Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 94 (2016) 485 – 490

Procedia Computer Science

The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies (IoTNAT' 2016)

Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework

Nabeel Khan[a], Adil Al-Yasiri[b]*

[a]University of Salford, 43 Cresent Salford, Manchester and M5 4WT, United Kingdom
[b]University of Salford, 43 Cresent Salford, Manchester and M5 4WT, United Kingdom

Abstract

Cloud Computing allows firms to outsource their entire information technology (IT) process, allowing them to concentrate more on their core business to enhance their productivity and innovation in offering services to customers. It allows businesses to cut down heavy cost incurred over IT infrastructure without losing focus on customer needs. However, to a certain limit adopting Cloud computing has struggled to grow among many established and growing organizations due to several security and privacy related issues. Throughout the course of this study several interviews were conducted, with cloud developers and security experts, and the literature was reviewed. This study enabled us to understand, current and future, security and privacy challenges with cloud computing. The outcome of this study led to identification of total 18, current and future, security issues affecting several attributes of cloud computing.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Cloud Computing; Security; Vulnerabilities; Threats.

1. Introduction

The scalability and extensibility of distributed software architectures have led to the concept called Cloud Computing. Cloud computing is a technology used to deliver the hosted services over the Internet. Through this technology, users don't have to manage their own IT resources; instead they purchase their IT needs as services over the internet [1].

* Corresponding author. Tel.: +44-161-295-6399
E-mail address: a.al-Yasiri@salford.ac.uk

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.08.075

Cloud computing main objective is to provide secure, quick and convenient data storage with all services delivered over the internet. Cloud computing has a distributed architecture and contains a computational paradigm which enables it to enhance availability, scalability, agility, collaboration and adaptability of the system. Cloud computing technology allows in reducing the rates spent on computing infrastructure, boosting performance and increasing efficiency of an organization [2, 3].

Cloud has many specific attributes compared to many traditional technologies such as huge pool of resources and mostly belonging to cloud providers are heterogeneous, distributed and completely virtualized. It's because of this reason traditional security measures like identification, authentication and authorization is not enough in case of cloud computing [4]. Security controls and mechanisms in traditional IT is more or less very similar and useful to that of current form of cloud for most of its delivery models. But, cloud computing presents different organizational risks than traditional IT due to its ways of service deployment, operations and enabling technologies. Unfortunately, security integration into these services often makes it more difficult to provide more substantial solution to the problem [5].

Moving organization's critical applications and legacy database full of sensitive information to cloud service provider (CSP) with no control of their own data is a concern of many organizations. To diminish this concern, CSP must ensure that they continue to provide customers with same security and control to their applications and sensitive data as onshore system. In order to achieve this CSP must provide evidence to a customer that all service level agreements are met and compliance can be proved to auditors[6].

We have tried to present security issues related to cloud computing based on service delivery models i.e. security issues with software as a service, platform as a service and infrastructure as a service. Also, we have identified vulnerabilities and threats in cloud computing which leads to these security issues, where vulnerabilities refers to gaps in a system which allows attack to be successful and threats refers to an attack which is attempted on gaps in a system to exploit resources or information. By addressing these issues we are trying to strengthen cloud computing adoption framework's organizational preparedness section. As security is considered to be the most viable threat to cloud adoption, it is very important to add enough security information to the framework, in order to regain lost confidence level among small and medium organizations.

2. Related Work With Contribution

Security in cloud computing has always been a top concern for most organizations and that's the reason why most researches are on security in cloud computing. For this paper we reviewed several researches but here we will be mentioning some most recent and relevant ones. In [7] trusted third party model is proposed to secure the confidentiality and integrity of data, [8] only focuses on Identity and access management (IAM) security issues, [9] explains about securing documents in third party environment and security in Hadoop environment etc. Similarly, [10, 11, 12, 13, 14] have also shed some light on security concerns and with few solutions too, in different areas of cloud in terms of services and models, but none of these researches have given a solution of identified security concerns in regards to ease up cloud adoption by incorporating it in a framework.

