7th International Conference on Research in Science and Technology
October 19 – 21, 2018
Munich - Germany

A review of the Security challenges in the cloud computing

Thabit Atobishi [1] , Szilard Podruzsik [2] , Szalay Zsigmond Gabor[3]

1 School of Management and Business Administration, Szent Istvan University, Gödöllő , Hungary

2 School of Business and Management, Corvinus University of Budapest, Budapest, Hungary

3 School of Management and Business Administration, Szent Istvan University, Gödöllő , Hungary

Keywords: cloud computing, security , information and communication service

JEL Codes: M15, O32, O33

Abstract

The cloud computing is a new way to benefit the cutting edge information technology at low cost. Cloud computing has grown rapidly in last years and became one of the most important growing IT segments. though its great possibility and rapid growth there are many concerns about the security of cloud computing which threat the cloud computing systems and may slow down the adoption of this technology .this paper is a review paper the shield the light on the most important security challenges in cloud computing technology and the proposed solutions to address it .

1.**Introduction**

cloud computing is the new generation of IT services paradigm , it can be seen as a replacement of using individual generators of electricity by centralized grid (Gupta, Seetharaman, & Raj, 2013) also (Subashini&Kavitha, 2011) defined the cloud computing as " a style of computing where massively scalable IT-enabled capabilities are delivered as a service to external customers using internet technologies " .according to Dillon, Wu, & Chang(2010) cloud computing has many distinguished features such as : agility , location independence , multi-tenancy , reliability and scalability it is expected That the worldwide public cloud services will grow 17.3 percent in 2019 to reach total $206.2 billion (Gartner, Inc, 2018) . even though the cloud computing came with many benefits and is considered as a promised technology , it is faced by some challenges which limit the wide adoption of cloud computing in the world (Wei, et al., 2014).security and privacy are the major challenges of the cloud computing adoption (Wei, et al., 2014).

2. **cloud computing :definition , characteristic and the model of the services**

As a new trend the concept of cloud computing has been defined from many perspectives , a broad definition by U.S. NIST (National Institute of Standards and Technology) "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell& Grance,2011). Also Ramgovind, Eloff, & Smith (2010) suggested that cloud computing can be seen as a collection of hardware and software systems used to provide online services to end users .Farzad (2011) said that "cloud computing is a network-based environment that focuses on sharing computation or resources "

According to Alzain, Pardede, Soh, & Thom (2012) there is three cloud computing models :

1-infrasture as a service (Iaas)

2-platform as a service (Paas)

3-software as a service (Saas)

In infrastructure as a service users can use the hardware equipment of the service provider and in platform as a service users can utilize the operating systems licensed software to develop their own applications also in software as a service the users can use the applications according to Evans (2017) the main providers of cloud computing services are Microsoft as the market leader and the seconed one is Amazon and the third one is IBM . so cloud computing is growing rapidly . a survey by logic monitor "Cloud Vision 2020:

The Future of the Cloud Study" showed that 83% of enterprises workload will be in the cloud by 2020 . also it showed that 66% of the respondents considered security issues to be the main in adoption of cloud computing . the survey showed that digital transforming is the main factor driving the enterprises to engage in cloud computing .

3. **security challenges in cloud computing**

As mentioned earlier the security is at the top of concerns of the IT managers when they decide to make the decision of cloud computing .

3.1 networks

the threats related to networks such as the connectivity , , availability and deny of services (Khalil, Khreishah, &Azeem .2014). according to Ali, Khan, &Vasilakos (2015) since the cloud computing works through the internet and use internet the mechanisms between the service provider and customers and within cloud system in virtual machine technology so there are the same communication challenges of any IT communications like denial of service and IP- spoofing based flooding . from other hand there are internal communication challenges which is related to cloud computing technology like virtual network and security misconfigration . Minhaj (2016) said there are three types of the cloud computing threats related the networks :

3.1.1 port scanning : it can lead to denial of services through accessing the network hosting the target machine

