and security permissions.

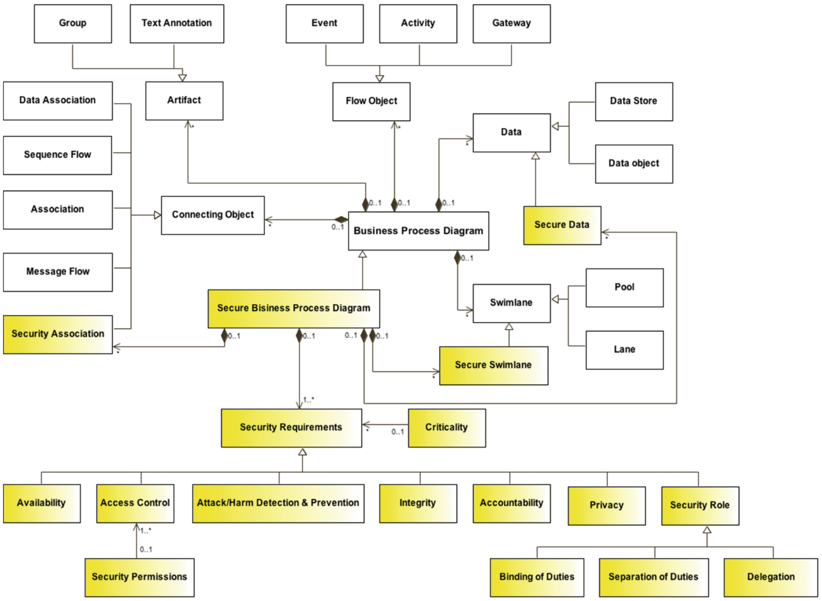


Fig. 6. Secure BPMN with extended elements

Table 1. Extended elements for security requirements and element of BPD

	BPMN elements								
Security requirements	Pool	Lane	Group	Activity	Message flow	Data object	Association	Security association	Secure swimlane
Availability	X	X	X	X	X		X	X	X
Access control	X	X	X	X					
Attack/Harm detection & prevention	X	X	X	X	X	X	X	X	
Integrity					X	X			
Accountability	X	X		X	X	X		X	X
Privacy	X	X	X						
Security role	X	X	X				X	X	X
Security permissions						X	X	X	X

Besides, according to [27], extensions which specify security requirements across various abstraction levels must ensure a hierarchical structure that is maintained to avoid confusion and construct redundancy. In our proposal we have associated a symbol (padlock in Table 2) to represent security requirements in a standard way for security requirements. Each security requirement is specified with a relevant symbol in the center of the symbol (see details in Table 2). We have considered to represent security requirements

(**Availability, Access Control, Attack/Harm Detection and Prevention, Integrity, Accountability, Privacy, Binding of duties, Separation of duties** and **Delegation**). According to [14], Accountability encompasses Non-Repudiation, Audit and Forensics. While Access control is associated with **security permissions**, such as *Restricted, Confidential, Proprietary* and *Public*) as depicted in the Table 5. Security Permissions will the specific security monitoring and enforcement mechanisms at the security governance level. Confidentiality is not considered in an explicit way because it underlies Privacy.

Table 2. Security requirements notations

Security Requirements	Security Property	Criticality		
		High	Medium	Low
Availability	This property expresses ensuring that all resources of multi-cloud are available and operational when they are required by authorized cloud users or cloud service providers	🔒	🔒	🔒
Access Control	Access to resources as well as actions need to be restricted to certain security permissions (e. g., restricted, Confidential, proprietary, public)	🔒	🔒	🔒
Attack/Harm Detection & Prevention	This property expresses the degree to which attempted or successful attacks (or their resulting harm) are detected, recorded, and notified	🔒	🔒	🔒
Integrity	This property expresses completeness, accuracy and absence of unauthorized modifications in all its components (e.g. data, sharing resources)	🔒	🔒	🔒
Accountability	This property expresses the ability to hold cloud users and cloud service providers responsible for their actions	🔒	🔒	🔒
Privacy	This property expresses the cloud users privacy requirements that should be satisfied and confidential	🔒	🔒	🔒

Besides, we introduce **security role**, associated with *Separation of Duties (SoD), Binding Of Duties (BoD)* and *Delegation* to characterize the security needs in heterogeneous multi-cloud collaboration (Table 3).

