International Journal of Latest Trends in Engineering and Technology
Vol.(7)Issue(4), pp.305-310
DOI: http://dx.doi.org/10.21172/1.74.042
e-ISSN:2278-621X

SECURITY ISSUES IN CLOUD COMPUTING

RakeshNag Dasari[1], Dr. Y. Prasanth[2], Dr. O. NagaRaju[3]

Abstract- Objectives: This paper introduces the concept of cloud computing and further explains the major security issues faced by cloud service providers Methods/Statistical Analysis: Security provider controls and approaches to provide cloud security.Findings: Approaches to handle security in cloud computingApplication/Improvements: Cloud Computing stack.

Keywords- Cloud Computing, Security

I. INTRODUCTION

Cloud computing is a form of distributed architecture that offers resources centrally to its customers. Customers can later use these resources to create web services for end-users. The concept that cloud service providers use is similar to internet service providers who provide broadband on per use basis. Centrally provided resources can be on-demand network access, storage access, server access, application access which can be managed without much vendor interference at the click of a button. These resources can be categorized into software as a service(SaaS), platform as a service(PaaS) and infrastructure as a service(IaaS)[1-3].

Various organizations make use of these services as they need to pay for the resources they are using on a per unit basis.

In case of startups who are severely constrained on funding cloud computing is an economical solution since they need not go ahead and procure resources and can make use of resources on consumption basis. Another advantage with cloud computing is that one can use software or platform or infrastructure for business needs without having to necessarily manage it. Earlier this idea was restricted to only academic arena and later spread to the corporate sector with companies like IBM, Microsoft and Oracle heavily investing in the concept of utility computing. Another advantage in the concept of cloud computing is that customer can rent resources based on their requirements which is financially very viable.

Cloud computing concept shall facilitate easy and faster access of applications over mobile devices by making the heavy applications lightweight in nature. Customers need not bother to secure the platform or software or infrastructure from malicious threats since the onus of managing the resource lies with the cloud service provider.

[1] *Department of computer science & Engineering, KL University, India*
[2] *Department of computer science & Engineering, KL University, India*
[3] *Department of Computer Science & Engineering, Govt. Degree College, India*

Evolution wise initially the first architecture that introduced the concept of virtualization was grid computing followed by distributed computing which was later perfected after the advent of cloud computing. Complicated online business applications can be hosted over the cloud and can be accessed from various computer browsers across the internet. The advantage here lies in the fact that the application is scalable and can provide superior throughput with huge computing power[4-7].

Security happens to be the key challenge facing the cloud computing environment. The reason being in the complex cloud setup there might be a group of people trying to access the cloud setup to access data and in the process malicious attack on data might get underway. Stringent strategies need to be incorporated so as to monitor for data breach if any[8-11].

One of the key advantages of cloud computing is that it turns out to be financially viable for small companies since they need not bother about managing and monitoring the complex infrastructure. They can pay for the quantum of infrastructure or platform or software used in the cloud stack per unit time. Cloud environment also facilitates in analytics[12-14].

Subsequent section explains about cloud computing infrastructure. Later security issues in cloud are explained. The final section deals with conclusion followed by references.

II. CLOUD COMPUTING INFRASTRUCTURE

Cloud computing is a technology that has evolved from distributed and grid computing. However this concept of distributed computing is shielded from end-users as the end-users are not aware of the architecture used to setup the cloud. The cloud can be categorized as public, private and hybrid cloud based on the ownership. If the cloud ownership is privately held by a corporate then it is termed as private cloud, if its available for public use then it is termed as public cloud and if the ownership is jointly held by public and private entities then it is termed as hybrid cloud[14-16].

Managing security in a private cloud is much easier than managing security in public or hybrid cloud. This is because in a private cloud setup malicious threats to the cloud setup will be less as compared to the other two architectures since in a private cloud setup access to the cloud infrastructure can be easily managed and monitored. In a cloud computing environment the central resources are rented out to customers by cloud service providers. Based on whether or not hardware or operating system or software is rented out cloud architecture can be termed as infrastructure as a service(IaaS), platform as a service(PaaS) and software as a service(SaaS)[17-18]. The diagram below depicts this architecture:

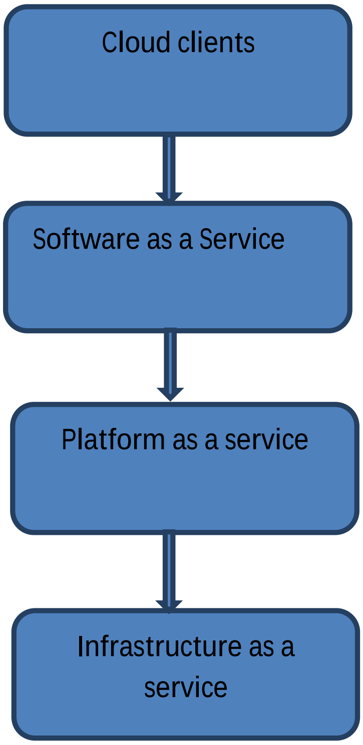

Fig 1: Cloud computing stack

Cloud computing is implemented using the concept of virtualization. The hardware, servers, storage is setup by the cloud service provider on which the service provider based on the requirement can install the operating system needed by the end-user. On this platform created the service provider can install few applications or software which can be used by the end-user. The end-user shall avail this cloud setup based on the requirements and on purely rental basis. This saves huge cost for the end-user since the infrastructure can be upgraded as and when the business grows and the same can be scaled down as well in case of loss in the business[18-20].

Another important aspect of cloud computing is security. It is very important to clearly describe role based access control properly since the onus of securing the infrastructure lies with the service provider. As the end user is not responsible to bother about the security aspect of cloud setup, the cloud service provider needs to be very careful any security breach can severely affect the service provider’s reputation in the market and also financially cripple the end-user. In the below diagram cloud architecture is clearly depicted[19].

Fig 1: This diagram depicts cloud computing stack architecture.

Fig 2: The diagram outlines differences between public, private and hybrid cloud

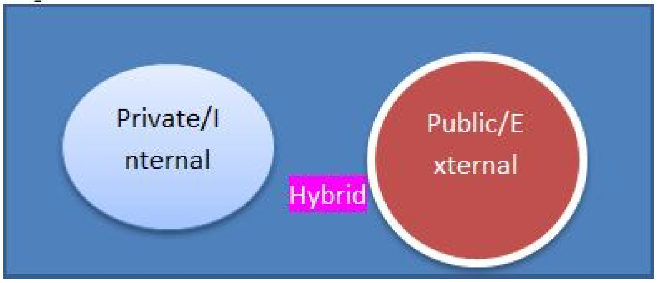

Fig 2: Public, private and hybrid architecture.

The above diagram clearly outlines the differences between public, private and hybrid cloud.

III. SECURITY ISSUES IN CLOUD

Cloud computing offers various possibilities and challenges to all its stakeholders. One of the major possibilities offered by the cloud environment is location transparency as the end-user and the customer need not be aware of the location where the cloud environment has been setup. This can also be considered as a challenge since location transparency can lead to security and reliability concerns to the customer as well as end-user. The security challenges offered by cloud computing are dynamic and vast in nature. Technical security provided by the cloud service provider is not always sufficient. Well-defined cloud strategic policies are needed to secure the cloud infrastructure which is a very significant aspect of cloud computing. Cloud computing is based on an element of trust wherein the end-user trusts the customer and the customer trusts the cloud service provider since managing and monitoring the cloud infrastructure is the responsibility of the service provider. Reliability and reputation of the service provider is also one of the key deciding factors when a customer or an end-user procures cloud infrastructure from service provider on a rental basis[21].

Various attacks possible in a cloud computing environment are mentioned below:

a) Phishing: It is a process of stealing critical information like userids and password from people posing as credible organizations on the internet.

b) Eavesdropping: It is an attempt to secretly listen to a conversation or a session with malicious intent.

c) Sniffing: It is an attempt to track the users accessing a particular infrastructure and get sensitive details from them with malicious intent.

d) Distributed denial of service: Here multiple systems infected by a malicious object target one particular system and block its smooth functioning hence impending its service. Thus the name distributed denial of service.

Accounting is another feature that needs to be properly carried out by the service provider. In accounting the service provider needs to maintain the information of people accessing the infrastructure using various sophisticated software’s such as intrusion detection systems. This helps to identify the attacker in case of security breach. One can also implement various authentication mechanisms such as biometric authentication so as to allow authorized users to access the cloud setup. Even if proper security strategies have been well defined and enough authentication and accounting policies are put in place there is always a possibility of insider attack since cloud infrastructure is maintained by cloud service providers and not by the team actually making use of the said infrastructure.