3.1.2 botnets : the data in the cloud systems can be steeled through a command and control system which is established with a bot-master and many machines which can be as a stepping-stone to steal private data

3.1.3 spoofing attacks :this kind of attacks depend on manipulate the IP address in a network's packet and redirecting the network traffic to the attackers

3.2.data and storage: Ali, Khan, &Vasilakos (2015) mentioned data storage level as The third level of the security challenges , since the users in cloud computing systems have less control than in conventional computing so the risks become different and more likely to occur . The main security to cloud storage is privacy, data recovery and vulnerability and data backup authentication control to protect the privacy of the information and that stored in the cloud . threats and problems related to data itself like redundancy , loos and leakages and privacy

3.2.1 Data leakage : there is a raising concern about the customer's data which will move to cloud service provider since it will be stored away from the customer's servers and because multi-tenant environment in the cloud computing . Singh, Jeong, & Park (2016) classified

security concerns of cloud computing into : software security , infrastructure security , storage security and network security .

3.3 Denial of services : out of service situation is more likely occur in cloud computing since it is multi-tenant architecture network (Sabahi .2011) . it happens when the attackers overfill the network and the servers with the requests that exceeds their capacity . this attack occurs through many ways such as SYN flood in which the server wait the acknowledgment from the attackers until the server eventually does not have the enough resources to serve the users , also it happens on the level of the networks TCP, UDP,

ICMP and DNS protocol packets and focus on disturbing the users connectivity over the networks by exhausting the victims networks (Yan, Yu, Gong, & Li, 2016) .

3.4 Vulnerability in virtualization :

ensuring that different users who are on the same physical resource are well separated and not interfering each other is a challenge of the virtualization of the cloud systems but current virtual machine management or the hypervisor doesn't ensure completely and perfect separation (Subashini & Kavitha. 2011) . Ali, Khan, &Vasilakos (2015) mentioned the architectural level of the security challenges in which the major challenges are virtualization which is the basic component of the cloud computing technology that enabled the multi tenancy and sharing in the cloud and the main challenges of the virtualization are VM image sharing(it can threat cloud system if it is used in malicious manner), VM isolation (because the users use the same physical resources which is virtually separated so cross VM attacks may occur) and VM escape (in this threat the attackers can escape from the control of the virtual machine management and consequently may access to other virtual machines), VM migration (moving a virtual machine to another physical computing resources without turning it off , so this situation can put the data of the virtual machine at risk) , VM rollback (basically it is a feature to increase the flexibility and the speed of cloud systems by allowing the retrieving of previous states of the VM when it is needed . but it can raise the security risks of the data violation and make some security problems that was patched in previous states).

Also Minhaj (2016) mentioned additional cloud computing virtualization related threats :

a Virtual machine based-attack : four types of virtual machine attacks

cross virtual machine side channel attack : in this case the attackers are able to get the information related to resource usage and other information from a target virtual machine

VM(virtual machine) creation attack : this attack happen through VM image

VM migration attack : this kind of attack occur when VM move from one physical resource to another

VM scheduler attack : by take address of scheduling of VM it can result in theft –of-service

Application-based challenges : these threats are related to the application which is running in the cloud . malware injection , shared architecture and web service are the main threats and attacks of applications in the cloud .

In software as a service model the main security efforts be outside of the service provider .from other hand in the platform as a service the greater security and control and control by the customers , in the case of infrastructure as a service the greatest security effort and management is done by the customers (Hashizume et al. , 2013).