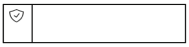
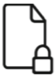
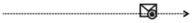
Table 3. Security roles notations

Security Roles				
SoD	This property expresses that two tasks have to be performed by two different cloud users or cloud service providers to avoid the risk of frauds	🔒	🔒	🔒
BoD	This property expresses that two activities must be performed by the same cloud user or cloud service provider	🔒	🔒	🔒
Delegation	This property expresses the transfer of execution rights for activities and access rights to data and cloud resources for cloud users or cloud service providers	🔒	🔒	🔒

Moreover, we add also a specificity with the **criticality** concept for the needs of the security rules during the governance mechanisms in order to prioritize the alerts and to measure the answers depending on the severity. We define as illustrated in the Table 3, 'High' represented with dark symbol in the center of padlock, 'Medium' in grey and 'Low' in blank.

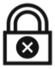
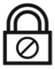
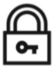
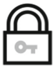
Modeling security requirements in the multi-cloud environment, introduces new considerations as depicted in the Table 4. Indeed, Swimlane represents cloud

Table 4. Secure objects

Secure Swimlane	
Secure Data	
Security Association	

service provider and as we explained in the previous sections, cloud services providers must be trusted and the collaboration must be secured in order to enhance multi-cloud security. Therefore, we have added the concept of **Secure Swimlane** to represent trust and secure transaction between clouds. However, association represents in our context transaction between clouds and must be secured. For this we add **Security Association**. Finally, Data are the center of the multi-cloud collaboration. In as such heterogeneous and multi-tenancy, Data are shared and must be secured. Thus, we propose **Secure Data**.

Table 5. Security permissions notations

Security Permissions		
Restricted	This property expresses that access is restricted only of authorized party (cloud users or cloud service providers)	
Confidential	This property expresses that the access concern confidential data	
Proprietary	This property expresses that only the owner party is authorized access (cloud users or cloud service providers)	
Public	This property expresses that access is authorized without identification for all	

8 Conclusion

The main contribution of this work is the proposal of a multi-cloud security requirements framework that is the initiate step of Multi-cloud security governance Framework. The first objective of our framework is to integrate security requirements in the business process to guarantee successful security governance, independently of the type of cloud deployment. Furthermore, the proposed framework is based on security standards and published guidelines, so that existing efforts on cybersecurity in cloud computing and the BPMN's security extension works.

In this paper, we have highlighted the security needs and the challenges to be achieve for security governance in multi-cloud environment. Moreover, we have presented a BPMN metamodel with core element and extension that allows us to incorporate security requirements into the Business Process Diagrams considering the multi-cloud specificity. With this extension, the proposed framework can pilote security to achieve Multi-cloud security governance.

Therefore, future work must be oriented to enrich the security requirements specifications with SLA consideration. Furthermore, we integrate the security requirements considering the multi-cloud context into SLA management in order to generate Multi-cloud security SLA.

References

1. Alzain, M.A., Pardede, E., Soh, B., Thom, J.A.: Cloud computing security: from single to multi-clouds. In: HICSS, pp. 5490–5499. IEEE Computer Society (2012)
2. Alzain, M.A., Soh, B., Pardede, E.: A survey on data security issues in cloud computing: from single to multi-clouds. JSW **8**(5), 1068–1078 (2013)
3. Shei, S., Kalloniatis, C., Mouratidis, H., Delaney, A.: Modelling secure cloud computing systems from a security requirements perspective. In: Trust, Privacy and Security in Digital Business - 13th International Conference, TrustBus 2016, Porto, Portugal, 7–8 September 2016, Proceedings, pp. 48–62 (2016)
4. Damasceno, J.C., Lins, F.A.A., Medeiros, R.W.A., Silva, B.L.B., Souza, A.R.R., Aragão, D., Maciel, P.R.M., Rosa, N.S., Stephenson, B., Li, J.: Modeling and executing business processes with annotated security requirements in the cloud. In: ICWS, pp. 137–144. IEEE Computer Society (2011)
5. Ficco, M., Palmieri, F., Castiglione, A.: Modeling security requirements for cloud-based system development. Concurrency Comput. Pract. Experience **27**(8), 2107–2124 (2015)
6. Goettelmann, E., Mayer, N., Godart, C.: Integrating security risk management into business process management for the cloud. In: CBI (1), pp. 86–93. IEEE Computer Society (2014)
7. Lins, F.A.A., Medeiros, R.W.A., Silva, B.L.B., Souza, A.R.R., Aragão, D., Damasceno, J.C., Maciel, P.R.M., Rosa, N.S., Stephenson, B., Li, J.: Ssc4cloud tooling: an integrated environment for the development of business processes with security requirements in the cloud. In: SERVICES, pp. 53–60. IEEE Computer Society (2011)
8. Oberle, K., Fisher, M.: ETSI CLOUD – initial standardization requirements for cloud services. In: Altmann, J., Rana, O.F. (eds.) GECON 2010. LNCS, vol. 6296, pp. 105–115. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-15681-6_8
9. Fan, W., Perros, H.: A novel trust management framework for multi-cloud environments based on trust service providers. Knowl. Based Syst. **70**, 392–406 (2014)
10. Labda, W., Mehandjiev, N., Sampaio, P.: Modeling of privacy-aware business processes in BPMN to protect personal data. In: Proceedings of the 29th Annual ACM Symposium on Applied Computing, pp. 1399–1405. ACM (2014)
11. Singhal, M., Chandrasekhar, S., Ge, T., Sandhu, R., Krishnan, R., Ahn, G.J., Bertino, E.: Collaboration in multicloud computing environments: framework and security issues. Computer **46**(2), 76–84 (2013)
12. Sandkuhl, K., Matulevicius, R., Kirikova, M., Ahmed, N.: Integration of it-security aspects into information demand analysis and patterns. In: BIR 2015, vol. 1420, pp. 36–47 (2015)