Although stringent mechanisms are put in place to avoid insider attack other serious vulnerabilities that exist in cloud computing are licensing issues of the software being used. Since the software used by the end-user is actually procured by the service provider there is always a possibility of licensing issues arising out of the installations. Software used by the service provider in setting out the cloud environment might have loopholes due to the use of insecure third party API's which might make the whole environment vulnerable to attacks. Another major issue in cloud computing is the availability of resources round the clock and this depends on proper managing the cloud infrastructure round the clock. Various controls have to be put in place by the service provider so as to make the cloud computing environment more secure[20]. Few of the controls are mentioned below:

a) Deterrent controls: The attackers in the case are given a warning that they will have to deal with serious consequences if they breach any data. It facilitates in avoiding any malicious attack by an unauthorized person.

b) Preventive controls: Strong authentication and authorization mechanisms while accessing the cloud stack aids in preventing any kind of malicious attack on data. It facilitates in reducing vulnerabilities if not totaling eliminating the same.

c) Detective controls: These controls detect any malicious attack on data and direct the relevant preventive controls to take corrective action against the perpetrators. The corrective action might range from blocking the malicious attacker or letting him off with a warning.

d) Corrective controls: These controls reduce the impact of a particular malicious attack on the system by taking corrective action in the case of an attack. The corrective action might vary from reverting the system to a previous stable state or take backup of the existing system periodically.

Various approaches via which security can be provided are:

a) Data Confidentiality: Confidentiality is the key approach to secure data. Various outsourced data is stored on the cloud. The primary expectation from customers is that the data confidentially is maintained such that no unauthorized user is able to access the data.

b) Data Access Controllability: Data authorization based on role based access control strategy is one of the key approaches in securing data. Various people designated to access various levels of data deployed on the cloud are given access to the data group which they are permitted to access via restricted authentication mechanisms.

c) Data Integrity: This approach deals with maintain the sanctity of data deployed on the cloud. The idea here is that even if the data gets corrupted then there must be mechanisms to restore earlier state of data such that the user who has trustworthily deployed data on the cloud does not lose any of his data items.

IV. CONCLUSIONS

Cloud computing offers a lot of advantages which are directly proportional to the threats offered by the said environment. The major aspect of proper implementation of the cloud computing concept is the strategy followed in securing the environment. Cloud computing gives virtual ownership of even a super computer to the end-user and due to security reasons this advantage cannot be ignored. The way forward is to thoroughly research and strengthen the security mechanisms and make the cloud infrastructure secure in every aspect.

REFERENCES

[1] Kenichi Humphrey M. Sabi, Faith-Michael E. Uzoka, Kehbuma Langmia, Felix N. Njeh, Conceptualizing a model for adoption of cloud computing in education, International Journal of Information Management, Volume 36, Issue 2, April 2016, Pages 183-191, ISSN 0268-4012, http://dx.doi.org/10.1016/j.ijinfomgt.2015.11.010.

[2] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, DDoS attacks in Cloud Computing: Collateral Damage to Non-targets, Computer Networks, Available online 8 April 2016, ISSN 1389-1286, http://dx.doi.org/10.1016/j.comnet.2016.03.022.

[3] Mahmoud M. El-Gayyar, Amira S. Ibrahim, M.E. Wahed, Translation from Arabic speech to Arabic Sign Language based on cloud computing, Egyptian Informatics Journal, Available online 18 May 2016, ISSN 1110-8665, http://dx.doi.org/10.1016/j.eij.2016.04.001.

[4] Vanessa Ratten, Continuance use intention of cloud computing: Innovativeness and creativity perspectives, Journal of Business Research, Volume 69, Issue 5, May 2016, Pages 1737-1740, ISSN 0148-2963, http://dx.doi.org/10.1016/j.jbusres.2015.10.047.

[5] Manuel Díaz, Cristian Martín, Bartolomé Rubio, State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing, Journal of Network and Computer Applications, Volume 67, May 2016, Pages 99-117, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2016.01.010.

[6] Weiwei Kong, Yang Lei, Jing Ma, Virtual machine resource scheduling algorithm for cloud computing based on auction mechanism, Optik - International Journal for Light and Electron Optics, Volume 127, Issue 12, June 2016, Pages 5099-5104, ISSN 0030-4026, http://dx.doi.org/10.1016/j.ijleo.2016.02.061.

[6] Merve Bayramusta, V. Aslihan Nasir, A fad or future of IT?: A comprehensive literature review on the cloud computing research, International Journal of Information Management, Volume 36, Issue 4, August 2016, Pages 635-644, ISSN 0268-4012, http://dx.doi.org/10.1016/j.ijinfomgt.2016.04.006.

