International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:12, No:8, 2018

SeCloudBPMN: A Lightweight Extension for BPMN Considering Security Threats in the Cloud

Somayeh Sobati Moghadam

***Abstract*—**Business processes are crucial for organizations and help businesses to evaluate and optimize their performance and processes against current and future-state business goals. Outsourcing business processes to the cloud becomes popular due to a wide varsity of benefits and cost-saving. However, cloud outsourcing raises enterprise data security concerns, which must be incorporated in Business Process Model and Notation (BPMN). This paper, presents SeCloudBPMN, a lightweight extension for BPMN which extends the BPMN to explicitly support the security threats in the cloud as an outsourcing environment. SeCloudBPMN helps business's security experts to outsource business processes to the cloud considering different threats from inside and outside the cloud. In this way, appropriate security countermeasures could be considered to preserve data security in business processes outsourcing to the cloud.

***Keywords*—**BPMN, security threats, cloud computing, graphical representation.

I. Introduction

NOWADAYS, cloud computing is one of the trending topics in Information Technology (IT), which enables ubiquitous, convenient, on-demand services [1]. Business process outsourcing helps in cutting the cost of expensive information systems infrastructure and data management [2]. Besides the previously mentioned advantages, cloud computing provides higher availability, scalability, and more effective disaster recovery rather than in-house operations [3]. However, since businesss data is a very valuable asset for many organizations and businesses, data confidentiality and privacy is the most concern. Highly confidential data about a companys operations are sensitive and privacy should be preserved.

BPMN: Business Process Model and Notation (BPMN) is a standard for business process modeling [4]. BPMN describes the order of activities and provides a conceptual view of businesses and their objectives, which enables organizations and businesses identifying, monitoring, and optimizing their business. The main goal of BPMN is analysis and improvement of business processes. BPMN diagrams are represented as flowcharts, which connects activities in a business process. The standard BPMN does not provide a clear specification of security aspects in the cloud [5]. Indeed, addressing security issues is identified as one of the three major challenges of BPMN [6]. Hence, security should be integrated into BPMNs as an essential part of Information System (IS) [7]. When data are outsourced to the cloud, BPMN could be used to represent security-related problems and threats in the cloud.

S. Sobati-M. is with the University of Hakim Sabzevari, Sabzevar, Iran (e-mail: s.sobati@hsu.ac.ir).

Contribution: Since cloud computing is still immature, security concerns were not considered in the proposed secure BPMNs, i.e., business process annotated with security information [8], in the literature . Business experts have essential security knowledge, but security in the context of cloud computing faces different challenges which should be considered and be involved in the design of secure business processes in the cloud. Even tough, many researches extended BPMN to address security requirements, but there are still some specific security aspects that are not considered because these models'primary concern is not the cloud threats [5]. In the other word, designing a secure businesses processes in the cloud is still a challenge. To overcome this shortage, in this paper, we propose SeCloudBPMN, a lightweight BPMN extension for graphical security threat representation, which enables to incorporate security requirement into business process diagrams in the cloud computing context. We consider security requirements related to the unreliability of the cloud environment.

II. Secure BPMN for Cloud Computing (SeCloudBPMN)

SeCloudBPMN introduces new graphical elements for visualization different security threats and security breaches for a cloud-based business process model (listed in Fig. 1). The propose of security in the cloud is to keep information in all its locations (within and outside the cloud) and consequently, an IS , where information is created, processed, stored, transmitted, free from threats. In the cloud scenarios, in addition to outsiders, there is also security threats from insiders. Since data and information is stored and processed in the cloud, the cloud service provider's employees are another threat who have access to data and a great opportunity to disclose security [9]. The cloud service provider faithfully complies to any service-level agreement and runs queries and provides results without alteration in computation and storage services, but a malicious insider may sends malicious codes, which results in data corruption [10]. Even though a honest cloud service provider's employee may attempt to gather some information about stored data. Hence, the honest employee sends analytical queries and gets the result and sales the result for its nefarious purposes.

III. Threat Modeling with SeCloudBPMN

In this section, first we describe a cloud outsourcing scenario (represented in black in Fig. 2). Within this scenario, we explain different security threats listed in Fig.

Threat	Description	Notation
Malicious exploitation	When private data sold out without authorization for some nefarious purposes	
Data Corruption	When stored data is altered or deleted by malicious codes	
Privacy breach	When data is accessed by unauthorized outsiders	
Session hijacking	An established session is exploited by an attacker	

Fig. 1 Security annotations in SeCloudBPMN: Elements, descriptions and their graphical syntax

1 (represented in red in Fig. 2) which may compromise data security in this scenario.