The security threats and vulnerabilities mentioned in this paper is one of the part of the stage 1 of the cloud framework which focuses on the readiness of the organization by making them aware of all the risks and preparedness associated with cloud computing as shown in figure 1. The contribution of this paper and eventually a cloud framework is in cloud computing adoption among small organizations and enhancing cloud security [15].

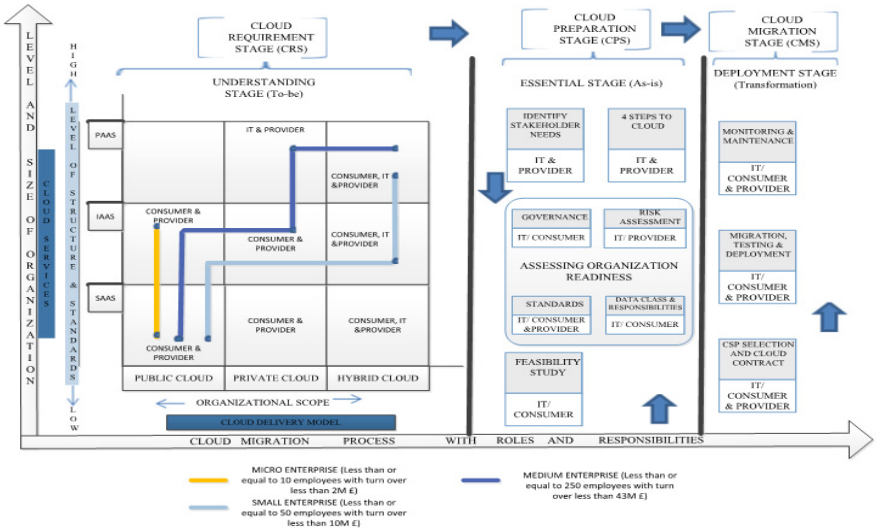

Fig. 1. Framework for cloud computing adoption.

3. Methodology and Data Analysis

The research methodology consisting appropriate techniques and steps was vital for this research program. The main stages of the methodology are outlined underneath:

- Reviewing previous literature and relevant cloud computing issues: In this step, previous relevant literature, surveys and studies have been reviewed to identify issues with cloud adoption.
- Identify and define the research problem: To do so, a qualitative research method has been adopted as a primary approach and following this; a number of semi-structured interviews were conducted with SMEs, cloud providers and developers to gather relevant information.
- Analysing data collected from interviews: The collected data from the interview is then analysed by applying the content analysis approach.
- Preparing a road map for SMEs: A structured guideline will then be designed in order to mitigate the cloud adoption barriers among SMEs.
- The fifth step of the research methodology concentrates on verification and validation of the proposed framework and gathers a feedback from SMEs and Cloud Service Providers (CSPs). For this, reflexivity workshops will be held.
- The feedback from the workshop will then be used to modify the framework to rectify and increase the efficiency of the framework.
- Finally, the proposed framework will then be prepared for use by SMEs in cloud adoption.

The information required for the current research on finding cloud barriers among SMEs, has been collected by using primary research techniques and secondary research techniques. Interviews were the main sources of finding the primary information; where the source of secondary information gathering is based on the literature review method. A similar approach was adopted by [16] in 2012 where she interviewed several IT experts to find out cloud computing risks and solutions for rationalizing and mitigating these risks. Also, similar research was conducted by [17] in 2014 where he explored the factors influencing the adoption of cloud computing and the challenges faced by the business and it is also supported by [18] as this approach provides an in depth knowledge about the research problem.

The content analysis is an approach applied in order to analyse the collected data. Firstly, the collected data was transcribed to avoid redundancy. It was then labelled according to the major attributes of cloud computing which makes the next step easy where data was divided into different themes. These themes were split into favourable attributes and non-favourable attributes of cloud computing in regards to SMEs. From the non-favourable attributes, several issues were identified which are hindering SMEs cloud adoption. These issues were

then segregated into technical and non-technical issues in order to get clear understanding behind these constraints. Then a guideline to SMEs is proposed based on the findings from interviews, government standards, previous surveys and literature review.

