IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Survey on Cloud Security Issues

Foram Suthar[1*], Samarat V.O. Khanna[2], Jignesh Patel[3]

[1]Department of Computer Engineering, Indus University, Gujarat, India
[2]Former Director of IICT, Indus University, Gujarat, India
[3]Department of Computational Engineering, Indus University, Gujarat, India

[*]*Corresponding Author: foram.suthar9@gmail.com, Tel.:07984334734*

DOI: https://doi.org/10.26438/ijcse/v7i3.120123 | Available online at: www.ijcseonline.org

Accepted: 16/Mar/2019, Published: 31/Mar/2019

Abstract— Everyone is moving from traditional services towards various cloud-based services at minimal cost. People are commonly using data storing and virtualization services because of their advantages. Increase in the use of these services is indeed increasing the challenges for its security in the cloud environment. Hence, security of cloud data and challenges related to it becomes the priority in the domain of cyber security. Many researchers have published different papers and have conducted different surveys related to security of cloud-based services, but researches show certain gap between cloud issue and their solution, few of them address data security issue and rest have virtualization problem. Here an effort is made to cover all factors related to security issue, and it has been derived properly and in clear way, which gives proper view of clouds security and challenges. Security of cloud platform is a major concern as the treats and attacks are increasing with advancement in the domain.

Keywords—Cloud Computing, Security, Virtualization, Cloud services

I. INTRODUCTION

Today we are living in a world surrounded by technology. The use of technology is increasing day by day because of the internet. Cloud computing is possible only because of the high-speed internet. Cloud symbol represents the communication over the internet. Now a day, many small and big organization are rapidly moving to the cloud network because, it provides fast access to the application and reduce the cost of the organization. Cloud computing is a model and works as a service provider. It provides different services or resources to the user so that an individual may not purchase the required service as a whole but can easily access it by giving nominal charges to the services provider.

Cloud computing works as a distributed system and gives the idea of two terms: virtualization and abstraction. Virtualization is related to resource pooling and resource sharing. More than one user can access the same resource at the same time from a multiple different location. Real life example of virtualization is electricity which is coming from sub-station and distributed into a different location and can be accessed by different people at the same time. Abstraction on other hand gives the abstract idea about resources. Here, data location, system information and other relevant details are not known to users. Cloud computing provides different resources like software, hardware, application, memory, networks etc. As per NIST “Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Network, Server, Storage, Application and Services) that can be rapidly provisioned and released with minimal management effort or servicers provider interaction”.

Cloud computing provides several characteristics like On-Demand self-services, Resource pooling, Broad network access, Elasticity, Virtualization etc. Cloud application developers have successfully developed an application for IaaS (Information as a Service) and PaaS (Platform as a Service) platform. This platform provides basic security services like firewall policy, user authentication policy, authorization, secure logging policy but still, data security is one of the basic biggest problems for cloud users [1].

Data comes at the topmost level for security in cloud computing due to multi-tenant and resource pooling nature. So, cloud infrastructure must provide extra level of security for data at server side, because data is communicated over the internet [2]. So, it is difficult to secure data against the threat of unauthorized person accessing the same. If the web application is insecure, customer cloud uses SQL injunction [3] to get, delete and manipulate another customer’s data. In order to prevent attacks in cloud infrastructure, implementation of an appropriate security mechanism is needed.

Virtualization play another important role in cloud computing, it provides resource sharing feature to the cloud user. Hardware virtualization is provided by IaaS based model of cloud computing, while on the other hand programming virtualization is offered by PaaS based model. It opens the door for new and unexpected multiple attacks. Virtualization gives the concept of Virtual Machine image [4] and Live Migration [4] which supports the cloud user but also induces the threats for the cloud. Hence, when security in cloud is at stake, two major aspects are to be considered equally i.e. data security and virtual machine security [5].

The paper is organized as follows, Section I contains the introduction of cloud computing and problems occurring in cloud computing, Section II contain detail description of cloud deployment model, Section III contain the challenges and security issues in cloud computing, Section IV concludes research work with future directions.

II. CLOUD DEPLYOMENT MODEL

Cloud offer two types of model one is based on services and another is based on infrastructure.

A. Cloud Service Model

Cloud service model is divided into three parts:

1) *SaaS (Software as a service)*
   - SaaS is software delivery model, delivering single application to multiple users. SaaS service is fully controlled by CSP (Cloud Service Provider) so customer has minimum control on security because executing platform lies outside the network of the user.
2) *IaaS (Infrastructure as a Service)*
   - IaaS provides virtualized computing resources over the internet. IaaS provide greater user control as compare to SaaS but less than that of IaaS.
3) *PaaS (Platform as a Service)*
   - PaaS provides all infrastructures to create and manage customer application. It gives maximum customer control on security as compare to IaaS and SaaS because execution platform lies inside the network of the user.

B. Cloud Deployment model

Cloud deployment model is categorized into four sub models.

