Study of Security Issues in Platform-as-a-Service (PaaS) Cloud Model

Walter Isharufe
Concordia University of Edmonton
Alberta, Canada
wisharufe@student.concordia.ab.ca

Fehmi Jaafar
Computer Research Institute of Montreal
Quebec, Canada
fehmi.jaafar@crim.ca

Sergey Butakov
Concordia University of Edmonton
Alberta, Canada
sergey.butakov@concordia.ab.ca

***Abstract* – Security is one of the key considerations when businesses look to adopt cloud models like Platform as a Service (PaaS). The main concern comes from the fact that business losses total control of deployed applications and data, leaving that trust in the hands of the Cloud Service Providers (CSP). Although CSPs put some level of security controls in place, it is ultimately the responsibility of the client to verify the presence of the controls and verify the suitability of their security needs. It is also the user's responsibility to ascertain compliance with these offerings to appropriate standards before patronage. This paper reviewed various security issues inherent in the PaaS cloud model, classified them according to the essential cloud characteristics and finally recommended high-level solutions to the identified security issues. The result of the review and recommendations provided can serve as a reference for organizations and individual users when deciding security needs and service level objectives for PaaS based deployments.**

Keywords – Cloud computing, Platform as a Service, Multitenancy Virtualization.

I. INTRODUCTION

In a traditional approach, organizations purchase software to develop and run business applications and hardware to host applications. Thus, organizations have to face responsibility and cost of maintaining these systems. Cloud computing paradigm may help to reduce such costs. With Platform as a Service (PaaS) cloud model, organizations can focus on the development of applications without worrying about servers and other infrastructure needed to develop and deploy applications. Indeed, the Cloud Service Provider (CSP) provides programming language, middleware, database, operating systems/virtual machine, servers, storage, networks and other services.

Despite its appealing benefits, the security of PaaS service model is one of the key concerns for prospective adopters. In a traditional setting where IT systems are resident in the organization's premise, the IT department and other users are responsible for ensuring adequate security mechanisms are in place whereas in a cloud setting, this responsibility is shifted to the CSP [1]. Clients require assurance of the security of their assets in the cloud and certainty of the security controls put in place by the CSP.

In cloud computing, responsibility for security and privacy is shared between the users and the CSPs. For PaaS, the application developers are responsible for ensuring security in their application while the CSP is to ensure proper isolation from other user applications and the overall security of the application environment [2].

A number of researchers have investigated security issues in the cloud environment. This paper focuses on the security of the PaaS cloud model. A systematic review of literature was carried out to identify and analyze critical security issues that can deter the use of the model. These issues are classified according to the five essential cloud characteristics from which they derive their root causes. It is important to note that the essential characteristics of cloud are made possible by some existing technologies such as virtualization, which has its specific vulnerabilities. Furthermore, a review of the security structure of Amazon Web Service (AWS) platform was done and result was presented by using a security framework designed by the authors in [1]. Selection of AWS was determined by Rightscale report showed that AWS was the most widely used (57%) over other vendor provisions [3].

The rest of this paper is organized as follows: Section II provides an overview of PaaS and discusses some of the benefits of PaaS. Section III presents a summary of some of the related work. Section IV discusses the methodology used in this study. Section V presents the analyses and discussion of identified security issues, security requirements and recommended countermeasures. Finally, section VI concludes the work and presents potential directions for future research.

II. BACKGROUND

The National Institute of Standards and Technology (NIST) defines PaaS as "the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider" [4]. PaaS is one of the three service models of cloud computing: it resides in-between Software as a Service (SaaS) and Infrastructure as a Service

978-1-7281-7116-6/20/$31.00 ©2020 IEEE

(IaaS) models. All the three service models are dependent on one another. IaaS provides the physical computing capabilities needed for the application development; deployment and hosting environment (PaaS) which is needed to host a SaaS application. According to user preference for environment, size and ease of access, PaaS can be deployed as public, private or hybrid cloud services. Public deployment is more cost-effective compared to private cloud as it involves sharing of resources hosted by the cloud provider with other users. In a hybrid deployment, organizations can house the more sensitive applications and data in their private domain and the less sensitive ones will be hosted in the public domain [5].

