Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ISSN: 0976-3376

Asian Journal of Science and Technology
Vol. 07, Issue, 11, pp.3903-3907, November, 2016

RESEARCH ARTICLE

A REVIEW OF CLOUD SECURITY: ISSUES AND PROTECTION MECHANISMS

*Vishal Ramesh, Arvind Pillai and Priya, G.

School of Computer Science and Engineering, VIT University, Vellore, India

ARTICLE INFO

Article History:
Received 22nd August, 2016
Received in revised form
19th September, 2016
Accepted 17th October, 2016
Published online 30th November, 2016

Key words:

Revolutionized,
Security mechanisms,
Confidential.

ABSTRACT

Cloud computing has revolutionized the method of delivery of software services, architectural infrastructure of various organizations and business models used by several leading firms. Incorporating several attributes of grid computing, utility computing and autonomic computing makes cloud computing a flexible computing model which provides features compatible with firms in multiple domains. This drastic change by firms to adopt cloud computing models because of the immense advantages offered has given rise to scepticism about the security and confidentiality of the information stored. Moreover, usage of resources obtained from third party cloud services has worsened the layer of protection set in place by traditional computing models. Therefore, this paper presents a review on two main aspects; firstly, an analysis of various security issues which are present in a cloud environment and secondly, various security mechanisms which will enhance the security of confidential data in a cloud environment.

INTRODUCTION

Cloud computing is considered to be one of the most important entities that evolved out of grid computing (C. Weinhardt *et al*, 2009). Cloud computing has provided a lucrative computing solution to a plethora of firms across various domains. This solution can be obtained when some or a major portion of the control of client's information is transferred to the client service provider (CSP). (Hossain and Ahmed, Vol.6, No.1, January 2014) give us information about three sensitive states or situations that are vulnerable to threats, the states are listed as follows:

- The transmission of personal sensitive data to the cloud server,
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

Eventhough there are numerous amalagams of entities used in the cloud computing realm, the pith of cloud computing remains the same – the infrastructure or the resources are generally owned by a third party host and the client has to only pay for what they use (Bisong *et al*, 2011) (Rashmi, 2013).

Since the resources have to transferred to a cloud service provider, several firms are worried about the lack of transparency. In a recent survey conducted by (Fugitsu Research Institute, 2010) on potential cloud customers, 88% of the customers are worried about lack of transparency and are concerned about people who have access to their data. Such statistics urge the cloud computing community to devise a plan to overcome issues of trust and security. Furthermore,a recent IDCI survey reported that 74% of IT executives and CIO's cited security as an important factor that precludes them from acquiring cloud service models (Clavister, 2009). Major cloud service providers such as Amazon EC2/S3 (M. Armbrust *et al*, vol. 53, no. 4, 2010) (Garfinkel, 2007), Microsoft Azure (Chappell, 2009) are not providing full transparency and capabilities to track file access history and data provenance of both the physical and virtual servers utilized (P. Buneman, 2000). Though cloud computing solves the problem of utilization to a certain extent using techniques implemented by virtualization, it is vulnerable to a large amount of security risks (Seccombe A, 2009). Fig. 1 depicts the complexity of security risks involved in a cloud environment. In Fig. 1, the top layer represents the six characteristics of a cloud network namely, ubiquitous network, rapid elasticity, measured service, on-demand self service, multi-tenancy and resource pooling. These characteristics can be realized with the help of the service delivery models represented in the middle layer, they are, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (Iaas). The bottom layer represents various deployment models of a cloud namely,

****Corresponding author: Vishal Ramesh***
School of Computer Science and Engineering, VIT University, Vellore, India

private cloud, community cloud, public cloud and hybrid cloud. These basic elements of a cloud require specific levels of security which vary depending upon the combination deployment models, service delivery models and the characteristic of cloud that needs to be implemented. However, providing assurance to secure all the corporate data is almost impossible to achieve because of different service delivery models like SaaS, PaaS and IaaS (Kandukuri BR *et al*, 2009). From Fig.1,we can observe the layers of security needed to protect the client's resources. The types of security are classified into security related to third party resources, application security, data transmission security and data storage security. This paper primarily focuses on security issues, vulnerabilities which encourage attacks from several third party malicious users and the measures which can be taken to protect the client's resources from being compromised. Security issues which are abstract and cannot be quantified such as trust are also discussed briefly in this paper.