In order to find out security specific issues with cloud computing and its adoption, security related questions were necessary. These questions with keywords and related concepts that were used during interviews are: secure cloud systems, cloud security, SaaS security, PaaS security, IaaS security, Cloud threats, Cloud vulnerabilities, Future cloud threats, Cloud recommendations, best practices and solutions. After the collection of data gathered from interviews, it was analysed based on cloud computing service delivery models. These issues were segregated as per so called SPI model which includes SaaS, PaaS and IaaS.

4. Identified Current and Future Challenges

Although, cloud computing has been successful in attracting customers, it is still considered as an emerging technology among the SMEs due to some challenges. Issues related to security and privacy are the significant issues associated with the cloud computing. These issue constraints the successful adoption of the cloud computing technology. There are a number of barriers hindering cloud computing adoption among SMEs. To identify and understand these, a pilot study was conducted in the form of systematic literature review and interviews with the IT managers of eight leading cloud service providers and four cloud experts and developers which have brought some major current and future security and privacy issues into limelight. These threats are described along with vulnerabilities in service models to show relationship between two and how a threat can take an advantage of some vulnerability to compromise the system. The results shown below are based on comments from cloud security experts and developers. Moreover, an appropriate reference is also provided to support their claims as well.

Some of the current threats are as follows:

Threat 01 (Account or Service Hijacking): This can be performed through weak credentials and social engineering. Attacker can do malicious activities which may compromise data sensitivity, data manipulation and redirection of any transaction [19]. This threat mainly happens when CSP offer services that can be accessed through Application Programming Interfaces like SOAP, REST or HTTP with XML/JSON, and security of the cloud depend on these interfaces. Some of the problems it imposes are: weak credential, insufficient authorization checks and input data validation. It affects almost all services (or layers) of cloud computing i.e. SaaS, PaaS and IaaS [20, 21].

Threat 02 (Data Scavenging): Attackers may be able to recover removed data as it may still exist on the device unless destroyed [22]. It happens due to data related vulnerabilities such as Data colocation with the data of unknown owners (competitors or intruders) with a weak separation. Also, incomplete data removal as data cannot be completely removed. All services are susceptible to this threat.

Threat 03 (Data leakage): This occurs when data is handled wrongly or incompetently while transferring, processing, storing or auditing [19, 23]. It usually happens for following reasons in all three services: when data collocation is done with a weak separation, incomplete data deletion, data backup done by untrusted third party providers and data stored in clear plain text. It also specifically affects IaaS due to following vulnerabilities: Unrestricted allocation and deallocation of resources with Virtual Machines (VMs), uncontrolled migration due to fault tolerance, load balance etc., uncontrolled snapshots to provide flexibility and visible IPs for VMs [24].

Threat 04 (Denial of service): Unavailability of resources for legitimate users from the system due to take over of all available resources from malicious user. This threat takes place due to vulnerabilities within insecure interfaces and APIs, unlimited allocation of resources. The extent of this threat affects all three services. [19, 20]

Threat 05 (Customer Data manipulation): In this threat data sent from application component is manipulated to attack on web applications, heading to the server's application. For example, SQL injection, command injection, crosses site scripting and insecure direct object reference. This happens due to vulnerabilities in SaaS interfaces and APIs [23, 25].

Threat 06 (VM escape): This threat affects infrastructure (IaaS) by exploiting hypervisor to take control of the underlying infrastructure [23, 22]. This is due to vulnerabilities in hypervisors as they have flexible configuration of VMs and complex hypervisor code to meet organization needs [26, 27].

Threat 07 (VM Hopping): This threat enables one VM to gain access on another VM [28]. This happen IaaS due to unrestricted allocation and deallocation of resources of VMs, complex hypervisor code and flexible VM configuration [29].

Threat 08 (Malicious VM creation): VM image can be created through valid VM account containing malicious code such as Trojan horse to corrupt provider repository [23]. This happens due to uncontrolled placement of VM images in public repositories and unpatched VM images in IaaS.