PaaS is mainly targeted at application developers although some offerings cater to operators. Some of the advantages of PaaS are reduced total cost of ownership, a faster time to market, scalability, self-service with reduced administration cost, team collaboration support [5]. All cloud deployment models carry unique characteristics and control requirements from the security standpoint. Such characteristics drive the necessity for a careful review as discussed in the following section.

III. Related Work

Authors of [6] reviewed several security concerns in the service models. In SaaS model, the user has no control over the application, the deployment environment or the underlying infrastructure. Thus, the responsibility of providing security lies on the CSP. Issues such as SQL injection flaws, access control weaknesses, cookie manipulation and some other potential issues that may affect the SaaS model were identified. The authors stressed on the need to secure the enterprise service bus (ESB) in the PaaS model and the need for hypervisor and physical security in IaaS. While [6] attempted to survey security issues in each of the three service models, however, the paper places more emphasis on SaaS and provides little on PaaS and IaaS. In addition, paper does not focus on countermeasures for potential security problems in PaaS.

The authors in [7] looked at Service Oriented Architecture (SOA) related security issues and API security issues which are peculiar to PaaS. The authors recommended mutual authentication and use of OAuth to prevent attacks such as input validation and XML attack. OWASP in [8], highlighted business continuity and disaster recovery, lack of secure software development lifecycle, vendor lock in, lack of adequate provisions in SLA, meeting compliance demands and control risks as the five main concerns in PaaS. This research reviewed some of the highlighted issues and recommended some controls.

An ISACA publication titled the "Security Mysteries in the Cloud" [9] outlined some security concerns in PaaS which are difficulty of securing distributed data, access privilege granted in debug mode that can be exploited and default ports for example, port 50070 used by distributed file systems such as Hadoop that can serve as attack vectors.

Virtualization is one of the key technologies in cloud computing. Resource provisioning, scaling and multitenancy is made possible with virtualization. In [10], the authors proposed the use of a constraint solver called "sugar" to monitor and detect VPN and IPsec configuration changes in virtual machines (VM) during VM migration. However, the paper did not describe vulnerabilities and threats in the technology. Authors in [11] focused on how virtualization-related security issues such as VM hoping, VM diversity, VM mobility issues affect the three service models. Countermeasures to address all the identified issues were not discussed in detail.

The authors in [12], discussed cryptographic and non-cryptographic methods such as Data Capture and Auto Identity Reference (DACAR) for preserving privacy of health records. Nonetheless, the authors focused mainly on privacy alone and did not extensively cover other important security concerns such as integrity and availability.

The authors in [13] examined issues of confidentiality, privacy, integrity in cloud computing and recommended some preventive and detective measures to counter these issues. The paper nevertheless, left out the issues that affect availability of resources. Authors in [14] stressed on the need to address multitenancy and authentication issues in service level agreement. Both papers presented security issues from a general cloud perspective and did not describe how the issues affect each of the cloud models.

In [15], the authors proposed the use of a mobile phone application to generate one time password (OTP) for login in the cloud. However, the authors did not discuss how the confidentiality of the tokens would be preserved in a case where it is synchronized across multiple devices belonging to the user. In a previous work, the authors [16] proposed an Information Flow Control (IFC) model similar to the use of sticky policy presented in [17] to control how data is shared and used different applications hosted in a PaaS offering. The authors focused only on confidentiality preservation and paper did not present a discussion on the threats and vulnerabilities that require addressing.

The authors in [18] studied the issues spanning from four of the five characteristics of cloud computing which pose concerns for access control and privacy. They surveyed the issues of vulnerable host, objects and lack of interoperability due to the use of heterogeneous hosts/ host components (Resource pooling and rapid elasticity characteristics); the need for communication confidentiality as endpoints connect to the PaaS service (Broad Network Access). The authors also discussed privacy during authentication, integrity of logs and the use of "byzantine quorum" for service continuity and fault tolerance. Our paper follows the approach used by the authors in [18]. However, the authors left out the issues that arise from the on-demand characteristic of cloud computing. On demand self-service includes a web portal

where prospective customers can provide themselves with PaaS cloud service. This interface can be abused by a malicious user and web attacks can be carried out through this interface. Thus, it is important to discuss the issues introduced by this essential characteristic alongside other issues arising from the other four characteristics.