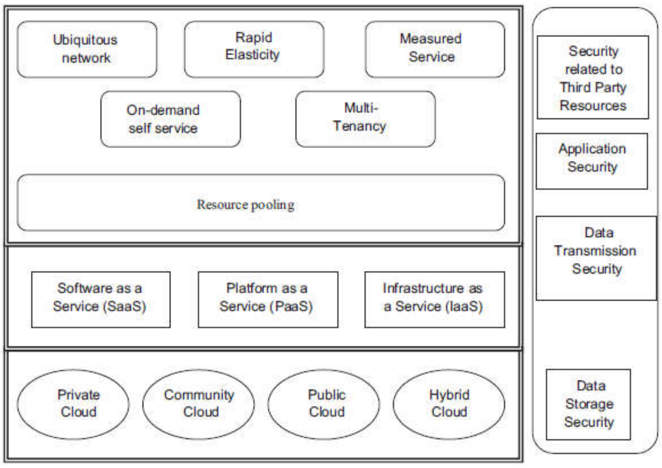

Fig. 1. Complexity of security in cloud environment (S. Subashini, 2011)

Security Issues in cloud computing

Cloud computing is a rather new but broad field and it covers a lot area. For such a field, there are obviously going to be a lot of problems. For a still not fully mastered technology, it is hard to come up with solutions for each and every problem that arises. The problems that arise can be broadly classified into the following categories (Nelson Gonzalez, 2012) (Rabi Prasad Padhy, 2011) (Keiko Hashizume, 2013) (Hossain, Vol.6, No.1, January 2014) (Pradeep Kumar Tiware, 2012) (Manpreet Kaur, 2015). They are as follows:

- Network security: They are the issues that arise in network communications.
- Interfaces: It concentrates on the issues that arise with regard to user and administrator interface.
- Data security: It deals with the securing of data with regard to confidentiality, availability and integrity.
- Virtualization: It focuses on effective separation of a Virtual Machine and any resulting problems in that process.
- Governance: It deals with the issues related to losing admin privileges and resulting security breaches.
- Legal issues: It deals with everything that has to do with any legal requirements like the location of data in various places.

Any issue that one may come across in a cloud computing architecture can be classified into one or more of the above mentioned categories. Apart from the technical aspects of security, there is one more aspect, which is trust. It is a predominant issue in cloud computing that is an abstract concept and hence cannot be classified or quantified. It can be between any combination of human and machine.

Let us look at some of the above mentioned reasons

Network Security

Networks are of different types. E.g.public, private, shared, non-shared, small area, large area networks and each and every one of them have their own security issues that have to be dealt with. The problems associated with network security include Sniffer attacks, DNS attacks, issue of reused IP address, Distributed Denial of Service (DDoS), eavesdropping, man in the middle attack and many more (Rabi Prasad Padhy, 2011) (Manpreet Kaur, 2015) (Farhan Bashir Shaikh, December 2011). A Domain Name Server (DNS) translates the domain name to an IP address. There are cases where the user has called the server by its name but has been transferred unknowingly to another cloud instead of the one he requested for. This is why using IP address is not always feasible. The Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but even then there are cases when these security measures are ineffective (Rabi Prasad Padhy, 2011) (Manpreet Kaur, 2015) (Dimitrios Zissis, 2012) (Zhong Hua, 2016).

Sniffer attacks are initiated by applications that can acquire packets of data that flow in a given network. If the data transfer is not protected by some sort of an encryption, there is a possibility that key information that flows through the network can be intercepted and the data that it contains be misused by a person with malicious intent. A sniffing detection platform that is centred on resolving addresses based on the Round Trip Time can be used to prevent sniffer attacks(Rabi Prasad Padhy, 2011) (Manpreet Kaur, 2015) (Dimitrios Zissis, 2012) (Zhong Hua, 2016). Reused IP address issues are a big network security concern and they have been ever since the origin of cloud computing. When a user acquires a new IP address and shifts from an existing network, his prior IP address is given to a new user based on the time of installation of a new device. This assignment is arbitrary. Because of this, the new user can have access to the data of the old user for a limited time because the changing of IP addresses in the DNS cache takes a while to process. If the new user does not have proper security measures, a hacker can steal the data of the old user using the same IP address which is now outdated and not applicable to him/ her anymore.(Nelson Gonzalez, 2012) (Rabi Prasad Padhy, 2011) (Hossain, Vol.6, No.1, January 2014) (Manpreet Kaur, 2015).