13. Firesmith, D.: Specifying reusable security requirements. J. Object Technol. **3**(1), 61–75 (2004)
14. Maines, C.L., Llewellyn-Jones, D., Tang, S., Zhou, B.: A cyber security ontology for BPMN-security extensions. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), pp. 1756–1763. IEEE (2015)
15. Hoener, P.: Cloud computing security requirements and solutions: a systematic literature review. B.S. thesis, University of Twente (2013)
16. Iankoulova, I., Daneva, M.: Cloud computing security requirements: a systematic review. In: 2012 Sixth International Conference on Research Challenges in Information Science (RCIS), pp. 1–7. IEEE (2012)
17. Bernsmed, K., Meland, P.H., Jaatun, M.G.: Cloud security requirements-a checklist with security and privacy requirements for public cloud services (2015)
18. Rodríguez, A., Fernández-Medina, E., Piattini, M.: A BPMN extension for the modeling of security requirements in business processes. IEICE Trans. **90-D**(4), 745–752 (2007)
19. Naveed, R., Abbas, H.: Security requirements specification framework for cloud users. In: Park, J., Stojmenovic, I., Choi, M., Xhafa, F. (eds.) Future Information Technology, pp. 297–305. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-40861-8_43
20. Brucker, A.D., Hang, I., Lückemeyer, G., Ruparel, R.: SecureBPMN: modeling and enforcing access control requirements in business processes. In: 17th ACM Symposium on Access Control Models and Technologies, SACMAT 2012, Newark, NJ, USA, 20–22 June 2012, pp. 123–126 (2012)
21. Lodderstedt, T., Basin, D., Doser, J.: SecureUML: a UML-based modeling language for model-driven security. In: Jézéquel, J.-M., Hussmann, H., Cook, S. (eds.) UML 2002. LNCS, vol. 2460, pp. 426–441. Springer, Heidelberg (2002)
22. Cherdantseva, Y.: Secure*BPMN: a graphical extension for BPMN 2.0 based on a reference model of information assurance & security. Ph.D. thesis, Cardiff University, UK (2014)
23. Cherdantseva, Y., Hilton, J.: A reference model of information assurance & security. In: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), pp. 546–555. IEEE (2013)
24. Salnitri, M., Dalpiaz, F., Giorgini, P.: Modeling and verifying security policies in business processes. In: Bider, I., Gaaloul, K., Krogstie, J., Nurcan, S., Proper, H.A., Schmidt, R., Soffer, P. (eds.) BPMDS/EMMSAD -2014. LNBIP, vol. 175, pp. 200–214. Springer, Heidelberg (2014)
25. Goettelmann, E., Dahman, K., Gateau, B., Godart, C.: A formal broker framework for secure and cost-effective business process deployment on multiple clouds. In: Nurcan, S., Pimenidis, E. (eds.) CAiSE Forum 2014. LNBIP, vol. 204, pp. 3–19. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-19270-3_1
26. Nacer, A.A., Goettelmann, E., Youcef, S., Tari, A., Godart, C.: Obfuscating a business process by splitting its logic with fake fragments for securing a multi-cloud deployment. In: 2016 IEEE World Congress on Services (SERVICES), pp. 18–25. IEEE (2016)
27. Firesmith, D.: Engineering security requirements. J. Object Technol. **2**(1), 53–68 (2003)