Threat 09 (Insecure VM migration): In this threat, an attacker can access data illegally during migration, transfer a VM to an untrusted host and disruption or DoS by creating and migrating several VM [20]. All this happens during live migration of virtual machines in IaaS as it exposes the content of VM to the network [30].

Threat 10 (Sniffing/Spoofing virtual networks): An attacker can use VM to track virtual networks and even use ARP spoofing (address resolution protocol) to redirect packets from or to other VMs which leads in linking of MAC address with network IP [31]. This happens due to vulnerability in virtual networks where virtual bridges in IaaS are shared by several virtual networks [31].

We identified 8 potential challenges to be faced in future of cloud computing which in lieu is going to affect its adoption as well. These challenges are as follows:

1. Eaves Dropping: It is an unauthorized monitoring or intercepting of video conferencing, instant messages, phone calls etc. It usually takes place when IP is hacked.
2. Hypervisor viruses: This happens if a system is affected by the virus in a hypervisor layer of cloud.
3. Legal interception point: It is a legal authority built for the purpose of analysing data consisting of signal, network management info or the content of the communication. If this data goes in wrong hand or gets leaked then consequences could be devastating.
4. Virtual machine security: Virtualization has become a vital part of cloud computing and brings complex and risky security environment. If a virtual machine is compromised then it may lead to several other threats to the entire system.
5. Trusted transaction: Through this all transactions like e-business, data etc. are done on a trust basis between two ends. But, security of this trusted platform is still a big challenge.
6. Smartphone data slinging: Use of smartphones for accessing confidential and secured data gives rise to risks of getting system compromised.
7. Insecure APIs: Cloud customers manage and interact with services using set of APIs. If these APIs are compromised then enterprise can be exposed to confidentiality availability and password integrity sort of devastating issues.
8. Shared technology vulnerabilities: To achieve high end scalability to customers CSPs deliver services by sharing infrastructure, platforms and applications. The risk is when guest operating system gains access to other unnecessary shared levels which influence the entire system.

5. Results and Further Work

In the process we extracted more than 70 cloud security papers and research journals published within last 5 years in the relevant area. From this literature we identified few current challenges with cloud computing security that are mostly associated with virtualization layers of the cloud computing. The remaining current and future challenges were found during the interviews with CSPs and security experts. To counter these issues a security guide is to be formulated in order to strengthen cloud preparation stage (CPS) of the proposed cloud adoption framework.

6. Conclusion

The usage of cloud computing is slow among SMEs, as SMEs require services more in the area of offering infrastructure and software as a service. The study and analysis of these security issues have led to understanding of cloud computing security vulnerabilities that exist and it will assist enterprises to shift towards cloud. We covered traditional web applications, data hosting and virtualization as per their occurrence in service models: IaaS, PaaS and SaaS. As described in this paper, most security issues are due to vulnerabilities in virtualization, storage and network which are also major enablers of cloud computing technology. Explaining cloud security issues is not enough, that's why we presented vulnerabilities which may lead to threat, so that it can be easy to formulate contribution of these threats. We believe that it will encourage and accelerate the adoption of cloud computing among small and medium enterprises.