Consider a scenario in which an organization (presented as the BPMN pool *Organization*) would like to outsource data storage and computation to a Cloud Service Provider (CSP) (pool *Cloud service provider*). In order to send data, the organization sends a request to the storage service (lane *storage service*) with an inquiry to the storage system administrator, which verifies the request. If the request is accepted, the administrator sends a confirmation to the organization. Otherwise, the organization gets a notification about the failure. Then, data can be sent to the cloud (task *store data*) to store in a database at the storage service. During this phase, a session is established between the organization and the CSP (lane *Established session*). After storing data at the CSP's, the organization wishes to execute some computations over stored data. The organization sends a query to the computation service (lane *computation service*). Once the request is verified by the computation service administrator, the query is accepted and is sent to the storage service. The query is executed and requested data is retrieved and the query result is sent back to the organization.

In this scenario, there exist potential threats, which threaten the security of organization's data (represented with red color in Fig. 2).

Let's say, that there exists an outsider, i.e., an attacker from outside the cloud (presented in red pool *Outsider*) and also an insider, i.e., an attacker inside the cloud (presented in red pool *Insider*). A malicious insider may send malicious codes to the database to manipulate, modify, delete or alter data. If the insider is not malicious (it is called curious insider), he/she would like to get extra information about data. These attackers may cause different threats listed in Fig. 1, which we describe in the following subsections.

A. Data Corruption

The insider (lane Insider) may causes malicious exploitation or data corruption. Since the insider, e.g., the CSP, has access to stored data at the cloud, may attempt to exploit data for its nefarious purposes. A malicious insider tries to manipulate data (task *Intent to manipulate data*). To this end, the malicious insider sends malicious codes to the database in the storage service to infect data, which lead to data corruption.

B. Malicious Exploitation

Data corruption occurs by curious (not malicious) insider. The insider intents to extract some information about outsource data. The insider creates analytical queries and sends to the computation service administrator. Sine the query is sent from inside the cloud, it looks like an ordinary query, which is sent by the organization. After accepting the query, the administrator sens it to the database, the results are extracted and sent back to the insider.

C. Privacy Breach

Privacy breach happens when data is accessed by unauthorized users (lane *Malicious attacker*). The outsider breaks to the storage service and then has access to all data stored at the CSP's. The outsider uses DBMSs (Data Base Management System) bugs and uses these vulnerabilities to get root access to the database. After getting root access, the outsider has full access to stored data.

D. Session Hijacking

An outsider, is also known as man-in-the-middle attacker, attempts to hijack an established session between the organization and the CSP and gets information being passed. This happens when unsafe protocols is used between the organization and the CSP. The outsider would try to get information passed. When data is sent to the CSP by the organization, the outsider which sees all the passed messages and data, gets them and causes privacy breach.

IV. Conclusion and Future Works

BPMN is a visualization language for business processes modeling, which allows to incorporate security requirements in the cloud. This paper, introduces SeCloudBPMN, a BPMN extension which integrates security threats in the cloud environment into business process diagrams. The BPMN is extended in order to illustrate and express security threats in the cloud. In this way, business's security experts would be able to consider different security countermeasures in their end product.

The next step, should be proposing a secure-enabled BPMN with new security notations for the cloud and then transforming this model into a concrete model, which can be implemented in real world practical scenarios. For security threats represented in SeCloudBPMN, new security notations