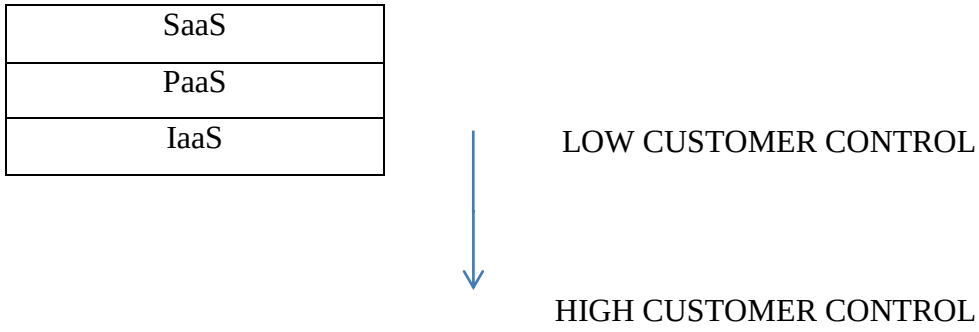

Figure 1.security level in the service models: Source (own construction)

Hashizume et al. (2013) classified the security issues in cloud computing according to the service model and then mentioned the security challenges associated with each model , in SaaS the main challenges such as applications security and multi-tenancy ,in PaaS the main challenges Third-party relationships and Development Life Cycle , in IaaS the challenges are associated with Virtualization .from other hand there are non-technical challenges that can threaten the security of the clod computing systems like : lack of deep investigation of the employees before hiring , not checking the customers background and lack of security awareness . Subashini & Kavitha(2011) described the security issues in cloud computing from the perspective of service delivery models as following :

Security issues in software as a service : data security , network security , data locality (in many countries like EU they do not allow the local data to be stored outside the country because of privacy issue), data integrity (to ensure data integrity the atomicity , consistency , isolation and durability characteristic should be considered , but in cloud computing environment we have multiple databases and multiple applications so it is needed to be handled correctly to preserve data integrity . also sometimes the applications in the cloud may have different levels of availability and service level agreement which

make the data integrity more complicated) , Data segregation (the main distinguished property of cloud service providing is multi tenancy which mean multiple users will store their data at the same data storage resources . so a security challenge can hack other's users data become more likely to occur) , data access (when the enterprises moved their data to cloud environment the accessibility to the data will subject to the enterprise's security policy which should be coordinated with the cloud service provider to prevent any unauthorized access to the enterprise's data)

Web application security : since the web applications and software as as service are very similar so most of web challenges are possessed by SaaS model , the most security risks of web applications that inherited by SaaS model are broken authentication , cross-site scripting , security misconfiguration and Insufficient transport layer protection .

3.6 non technical challenges (contractual and legal issues)

as the cloud services means moving the data and the administrative application to the cloud service provider so many legal issues come to the front .a service level agreement is a contract between the customer and the cloud service provider to manage the issues of performance assurance , the compliance regulations and monitoring . alsobecause the users and service providers located sometimes in different locations which may have different laws and regulations so legal issues arise in cloud computing environment , also E-discovery can violate the user's privacy of other countries (Ali, Khan, &Vasilakos.2015). E-discovery is " the process by which one party (for example, the plaintiff) is entitled to "discover" evidence in the form

of "electronically stored information" that is held by another party (for example, the defendant), and that is relevant to some matter that is the subject of civil litigation (that is, what is commonly called a "lawsuit") " (Oard & Webber, 2013) .

4. The solutions

There are many organizations and associations working on the security challenges in cloud computing such as cloud security alliance and cloud security website and the open grid forum(Subashini&Kavitha .2011), one possible solution for security concerns is to isolate the resources to secure the data processing by separating the cashes of the processors in virtual machines and isolate the virtual cashes from the hypervisor cashes (Subashini&Kavitha .2011) . The SaaS providers can support the identify management and sign on by these methods : independent identify management stack , credential synchronization and federate Idm . Ali, Khan, &Vasilakos(2015) proposed advanced cloud security protection for more secure cloud resources. it can guard the network against the attacks and it can also prevent cross tenant threats through monitoring of the running VM on the host platform . Another solution is the cyber-guarded to improve the security of the

networks by adopting virtual networks devices .trusted third party service within the cloud environment to increase the trust of the cloud service and to protect and keep the confidentiality and integrity and authenticity of the cloud's data and networks (Zissis&Lekkas, 2012).