[7] Nianxin Wang, Huigang Liang, Yu Jia, Shilun Ge, Yajiong Xue, Zhining Wang, Cloud computing research in the IS discipline: A citation/co-citation analysis, Decision Support Systems, Volume 86, June 2016, Pages 35-47, ISSN 0167-9236, http://dx.doi.org/10.1016/j.dss.2016.03.006.

[8] Mohammad Masdari, Sima ValiKardan, Zahra Shahi, Sonay Imani Azar, Towards workflow scheduling in cloud computing: A comprehensive analysis, Journal of Network and Computer Applications, Volume 66, May 2016, Pages 64-82, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2016.01.018.

[9] Jen-Ho Yang, Pei-Yu Lin, A mobile payment mechanism with anonymity for cloud computing, Journal of Systems and Software, Volume 116, June 2016, Pages 69-74, ISSN 0164-1212, http://dx.doi.org/10.1016/j.jss.2015.07.023.

[10] Kaiyang Liu, Jun Peng, Heng Li, Xiaoyong Zhang, Weirong Liu, Multi-device task offloading with time-constraints for energy efficiency in mobile cloud computing, Future Generation Computer Systems, Volume 64, November 2016, Pages 1-14, ISSN 0167-739X, http://dx.doi.org/10.1016/j.future.2016.04.013.

[11] Shiliang Luo, Bin Ren, The monitoring and managing application of cloud computing based on Internet of Things, Computer Methods and Programs in Biomedicine, Volume 130, July 2016, Pages 154-161, ISSN 0169-2607, http://dx.doi.org/10.1016/j.cmpb.2016.03.024.

[12] Yinghui Zhang, Xiaofeng Chen, Jin Li, Duncan S. Wong, Hui Li, Ilsun You, Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing, Information Sciences, Available online 26 April 2016, ISSN 0020-0255, http://dx.doi.org/10.1016/j.ins.2016.04.015.

[13[Dara G. Schniederjans, Douglas N. Hales, Cloud computing and its impact on economic and environmental performance: A transaction cost economics perspective, Decision Support Systems, Volume 86, June 2016, Pages 73-82, ISSN 0167-9236, http://dx.doi.org/10.1016/j.dss.2016.03.009.

[14] Min Xia, Teng Li, Yunfei Zhang, Clarence W. de Silva, Closed-loop design evolution of engineering system using condition monitoring through internet of things and cloud computing, Computer Networks, Volume 101, 4 June 2016, Pages 5-18, ISSN 1389-1286, http://dx.doi.org/10.1016/j.comnet.2015.12.016.

[15] Xiaobo Ji, Fan Zeng, Mingwei Lin, Data transmission strategies for resource monitoring in cloud computing platforms, Optik - International Journal for Light and Electron Optics, Volume 127, Issue 16, August 2016, Pages 6726-6734, ISSN 0030-4026, http://dx.doi.org/10.1016/j.ijleo.2016.04.114.

[16] Minhaj Ahmad Khan, A survey of security issues for cloud computing, Journal of Network and Computer Applications, Volume 71, August 2016, Pages 11-29, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2016.05.010.

[17] Parnia Samimi, Youness Teimouri, Muriati Mukhtar, A combinatorial double auction resource allocation model in cloud computing, Information Sciences, Volume 357, 20 August 2016, Pages 201-216, ISSN 0020-0255, http://dx.doi.org/10.1016/j.ins.2014.02.008.

[18] Xu Yang, Xinyi Huang, Joseph K. Liu, Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing, Future Generation Computer Systems, Volume 62, September 2016, Pages 190-195, ISSN 0167-739X, http://dx.doi.org/10.1016/j.future.2015.09.028.

[19] Satish Kumar, Anita Ganpati, An Approach for Data Security from Malicious Attacker in Cloud Computing, Indian Journal of Science and Technology, Volume 9, Issue 32, August 2016, ISSN: 0974-6846

[20] B. S. Kiruthika Devi, T. Subbulakshmi, A Comparative Analysis of Security Methods for DDoS Attacks in the Cloud Computing Environment, Indian Journal of Science and Technology, Volume 9, Issue 34, September 2016, ISSN: 0974-6846

[21] Deevi Radha Rani, Sk. Nazma Sultana, Pasala Lourdu Sravani, Challenges of Digital Forensics in Cloud Computing Environment, Indian Journal of ScienceandTechnology, Volume 9, Issue 17, May 2016, ISSN: 0974-6846