Data Security

Data Security refers to issues such as confidentiality, integrity and availability. Confidentiality is defined as the privacy of data. Integrity is defined as the correctness of data. Availability refers to the availability of data at any given time and place (Rabi Prasad Padhy, 2011). Data privacy is a very important concern in cloud computing. A user values his data and it is absolutely vital that his data is not being shared to someone whom he does not want to share the data with. But this is hard to achieve because all cloud providers store data globally and the users are not even aware of the location of their data. Moreover, the rules about data storage is different in different geographic locations and this gives a potential lapse of regulation by the cloud provider. This can be resolved by constantly checking the data in the cloud by a third party who serves as a Privacy Checking Committee. This committee can also help in formulating the rules of data story for the cloud provider. This ensures that the data is stored as per the wishes of the user and that it also complies with all the legal requirements.(Nelson Gonzalez, 2012) (Rabi Prasad Padhy, 2011). Data corruption can occur in a lot of levels and for any type of data. This might be because of the confusion that arises while storing various data types or conversion of one data type to another. This will mean that some information is lost which may or may not be vital. In a separately functioning cloud with only one database, it is very easy to ensure data integrity by monitoring the database transactions. Transactions follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity.(Rabi Prasad Padhy, 2011) (Keiko Hashizume, 2013) (Hossain, Vol.6, No.1, January 2014).

Virtualization

Virtualization is a key component of cloud computing. The key feature of a Virtual Machine is that it saves its state every once in a while so that the state can be reverted back whenever required. It is also easy to pause a state at given point and also to restart a paused state whenever needed. This gives rise to the problem of making sure that the various states that are simultaneously running on both a virtual and physical machine are separate from each other. Owing to the multiple states that are present, duplicity of a previous state becomes very simple. The transfer of a prior state to another machine will not even be noted by the machine. Because of this dynamic nature, it is very hard to ensure security. The security breach or a change of state will not even be recognized by the user. Owing to the various changes in state in a transient manner, it is impossible to maintain a proper record of all of it because it is expensive and a separate database is required just for this. Thus, ensuring that there are no lapses in security is a very big ask for the cloud provider.(Farhan Bashir Shaikh, December 2011) (Dimitrios Zissis, 2012) (Zhong Hua, 2016).

Mechanisms for protection in cloud computing

As presented in the previous section, there are significant number of sources from which security threats may arise, to preclude this compromise of resources, numerous security mechanisms and algorithms have been developed. Moreover, each algorithm is unique in its own way of protecting against a particular type of attack. Some of the most effective and commonly used algorithms are discussed in this section. (Taiwade, 2015) proposes a mechanism which lays emphasis on client side security, the Client's credentials and MAC address are stored in a database. When the client tries to login, a random token is generated for that particular MAC address and the client is asked to enter this random code as a 2nd layer of security, if the code entered by the client matches with the code generated by the system for that particular MAC address, then access is granted. The process is illustrated in Fig. 2.

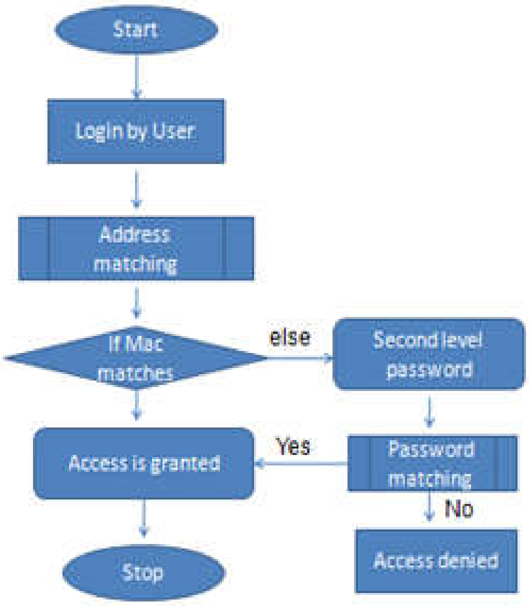

Fig. 2. The Data Flow Representation (Taiwade, 2015)

