ISSN No. 0976-5697

Volume 8, No. 2, March 2017 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review

Iqra Altaf Mattoo
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
iqraaltaf61@gmail.com

Abstract: Cloud computing is a set of Information Technology services offered to the users over the web on a rented base. Cloud computing has many advantages such as flexibility, efficiency, scalability, integration, and capital reduction. Security is one of the main challenges that hinder the growth of cloud computing. This study introduces a brief analysis of the issues and challenges of cloud computing security. "Cloud computing services will be varied and must be defined from the perspective of the users of the service. These services can range from one-off automated IT tasks to services that are made up of application and infrastructure components and tethered to business processes. The most impactful deployments encompass IT task and service automation and also venture into business service automation".

Keywords: Cloud computing; Security issues; DOS; Data loss; Challenges.

I. INTRODUCTION

Cloud Computing came with the merging of many technologies. Obviously, hardware is required. Relatively low-priced servers and storage makes data centers possible. Increased accessibility and availability of high-speed Internet connections means these data centers can be located where it is most economical. Naturally, a data center alone does not constitute Cloud Computing. Cloud Computing is recognized through the Cloud Computing Stack. The Cloud Computing Stack arranges the hardware/software of a data center into various service layers.

Cloud computing is a model for enabling pervasive, convenient, on-demand network access to a shared group of configurable computing resources (e.g., networks, storage, servers, applications, and services) that can be quickly provided and released with less management effort. This cloud model consists of five important characteristics, three service models, and four deployment models. The main idea of cloud computing is to provide both software and hardware as services. There are three layers of services over the cloud. These are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [2]. Individuals and organizations have been considering services over the cloud to cut the costs of expenditure, without any compensation in utilizing recent technologies [3].

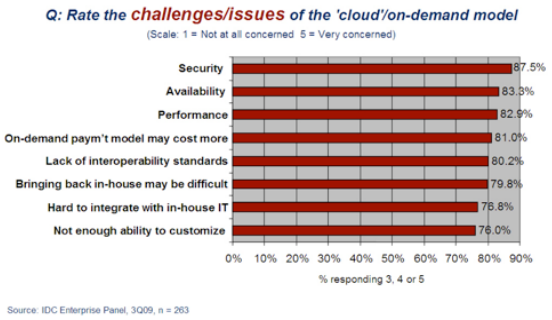

Figure 1: IDC Survey Report

The International Data Corporation (IDC) conducted a study [1] (see Figure 1) of 263 IT executives and their line-of business colleagues to estimate their views and know their companies use of IT cloud services. Security placed first as the greatest challenge of cloud computing. Followed in this paper, Section II discusses security issues in cloud. In section III, challenges of cloud computing security are being discussed and later sections include conclusion and references.

II. SECURITY ISSUES IN CLOUD COMPUTING

The CSA has warned that the shared nature of cloud computing introduces the possibility of new security breaches that can wipe out any gains made by switching to cloud technology. Cloud computing environment provides users with capabilities to process and store and their data in third- party data centers [4]. Establishments use the cloud in a variety of different service models and deployment models (private, public, hybrid, and community) [5]. Security concerns related to cloud computing environment fall into two categories: security issues faced by cloud providers and security issues faced by their customers [6]. The liability is shared, however the provider must guarantee that their infrastructure is safe and that their clients' data and applications are secure, while the user must take measures to strengthen their application and use strong passwords and authentication measures. Enterprises are no longer sitting on their hands, doubting if they should risk transferring their sensitive data and applications to the cloud. They're doing it but still the security remains a serious concern.Some security issues are discussed below:

Data Breaches:Cloud computing and services are to some extent new but data breaches have been there for years. A study made by the Ponemon Institute entitled "Man In Cloud Attack" reports that over 50 percent of the IT and security experts surveyed and believed that their organization's security measures to protect data on cloud services are low. The inclusive data breaching was three times more possible to occur

for businesses that use the cloud rather than those who don't use the services of cloud.

Hijacking of Accounts:Attackers now have the skill to use your login information to distantly access critical data stored on the cloud. Some other methods of hijacking include scripting bugs and reused passwords, which permit attackers to easily steal credentials without detection. In April 2010 Amazon faced a cross-site scripting bug that targeted even the credentials of customers.

Insider threat:An attack from inside your organization may seem questionable and doubtful, but the insider threat remains there. Employees can use their authorized access to an organization's cloud-based services to exploit and misuse information such as financial forms, customer accounts, and other critical information.

Malware injection: Malware injections are scripts or code that is embedded into cloud services and behave as "valid instances" and run as Software as a service (SaaS) to cloud servers. This means that malicious code could be injected into cloud services and observed as part of the software that is running within the servers of the cloud environment. Once an injection is executed and the cloud begins working with it, attackers can snoop and compromise the integrity of critical information and data.

Abuse of cloud services:The cloud's incomparable storage capacity has permitted both hackers as well as legal users to host and spread malware, illicit software, and other digital assets. These risks consist of sharing of pirated software, music, videos, or books. You can decrease your exposure to risk by continuously monitoring usage and setting strategies for what your employees host in the cloud.

Denial of service attacks:Unlike other types of cyber-attacks, which are usually launched to create a long-term foothold and hijack sensitive information, denial of service attacks do not challenge to breach your security perimeter.