This research attempts to bridge these gaps by studying various ways by which all the five essential characteristics of cloud computing can introduce vulnerabilities in a PaaS system and map required controls to identified issues. Table I contains a taxonomy of security issues propagating from the five essential characteristics and mitigation recommendations.

IV. REVIEW OF PAAS SECURITY

A. Approach

We examined in this paper the security concerns in public PaaS and we studied controls according to requirements from the CSA cloud control matrix. Finally, we provided recommendations for solving identified issues. The following steps have been performed to achieve the objectives of the research: we conduct a review of related works and the Cloud Standards Customer Council (CSCC) PaaS guide [5] to understand the PaaS architecture and identify potential security risks and vulnerabilities in PaaS. We classified identified security issues based on the five essential cloud characteristics. Appropriate controls from the CSA cloud control matrix were mapped to identify risks that threaten the security of user objects (data and application files) in the three layers of PaaS. Then, we presented the set of mitigation steps and the CSA cloud matrix requirements.

B. Essential Cloud Characteristics and Security Issues

There are five essential characteristics of cloud computing. Unfortunately, these characteristics introduce risks that are unfamiliar to information technology professionals [18]:

- On-demand self-service: a feature that allows users to request and manage required services via web portals and management interface without physically interacting with service providers. These interfaces are prone to attacks that can result in unauthorized access if not properly managed.
- Broad network access: attackers can exploit vulnerabilities such as improper SSL configuration to carry out man-in-the-middle attack. Specific tools can be used by an attacker to intercept and modify HTTPS traffic and gain unauthorized access into a PaaS web application [19]. If successful malicious code is injected into the PaaS environment, this will create damage to user applications and infrastructural resources in the back end.
- Resource pooling: resources such as containers, VMs, CPU, and disks are grouped and shared among multiple user applications. Side channel attacks can occur if the resources are not properly isolated and protected.
- Rapid elasticity: based on demand, resources are provisioned (scaled up) and de-provisioned (scaled down). A resource can be reallocated to another user. It is possible for the new user to recover previous user's data from memory if the right measures are not taken.
- Measured service: the cloud service provider constantly monitors and measures resource usage for billing, optimization and reporting. If these resources are not protected from malicious users, data used in billing can be manipulated.

C. Security Issues in PaaS Layers

PaaS structure can be divided into three layers [20]: the front-end layer where it interfaces with SaaS, the middle layer where apps are stored, runtime, database management software, and middleware resides, and finally the back end where database storage, networking components, object storage, server, CPU resides. A PaaS architecture model is shown in Figure 1.

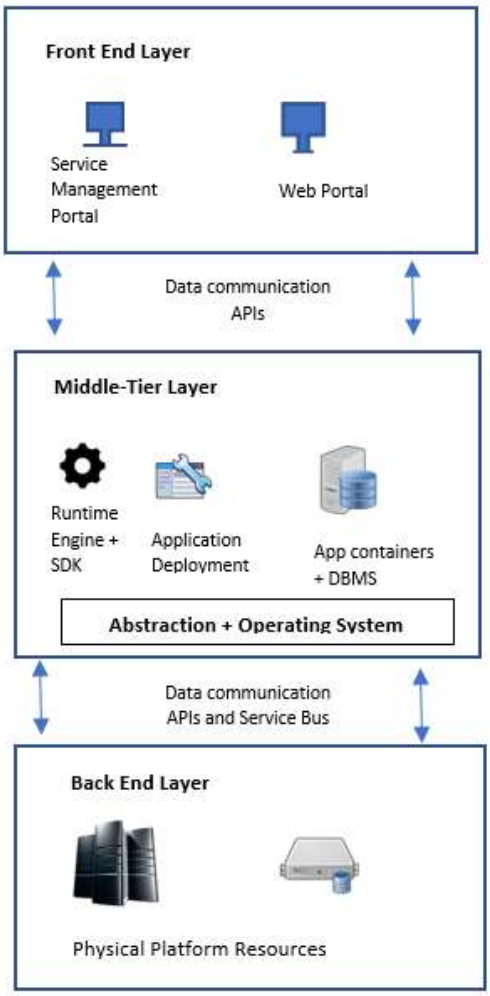

Figure 1: PaaS Architecture Reference Model [20]