Authentication is a process by which confidentiality of data can be maintained, i.e. a malicious user who tries to access the data is denied access through certain mechanisms. RSA(Baize, 2014) uses a single login to provide strong authentication methods, it considers public and private cloud as separate entities. To provide strong security mechanisms to private cloud, it proposes a centralized virtualization management console which precludes access of malicious users. RSA provides three main schemes: two factor authentication, adaptive authentication and knowledge based authentication, using these schemes RSA has managed to reduce cost and improve efficiency of security. Amazon Web Services (AWS) (AWS, 2016) ensures protected transfer of private information between the web server and the browser used by the client by using its own virtual private cloud, it uses authentication mechanisms like Multifactor authentication (MFA) to improve identity management and access management, AWS MFA requires the user to provide an additional six-digit code in addition to the standard username and password. Shibboleth (Cantor, 2010) allows user to access different services with a single piece of information, it uses only one identity and password to authenticate access to multiple services provided by different organizations or corporations. Authorization is another security measure in which the user submits a piece of information like a password or a secure code to access a particular service. Oracle (Orcale, 2015) uses their Oracle Database Vault to protect application data from multiple administrative users and to enhance authorization. VMware (VMware, n.d.) integrates software policies and official directories with the policies of the service provider to ensure a powerful authorization mechanism. The end user given authority to access the data by using one of three methods: soft token, hard token and certificate, the administrator is only given access to the files required to complete the job, moreover, VMware provides resource management techniques to preclude starvation of virtual machines, consequently, preventing denial of service (DoS) attacks.

Encryption is technique by which a piece of information is encoded to form a cipher text which can only be read by authorized users who possess the required key. Dell provides encryption called Dell Data Protection | Encryption for all its users who store information on an external hard disk, this process is done autonomously i.e. no human intervention is required to enforce encryption and policies. Moreover, Dell uses Transparent File Encryption which gives access of information to specific users who are listed in a database, auditing and monitoring services are also provided. This autonomous encryption without disrupting the services currently in use was implemented by dell in Virginia Commonwealth University (Dell, n.d.). Hardware based encryption is built into storage area networks (SAN) by Online Tech (Pham, 2013), moreover, the entire server is encrypted to ensure maximum safety, they also provide back-up recovery and disaster recovery services. Access control is method by which access is provided to only those who have authorization. McAfee (McAfee, n.d.) provides a coordinated security model to prevent unauthorized access in private clouds, when a first tries to enter the cloud, it is inspected by the McAfee Virtual Network Security Platform, an inline virtual prevention system (IPS). Then, an improved malware policy examines the file, if the file is suspected to contain any insidious programs, then it is sent to the McAfee Advanced Threat Defence which scans the file and sends the information to the McAfee Threat Intelligence Exchange.

Conclusion

In conclusion, cloud computing is progressing at a drastic rate and will soon replace various traditional models, this precipitous change is accompanied by several security issues and also various security mechanisms to counter these issues. Based on data collected from various cloud providers, a look into the problems arising and the corresponding solutions was observed. It was observed that the number of security problems related to legal issues, compliance and governance is quite large. At the same time, the number of proposed solutions for those issues are also quite large. In other words, these concerns are highly relevant and frequent but a lot of research has gone into tackling these resources. The case is completely opposite when we look at the errors related to virtualization, isolation and data leakage. Virtualization amounts for around 12% of problem causes but only 3% for solutions. This means that such problems are fairly significant when it comes to cloud computing, but little is available in terms of solutions. This indicates the need for research in these areas that are still prominent in terms of problems but very sparse when it comes to actually arriving at a solution.

REFERENCES

AWS. 2016, June. Amazon Web Services White Paper. Retrieved from https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Baize, E. 2014. Cloud Security Mechanisms for Data Protection: A Survey. *International Journal of Multimedia and Ubiquitous Engineeri*, 81-90.