References

1. Georgios I, Smithson S , Lybereas T, *Trends in information technology in small businesses*, Idea Group Publishing, UK, ISBN 9781930708044, 2001.
2. Cloud Security Alliance, *Security guidance for critical areas of focus in Cloud Computing*, V3.0, 2011.
3. Khalid A, *Cloud Computing: applying issues in Small Business*, International Conference on Signal Acquisition and Processing (ICSAP'10), 2010, pp 278–281.
4. Li W, Ping L, *Trust model to enhance Security and interoperability of Cloud environment*, Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, 2009, pp 69–79.
5. Rittinghouse JW, Ransome JF, *Security in the Cloud*, Cloud Computing. Implementation, Management, and Security, CRC Press, 2009.
6. GiljeJaatun M, *Cloud Computing: First International Conference, CloudCom 2009*, Beijing, China, Proceedings, December 1-4, 2009. Springer.
7. Anne Thomas M, *Cloud Computing: the Gap between Hype and Reality*, presentation by VP and Research Director Burton Group ECAR Symposium December 5 Boca Raton FL, USA, 2008.
8. Gillam L, *Cloud Computing: Principles, Systems and Applications*, 2010,Springer.
9. Yaseen, Qussai, Althebyan Q, Panda B, Jararweh Y, *Mitigating insider threat in cloud relational databases*, Security and Communication Networks,2016.
10. Hendre A, Joshi KP, *A Semantic Approach to Cloud Security and Compliance*, 2015 IEEE 8th International Conference on Cloud Computing", New York City, June 27- July 2, 2015.
11. Al-Ayyoub, Mahmoud, Jararweh Y, Benkhelifa E, Vouk M, Rindos A, *SDSecurity: a software defined security experimental framework*, In Communication Workshop (ICCW), 2015 IEEE International Conference on, pp. 1871-1876. IEEE, 2015.
12. Damenu TK, Balakrishna C, *Cloud Security Risk Management: A Critical Review* , 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, 9-11 September.
13. Singh LV, Bole AV, Yadav SK, *Security Issues of Cloud Computing- A Survey*, International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 1, January 2015.
14. Varsha Wadhwa A, Gupta S, *Study of Security Issues in Cloud Computing*, International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 6, June 2015, pg.230 – 234.
15. Khan N, Yasiri AA, *Framework For Cloud Computing Adoption: A RoadMap for SMEs to Cloud Migration,*. International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2015, Vol. 5, No. 5/6, December.
16. Himmel MA, *Qualitative Analysis of Cloud Computing Risks and Framework for the Rationalization and Mitigation of Cloud Risks,* (January 1, 2012). *ETD Collection for Pace University.* PaperAAI3520142.
17. Nedev S, *Exploring the Factors Influencing the Adoption of Cloud Computing and the Challenges Faced by the Business*, 2014, Sheffield Hallam university.
18. Walliman.N, *Your Undergraduate Dissertation: The Essential Guide for Success*. 2nd Edition ed., London, 2012, SAGE PUBLICATION.
19. Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*., 2010.
20. Dawoud W, Takouna I, Meinel C, *Infrastructure as a service security: Challenges and solutions*. The 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany. IEEE Computer Society, Washington, DC, USA, 2010, pp 1–8.
21. Carlin S, Curran K, *Cloud Computing Security*, International Journal of Ambient Computing and Intelligence, 2011, 3(1):38–46.
22. Jansen WA,"*Cloud Hooks: Security and Privacy Issues in Cloud Computing*, Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI. IEEE Computer Society, Washington, DC, USA, 2011, pp 1–10.
23. Grobauer B, Walloschek T, Stocker E, *Understanding Cloud Computing vulnerabilities*, IEEE Security Privacy, 2011, 9(2):50–57.
24. Ertaul L, Singhal S, Gökay S, *Security challenges in Cloud Computing*, Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, 2010, pp 36–42.
25. OWASP, *The Ten most critical Web application Security risks*, 2010.
26. Morsy MAGrundy J, Müller I, *An analysis of the Cloud Computing Security problem*, Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia, 2010.
27. Yaseen, Qussai, Althebyan Q, Jararweh Y. *Pep-side caching: an insider threat port*, In Information Reuse and Integration (IRI), 2013 IEEE 14th International Conference on, pp. 137-144. IEEE, 2013.
28. Jasti A, Shah P, Nagaraj R, Pendse R, *Security in multi-tenancy cloud*, IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA,2010, pp 35–41.
29. Winkler V, *Securing the Cloud: Cloud computer Security techniques and tactics*, Elsevier Inc, Waltham, MA, 2011.
30. Rittinghouse JWRansome JF, *Security in the Cloud*, Cloud Computing. Implementation, Management, and Security, CRC Press 2007.
31. Wu H, Ding Y, Winer C, Yao L, *Network Security for virtual machine in Cloud Computing*, 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society Washington, DC, USA, 2010, pp 18–21.