TABLE I. SUMMARY OF THE LITERATURE REVIEW

Authors	Issues Covered	Solution Approach/ Recommendations	Gap Analysis/Limitations
Khara, S and Gupta, A [13]	Confidentiality, integrity, privacy and authentication issues in cloud computing	Preventive measures such as encryption before outsourcing, use of multimodal biometric; and detective measures such as the use of intrusion detection.	Issues that affect availability were not covered. Recommendations were mostly technical.
Mohamed Al Morsy [7]	SOA related issues such as MITM, XML, replay, injection and input validation	Mutual authentication, authorization and Web Service Security. Open Authentication (OAuth) in APIs to enforce authentication and authorization.	The issue of data privacy/or data misuse with the application of OAuth was not discussed.
Basim Alhadidi [15]	Authentication	Use of mobile phones to generate One Time Password (OTP) used for login	Users cannot login if mobile phone is lost. Did not address the risk of authentication apps syncing tokens across different devices.
Thomas F. Pasquier et al. [16]	Fine-grained control of inter-application information in PaaS and isolation of applications.	Information Flow Control (IFC) model for applications with the use of tags/labels to describe data transfer/use policies among application processes.	Processing policy tags may affect performance The proposed model does not extensively cover the scenario where authorization problems may deter availability of data
Assad Abbas and Samee Khan [12]	Privacy-preserving methods for electronic health records in the cloud.	The use the Data Capture and Auto Identity Reference (DACAR) platform to ensure privacy in the transfer and processing of electronic health records.	The paper focused mainly on privacy and does not extensively cover other important security issues.
Arash Eghtesadi et al. [10]	Detecting and preserving security configurations in virtual machines during migration.	Proposed the use of a constraint solver-Sugar fed with formulas to detect and verify intrusion monitoring and IPsec protection preservation before and after VM migration	Focus was exclusively on integrity preservation during VM migration.
Rong et al. [14]	Lack of standards and authentication issues.	Security mechanisms that should be included in service level agreement (SLA).	Focus was mainly on security issues and less on solutions.
Mehmet Sandikkaya et al. [18]	Interoperability issues and mutual vulnerability of host due to resource pooling and rapid elasticity characteristic.	PaaS design that includes policy enforcement points, trusted computing base (TCB) to evaluate request via service calls, sticky access policy encapsulated with user objects, mechanism for mutual authentication, and the use of Transport Layer Security (TLS) for confidential communication.	No discussion on issues posed by on-demand service characteristics. The solution proposed did not entirely follow a defense-in-depth approach. Did not discuss specific threats to PaaS layers.
Hsin-Yi Tsai et al. [11]	Virtualization related issues such as VM hopping and VM mobility	Proper patch management and emphasized the importance of a clearly defined service level agreement (SLA)	Focus was on virtualization related issues only. Issues that affect virtualization may ultimately affect PaaS
Subashini and V. Kavitha [6]	Data segregation, data locality, securing ESB and the hypervisor.	Security testing and input validation for web application front -end access. The need for reliability on location of customer data.	Countermeasures were not presented. Only testing and validation were recommended.

The probability that unauthorized access to web portal/console and management interface (which resides in the front end) can occur in the cloud environment is higher than in a traditional system accessed by a limited number of administrators [21]. Vulnerabilities in the front-end layer can be exploited to gain access through attacks such as cross-site scripting, SQL injection, cross-site request forgery, brute-force attacks, etc. The middle tier which houses the operating system, runtime environment, containers and applications can be exposed to malware, exploitation of configuration weaknesses by attackers, cross-tenant attacks, etc. The back end which comprises physical storage, computing and networking devices need to be protected from unauthorized access, damage, power outages and natural disasters.

D. Issues Assessment

Assessment of the issues can be done using the following two factors:

- Likelihood of occurrence: this indicates the probability that a given threat will exploit the vulnerability in an identified asset. A value of low, medium or high is assigned according to the level of possibility.
- Impact: this indicates the effect on an asset. The effect can be the distortion of confidentiality, integrity and availability of data and services.