Bisong, A. a. 2011. An Overview of the Security Concerns in Enterprise Cloud Computing. *International Journal of Network Security and Its Applications*, 30-45.

Weinhardt, C. A. A. 2009. Cloud Computing - A classification, business models, and research directions. Business and Information Systems Engineering, 391-399.

Cantor, S. 2010. Understanding shibboleth. Retrieved from https://wiki.shibboleth.net/confluence/display/SHIB/UnderstandingShibb

Chappell, D. 2009. Introducing Microsoft Azure. Retrieved from http://www.microsoft.com/windowsazure/Whitepapers/IntroducingWindowsAzure/default.aspx

Clavister. (2009, October 21). Security in the cloud, Clavister White Paper. Retrieved from http://www.it-wire.nu/

Dell. (n.d.). Healthcare and educational. Retrieved from http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/Dell_VCU_CASESTUDY.pdf

Dimitrios Zissis, D. L. 2012. Addressing cloud computing security issues. Future Generation Computer Systems, 583-292.

Farhan Bashir Shaikh, S. H. (December 2011). Security Threats in Cloud Computing. 6th International Conference on Internet Technology and Secured Transactions.

Garfinkel, S. 2007. An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS. Center for Research on Computation and Society, Harvard University.

Hossain, M. A. (Vol.6, No.1, January 2014). Cloud Computing and Security Issues In the Cloud. *International Jounal of Network Security and Its Applications* (IJNSA).

Institute, F. R. 2010. Personal data in the cloud : A global survey of consumer attitudes.

Kandukuri BR, P. V. 2009. Cloud security issues. IEEE international conference on services computing, 517-20.

Keiko Hashizume, D. G.M. 2013. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*.

Armbrust, M. A. F. (vol. 53, no. 4, 2010). A view of cloud computing. Communications of the ACM, 50-58.

Manpreet Kaur, H. S. 2015. A Review of Cloud Computing Security Issues. *International Journal of Advances in Engineering and Technology*.

McAfee. (n.d.). Securing Private Cloud. Retrieved from http://www.mcafee.com/us/resources/solution-briefs/sb-securing-private-cloud.pdf

Nelson Gonzalez, C. M. 2012. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing : Advances, Systems and Applications*.

Orcale. (2015, February). Oracle Database 12c Security and Compliance White Paper. Retrieved from http://www.oracle.com/technetwork/database/security/security-compliance-wp-12c-1896112.pdf

Buneman, P. S. K. 2000. Data provenance: Some basic issues. FST TCS : Foundations of Software Technology and Theoretical Computer Science, 87-93.

Pham, T. (2013, September 10). Online Tech. Retrieved from http://resource.onlinetech.com/introducing-online-techs-encrypted-enterprise-class-clouds/

Pradeep Kumar Tiware, D. B. 2012. Cloud Computing Security Issues, Challenges and Solutions. *International*

Journal of Emerging Technology and Advanced Engineering Vol. 2, Issue 8.

Priya .G, J. N. (September 2016). A Reputation Based Trustworthy System For Cloud Environment. *International Journal of Pharmacy and Technology,* Vol 8, No. 3, 16702-16708.

Rabi Prasad Padhy, M. R. 2011. Cloud Computing: Security Issues and Research Challenges. *International Journal of Computer Science and Information Technology and Security* Vol. 1 , No. 2.

Rashmi, S. G. 2013. Securing Software as a Service Model of Cloud Computing : Issues and Solutions. *International Journal on Cloud Computing: Services and Architecture*, 1-11.

Subashini, S. V. K. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications,* 1-11.

Seccombe A, H. A. 2009. Security guidance for critical areas of focus in cloud computing. CloudSecurityAlliance.

Taiwade, H. V. 2015. Enhanced Security Mechanisms for Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering* Vol. 5, Issue 7.

VMware. (n.d.). Securing the Cloud : Cloud Computing, Security Implications and Best Practices. Retrieved from http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/cloud/vmware-savvis-cloud-white-paper-en.pdf

Zhong Hua, X. W. 2016. Cloud Computing and the Essential of Security Management. *Open Access Library Journal.*

****