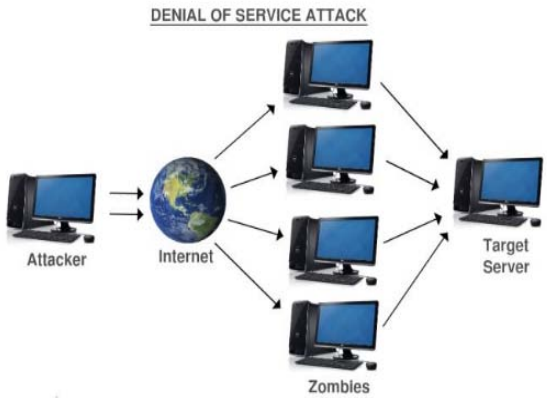

Figure 2: Denial of Service (DOS) Attacks

Instead, they try to make your servers and website unavailable to authorized users.In some cases, however, DoS is also used as a mask for other malicious actions, and to take down security applications such as firewalls.

Shared vulnerabilities: Cloud security is a mutual relationship between the provider and client. This relationship requires the client to take preventive actions to defend their data. While major providers like Dropbox, Box, Microsoft, and Google have consistent measures to secure their side, fine grain control is up to the client.

Data Loss:On cloud data can be easily lost through natural disaster, a malicious attack, or a data wipe done by the service provider as shown in figure 2.

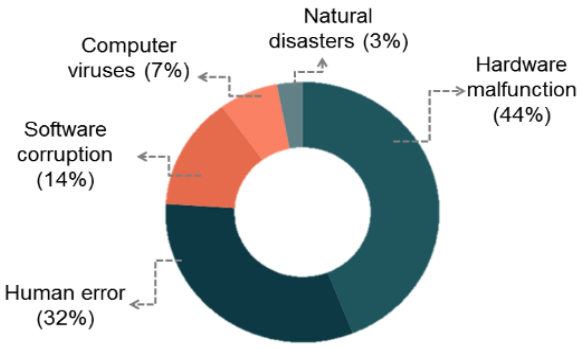

Figure 3: Analysis of Causes of Data Loss.

The businesses that don't have a recovery plan can get affected very badly if their sensitive data is lost by any means mentioned above. Securing your data means to look over your provider's back up measures or procedures as they relate to physical access, storage locations, and disasters.

III. Cloud Computing Challenges

The challenges related to cloud computing environment have always been there. Companies are well aware of the business value that cloud computing brings and are taking steps towards switch to the cloud. A smooth changeover involves a thorough understanding of the advantages as well as challenges involved. Like any new technology, the adoption of cloud computing is not free from challenges. Some of the most important challenges are as follows:

Security and Privacy: The topmost concern that everybody seems to agree as a challenge with cloud is security. The privacy and data security concerns are on the top of nearly every survey. For instance, hackers can use Cloud to organize botnet as Cloud frequently delivers more reliable infrastructure services at low price for them to start an attack [8].

***Interoperability and Portability*:** Businesses should have the power of migrating in and out of the cloud and switching to different providers whenever they need. Cloud computing services should have the ability to incorporate smoothly with the on premise IT.

***What to migrate*:** Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that organizations still have security/privacy concerns in moving their data on to the Cloud. The survey shows that in three-year time, 31.5% of the organization will move their Storage Capacity to the cloud. However, this number is still relatively low compared to Collaborative Applications (46.3%) at that time [9].

***Performance and Bandwidth Cost*:** Businesses can save some money on hardware but they need to spend more for the bandwidth. This can be a low cost for smaller applications but can be considerably high for the applications that require large amount of data. Delivering complex and demanding data over the network requires sufficient bandwidth. Because of this, many businesses are still waiting for a reduced cost before moving to the cloud

IV. CONCLUSION

Although cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the internet, there is much to be careful about. There are many new technologies evolving at a faster rate, each with technological advancements and with the potential of making human lives easier. But, one must be very careful to understand the security risks and challenges posed in utilizing these technologies has many advantages, but it also has different security concerns that could be raised. When data is being stored in big data centers all around the world, the data could eventually become a target for attacks or it could be altered by the employees of cloud service provider. With the advent of this technology, cloud computing was first commercialized and then its pros and cons were taken into consideration.

V. REFERENCES

[1] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” Computer Security Division, IT Laboratory, National Institute of Standards and Technology, Gaithersburg, 2011.

[2] Michael Armbrust, Matei Zaharia. "A View of Cloud Computing, April 2010, Communications of The ACM". *Cacm.acm.org*. N.p., 2017.

[3] M. Jensen, J. Schwenk, N. Gruschka and L. Iacono, “On Technical Security Issues in Cloud Computing,” *IEEE International Conference on Cloud Computing, Bangalore*, 21-25 September 2009, pp. 109-116.

[4] Haghighat, M., Zonouz, S., & Abdel-Mottaleb, M. (2015). CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications, 42(21), 7905–7916.

[5] M. K. Srinavasin, K. Sarukesi, P. Rodrigues, M. S. Manoj, P. Revathy, "State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment"*in Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, 2010.

[6] "Swamp Computing a.k.a. Cloud Computing". *Web Security Journal.* 2009-12-28. Retrieved 2010-01-25.

[7] "Top Threats to Cloud Computing v1.0" (PDF). Cloud Security Alliance. Retrieved 2014-10-20.

[8] S. Ramgovind, M. Eloff, Smith. “The Management of Security in Cloud Computing” *in Proceedings of IEEE International Conference on Cloud Computing, 2010.*

[9] Gens, Frank. "New IDC IT Cloud Services Survey: Top Benefits and Challenges". *IDC exchange*. N.p., 2009.

[10] B. Bashir, A. Khalique, “A Review on Security Versus Ethics”. *International Journal of Computer Applications*, Vol. 151, No. 11, 2016.

[11] H. Fayaz, A.Khalique, “A Review on Sociological Impacts of Social Networking”. *International Journal of Engineering, Applied Sciences and Technology*, Vol. 1, pp.6-12, 2016.

[12] T. Bazaz, A. Khalique, “A Review on Single Sign On Enabling Technologies and Protocols”. *International Journal of Computer Applications*, Vol. 151, No. 11, 2016.