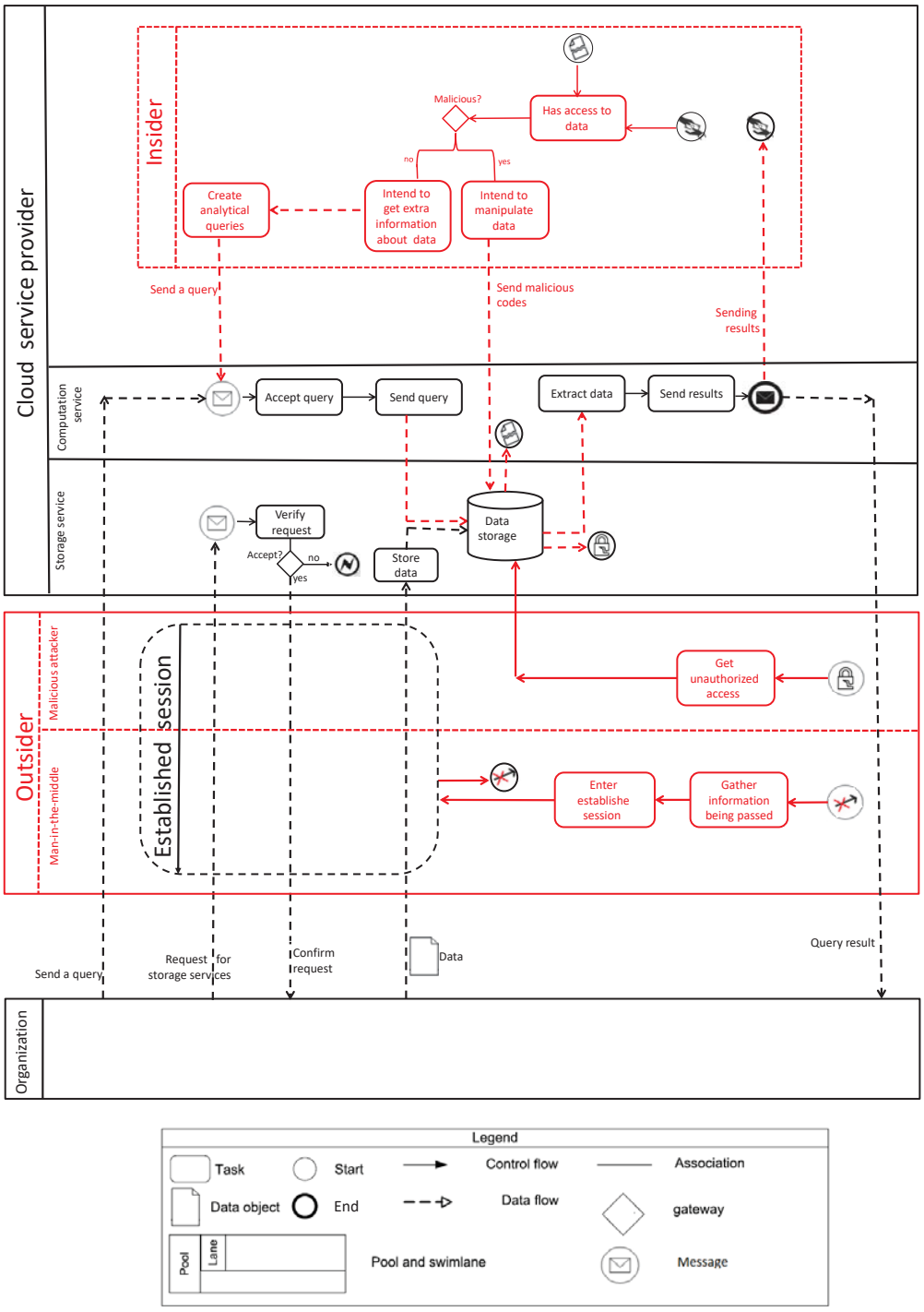

Fig. 2 Security threats in the cloud business processes

would be introduced to represent required countermeasures for each security threat. For instance, for privacy breach data encryption can be implemented to protect data privacy. Moreover, the proposed model must be extended to incorporate other security aspects such as access control, integrity, and availability checking. Access control policies specify allowed operations based on job functions within an organization.

REFERENCES

[1] S. Sobati-Moghadam and A. Fayoumi, "Private collaborative business benchmarking in the cloud," in *Computing Conference 2018. London, UK*. IEEE Xplore, 2018.

[2] E. Shi, J. Bethencourt, T.-H. Chan, D. Song, and A. Perrig, "Multi-dimensional range query over encrypted data," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 2007, pp. 350–364.

[3] E. Damiani, S. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Key management for multi-user encrypted databases," in *Proceedings of the 2005 ACM workshop on Storage security and survivability*. ACM, 2005, pp. 74–83.

[4] OMG, *Business Process Model and Notation (BPMN), Version 2.0*, Object Management Group Std., Rev. 2.0, January 2011. [Online]. Available: http://www.omg.org/spec/BPMN/2.0

[5] M. Rekik, K. Boukadi, and H. Ben-Abdallah, "Towards outsource-ability enabled BPMN," in *ICSOFT-EA 2015 - Proceedings of the 10th International Conference on Software Engineering and Applications, France, 20-22 July,*, 2015, pp. 5–14. [Online]. Available: https://doi.org/10.5220/0005513500050014

[6] Y. Alotaibi, "Business process modelling challenges and solutions: a literature review," *Journal of Intelligent Manufacturing*, vol. 27, no. 4, pp. 701–723, Aug 2016. [Online]. Available: https://doi.org/10.1007/s10845-014-0917-4

[7] A. Goldstein and U. Frank, "A language for multi-perspective modelling of it security: Objectives and analysis of requirements," in *Business Process Management Workshops*, M. La Rosa and P. Soffer, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 636–648.

[8] T. Neubauer, M. Klemen, and S. Biffl, "Secure business process management: A roadmap," in *Proceedings of First International Conference on Availability, Reliability and Security, ARES*, 2006.

[9] D.-H. Yang, S. Kim, C. Nam, and J.-W. Min, "Developing a decision model for business process outsourcing," *Comput. Oper. Res.*, vol. 34, no. 12, pp. 3769–3778, Dec. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.cor.2006.01.012

[10] S. Sobati-M, J. Darmont, and G. Gavin, "Enforcing privacy in cloud databases," in *Big Data Analytics and Knowledge Discovery - 19th International Conference, DaWaK 2017, Lyon, France, August 28-31, 2017, Proceedings*, ser. Lecture Notes in Computer Science, L. Bellatreche and S. Chakravarthy, Eds., vol. 10440. Springer, 2017, pp. 53–73.