5. Conclusions and future work

. as a new technology , the cloud computing came with great benefits , however some security challenges associated with cloud computing systems may slow down its use and adoption. In this study we reviewed the recent studies about the security cloud computing technology from different perspectives and identify the most important security challenges that threat the cloud computing systems. Networks, data and storage , Denial of services , Vulnerability in virtualization , Application-based challenges and non-technical (legal and contractual) challenges are appeared as the main challenges in cloud computing environment . the virtualization is the base of the cloud computing technology so it brought up new challenges that were not exist in traditional IT models , so it needs more focus in the future to develop new security solutions . the isolation of the resources is a proposed solution to secure the virtualization , also trusted third party service can be an effective way to solve the problem of of the trust and confidentiality and integrity of the data and the networks in the cloud .

Future studies should focus on each security challenge alone, and the new challenges that raised in the cloud computing and not inherited from the conventional technologies need more investigations especially the virtualizations challenges. Also an empirical research about the trusted third party solution is recommended to be investigated

References

1. Gupta, P., Seetharaman, A., & Raj, J. R. (2013).The usage and adoption of cloud computing by small and medium businesses.*International Journal of Information Management*, 33(5), 861-874. doi:10.1016/j.ijinfomgt.2013.07.00

2. Dillon, T., Wu, C., & Chang, E. (2010).Cloud Computing: Issues and Challenges.*2010 24th IEEE International Conference on Advanced Information Networking and Applications*. doi:10.1109/aina.2010.187

3. Mell, P. and Grance, T. (2011), "The NIST definition of cloud computing", available at: http://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019. (n.d.). Retrieved from https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019

4. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., &Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences*, 258, 371-386. doi:10.1016/j.ins.2013.04.028

5. Alzain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). Cloud Computing Security: From Single to Multi-clouds. *2012 45th Hawaii International Conference on System Sciences*. doi:10.1109/hicss.2012.153

6. Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The management of security in Cloud computing. *2010 Information Security for South Africa*. doi:10.1109/issa.2010.5588290

7. Evans, B. (2017, November 07). The Top 5 Cloud-Computing Vendors: #1 Microsoft, #2 Amazon, #3 IBM, #4 Salesforce, #5 SAP. Retrieved from https://www.forbes.com/sites/bobevans1/2017/11/07/the-top-5-cloud-computing-vendors-1-microsoft-2-amazon-3-ibm-4-salesforce-5-sap/#60a5599e6f2e

8. Cloud Vision 2020: The Future of the Cloud Study. (n.d.). Retrieved from https://www.logicmonitor.com/resource/the-future-of-the-cloud-a-cloud-influencers-survey/

9. Khalil, I., Khreishah, A., &Azeem, M. (2014). Cloud Computing Security: A Survey. Computers,3(1), 1-35. doi:10.3390/computers3010001

10. Singh, S., Jeong, Y., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75, 200-222. doi:10.1016/j.jnca.2016.09.002

11. Sabahi, F. (2011). Cloud computing security threats and responses. *2011 IEEE 3rd International Conference on Communication Software and Networks*. doi:10.1109/iccsn.2011.6014715

12. Oard, D. W., & Webber, W. (2013). *Information retrieval for e-discovery*. Boston: Now.

13. Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges. *IEEE Communications Surveys & Tutorials*, 18(1), 602-622. doi:10.1109/comst.2015.2487361

14. A Survey : Cloud Computing Challenges & Security Issues. (2017). *International Journal of Modern Trends in Engineering & Research*, 4(3), 57-61. doi:10.21884/ijmter.2017.4079.cfbgf
15. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(1), 5.doi:10.1186/1869-0238-4-5

16. Ali, M., Khan, S. U., &Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and 178. challenges. *Information Sciences*, 305, 357-383. doi:10.1016/j.ins.2015.01.025

17. 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. doi:10.1016/j.jnca.2010.07.006

18. Zissis, D., &Lekkas, D. (2012).Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592. doi:10.1016/j.future.2010.12.006