The likelihood and impact value can be based on expert opinion. Different factors such as industry environment, technology in place, mode of deployment, motivation and skill level of threat-agent can determine the level of likelihood of a vulnerability to be exploited.

For instance, according to OWASP [22], two sets of factors can determine likelihood of occurrence. The first is threat-agent factors: skill-level, motive, opportunity and size of the group of threat agents. The second set is vulnerability factors such as ease of discovery, ease of exploit, level of awareness to the threat agents, and likelihood of the exploit to be detected.

TABLE II. PAAS SECURITY ISSUES AND RECOMMENDATION

Security Issue	Vulnerability	Security element affected	Layer	Likelihood of Occurrence	Impact	CCM V3.0 Control ID	Recommended Mitigation Technique
Cloud Characteristic: On Demand Self-Service [ODSS] ***Description:*** *services can be provisioned to users without human interaction via web portals and self-service management interfaces provided by CSP. The security of the portal and interface is important as malicious users can use them as attack vectors.*							
Unauthorized access, Account hijacking, SAML attack	Weak authentication mechanism, insecure permissions, insecure default application configuration [25]	Confidentiality	Front end	Expert Opinion	Expert Opinion	IAM-02, IAM-05, IAM-09	***Technical*** Proper Identification and access management control - two-factor authentication SAML 2.0 for carrying authentication and authorization information, Use of Terminal Access Controller Access Control System plus (TACACS+) as it encrypts entire authentication process over RADIUS that encrypts only password. Use of Role Based Access Control (RBAC), least privilege access
							Operational Change default application settings such as database access password settings e.g. in .NET config file Awareness and training on the need for security There should also be a credential revocation policy with a short time period. If possible same day a staff is terminated from the job.
							Administrative Strong password policy, strong character combinations, etc. Risk and vulnerability assessment at least quarterly Pen testing to determine exploitability through client side applications

E. Mapping security issues to CSA cloud control matrix requirements

After identification and analysis of security issues, control requirements based on the cloud security alliance (CSA) cloud control matrix has been labeled. Identified issues are then mapped to specific control requirements. The document below provides a list of requirements for the three service models, SaaS, PaaS and IaaS covering sixteen domains. For this paper, the CSA CCM version 3.0.1 was used. Version 3.0.1 contains three new control domains namely mobile security, supply chain management, transparency and accountability; and interoperability and portability. Description of each control requirements mapped to identify issues can be found in the CSA CCM document.

F. Security Issues and Recommendations

Table II presents identified security issues classified under the on-demand self-service characteristic of cloud computing with the layers denoted in figure 1. We mapped the applicable control requirements under the sixteen domains of the CSA cloud control matrix are to the specific identified issues. Finally, we presented recommendations, divided into technical, operational and application[1].

As seen in Table II, certain issues such as unauthorized access, account hijacking and a host of others may arise from the "on-demand" characteristic of cloud computing.

On demand self-service characteristic involves providing cloud service users a management interface/ console via which they can provide services such as server instances, application servers and dependencies. If a cloud service user is not careful authenticated with his/her login credentials, a malicious user can gain access into the platform and perform malicious actions such as code modification, insert malware and other actions that may ultimately cause great havoc to customer applications and even the cloud system. This can result to financial loss, litigation cases, and reputation loss to both the cloud service customer and the provider. A real-life instance occurred in June 2014 when an unauthorized user gained administrative access into Code Spaces AWS EC2 console. The attacker demanded for ransom and deleted most of the company's data when it failed to comply with the demands. The company failed to make use of multi-factor authentication [23]. This event led to great financial and reputation loss for the organization and ultimately the closure of the company.

Organizations are at risk of such event presented above when they fail to provide the proper security measures. Depending on size of the business and sensitivity of

[1] See https://tinyurl.com/yayy4uvz for a full table taxonomy of PaaS security issues

applications deployed I the cloud, the impact of such an event can be enormous. To protect front-end features like the management console, the CSA requires certain Identity and Access management (IAM) controls requirement such as IAM 02, IAM 05 and IAM 09 presented in Table II to be implemented by the CSP and the service customer. This helps to ensure proper authentication and management of digital credential lifecycle of digital identity (human/device/process) [24]. As a recommendation, CSPs should provide technical controls such as multifactor authentication (MFA) and login credentials should be conveyed using latest security assertion markup language (SAML) version. On the other hand, the PaaS customers should implement strong password policies, perform regular vulnerability assessment and train employees how to control security issues.

V. Conclusion

This paper presented a study of critical security issues that affect the confidentiality, integrity and availability of user applications and data in the Platform as a Service model. We presented an overview of PaaS security issue and further discussed how the five essential characteristics of cloud computing can introduce vulnerabilities in different layers of the PaaS architecture. Identified security issues were classified according to the cloud characteristic from which they derive their root cause and control requirements from the CSA cloud control matrix were mapped to these issues. Additional research is needed to develop a standard PaaS architecture, which may help solve the issue of interoperability and vendor lock-in.

References

[1] Akinbi, A., Pereira, E., & Beaumont, C. (2012). Identifying security methods and controls for secure paaS cloud environments. In 14th Annual PGnet Symposium.

[2] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 8(6), 24-31.

[3] Weins, K. Cloud computing Trends: 2016 State of the Cloud Survey.

[4] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[5] Council, C. S. C. (2015). Practical Guide to Platform-as-a-Service.

[6] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

[7] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[8] OWASP-Cloud-Top 5 Risks with PAAS. (2009). [Online]. Available: https://www.owasp.org/index.php/Cloud_-_Top_5_Risks_with_PAAS. [Accessed 2017].

[9] Subramanian, S., & Munuswamy, D. Security Mysteries in the Cloud.

[10] Eghtesadi, A., Jarraya, Y., Debbabi, M., & Pourzandi, M. (2014, March). Preservation of security configurations in the cloud. In Cloud Engineering (IC2E), 2014 IEEE International Conference on (pp. 17-26). IEEE.

[11] Tsai, H. Y., Siebenhaar, M., Miede, A., Huang, Y., & Steinmetz, R. (2012). Threat as a service?: Virtualization's impact on cloud security. IT professional, 14(1), 32-37.

[12] Abbas, A., and Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics, 18(4), 1431-1441.

[13] Khara, S. and Gupta, A. (2017). Security Issues in Cloud,. International Journal of Innovations and Advancement in Computer Science, vol. 6, no.

[14] Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), 47-54.

[15] Alhadidi, B., Arabeyat, Z., Alzyoud, F., & Alkhwaldeh, A. (2016). Cloud Computing Security Enhancement by Using Mobile PIN Code. JCP, 11(3), 225-231.

[16] Pasquier, T. F. M., Singh, J., & Bacon, J. (2015). Information flow control for strong protection with flexible sharing in paas. In Cloud Engineering (IC2E), 2015 IEEE International Conference on (pp. 279-282). IEEE.

[17] Pearson, S., & Casassa-Mont, M. (2011). Sticky policies: an approach for managing privacy across multiple parties. Computer, 44(9), 60-68.

[18] Sandikkaya, M. T., & Harmanci, A. E. (2012). Security problems of platform-as-a-service (paas) clouds and practical solutions to the problems. In Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on (pp. 463-468). IEEE.

[19] El ‐ Hajj, W. (2012). The most recent SSL security attacks: origins, implementation, evaluation, and suggested countermeasures. Security and Communication Networks, 5(1), 113-124.

[20] Akinbi, A., & Pereira, E. (2015, October). Mapping Security Requirements to Identify Critical Security Areas of Focus in PaaS Cloud Models. In Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (pp. 789-794). IEEE.

[21] Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50-57.

[22] OWASP, (2016). OWASP Risk Rating Methodology. [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[23] C. S. A. (CSA). (2016)The Treacherous 12: Cloud Computing Top Threats in 2016.

[24] Priya, N. P. C., & Prabakaran, N. (2012). Security Management in Inter-Cloud. International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), 1(3), 233-235.

[25] Theoharidou, M., Tsalis, N., & Gritzalis, D. (2013, June). In cloud we trust: Risk-Assessment-as-a-Service. In IFIP International Conference on Trust Management (pp. 100-110). Springer, Berlin, Heidelberg.