1) *Public Cloud*
   - Cloud model is set of resources provided by cloud service provider. This service is provided to user or large business enterprises. Server is located at CSP (Cloud Service Provider) side, so security part is also manged by CSP. User remain unaware of file location used by CSP, geographical location of server and how data is stored within server. Thus, organization compromises with security which indeed is a major concern.
2) *Private Cloud*
   - Resources related to cloud are provided to an organization or a company by CSP. Ownership of cloud is with single organization or CSP. Private cloud solves the security issue of public cloud because cloud is manged by that organization only but, it introduces problems related to storage management, maintenance and keeping track of capacity.
3) *Community Cloud*
   - Community cloud serves the common function and purpose such as security, policies, mission, regulatory compliance etc. which is needed by multiple organizations. Cloud is manged by organization or third party. Main drawback of community cloud is data gets spared to multiple organizations [6] so data security and data privacy are compromised.
4) *Hybrid Cloud*
   - Hybrid cloud is mixture of more than two cloud models i.e. public, private or community. All models remain unique entity but bond with some standards and policies. Hybrid cloud offers cost and scale effective services as compared to public cloud but on other hand, compromises with data security when data migrate from public cloud to private cloud or vice versa.

III. CLOUD SECURITY ISSUES AND CHALLENGES

It is a huge leap for a user to switch from traditional service provider to cloud service provide, because trust is the major factor as data of the user is at stake. Trust is measure, which is generally based on some factor like data security, Virtual Image security, government policies etc. For security of cloud systems, here there is a consideration of three major factors: Confidentiality, Integrity and Availability (CIA).

A. Confidentiality

- Confidentiality assures that private and confidential information is restricted to access or disclose for unauthorized customers. In cloud environment service is distributed to multi-tenant user so it is possible that one of the users from group want to get unauthorized access of other customer data which is stored at same location. It may also be possible that CSP itself act as intruder and try to get access to their customer's private data.
- On bases of confidentiality following two categories have been discussed here.

1) Data Confidentiality

- Data transferred at CSP side is stored and processed in plaintext. CSP must take responsibility to protect client's data during its entire tenure. Data protection is basically done by different encryption techniques. CSP does not allow encrypting data at client side so the techniques used by CSP for encryption is not transparent which creates problem for data confidentiality. Migration of data is common process in cloud computing which cause problem in confidentiality. Migration is done by CSP. For example, user processes the data in India, stores it on server in UK and send it via US, then it became difficult to identified actual location of data [7]. When, user store data at server, data has to be backed-up for future purpose by CSP. For data back-up CSP sometimes use third-party support. Such an untrusted - third party can do unauthorized activity on customer's data.

2) Virtual Confidentiality

- IaaS offered hardware virtualization while PaaS offered programming virtualization service. IaaS provides virtual machine and virtual image-based services to cloud users for executing their program at server side. Anyone with authorized access to host can read and manipulate data which lies inside the VM (Virtual Machine), and hence it breaks the confidentiality. When data is basically migrated from physical storage to virtual storage in especially live VM migration [8], unauthorized user can do attacks (Trojan Horse) on other customer's data.

B. Integrity

- Integrity assured that information or data are only modified and changed by authorized party. Third person cannot access the data which are stored at cloud side. In cloud environment client's data or information transferred over the internet and cloud service are used by user via web browser, therefore all the web base attacks are likely to occur in cloud-based environment which can modify your data and try to break the integrity.
- Following categories have been discussed here under the various integrity requirements.

1) Data Integrity

- Data integrity is a big challenge for infrastructure as services, software as services and platform as services. Sometimes data integrity intentionally is done by CSP. CSP modified or discard the data which have been for past long time and not used by client regularly. Cloud provides storage service for data where user can store data for future purpose. There is possibility that attacker can delete or modify data during data backup process [9]. SQL injection attack is one of the common attacks that modifies the content of data which is stored in database on server side. Cross scripting attack is common malware injection attack where attacker adds malicious script (Java script, HTML, VBScript etc.) into vulnerable dynamic web page to gain data and access of user account and try to break data integrity.

2) Virtualization Integrity

- Not only for data confidentiality but for data integrity we need to take care during virtualization, especially for VMIs. CSP provider has full access of virtual machine because it is created by CSP. So, there is a chance that CSP itself do some malicious activity to get some user data. VM rollback and VM replication again introduce certain integrity problems in cloud computing. When we create replica of VMI, our data is transfer from one VM to another VM which allows hacker to get data from network.

C. Availability

- Availability assures that system is working smoothly, and services should be available all time to the customer. CSP provider must take care about the availability of services and is also responsible for a server health monitoring. Server degradation occurs during high load and over-consumption of resources which has to be taken care of by CSP. Cloud is providing multitenant services where the system has been shared with multiple users. Due to this service data, problems arise in data availability and virtualization availability which have been discussed in the following section.

1) Data Availability

- A DDOS (Distributed Denial of Service) attack is a very common and major attack in a cloud computing environment which breaks the availability. In DDOS attacker send a huge amount of request on the server. When the operating system of cloud computing detects huge amount of workload, it starts to work on it and provide more computational power. On the hand, a cloud computing server is fitting with the attacker. This type of attack was happed on the GitHub server on Feb 28, 2018. That server was hit with a sudden onslaught of traffic that clocked in at "1.35 terabits per second" which shows in (e.g. Figure 1). A natural disaster like flood, earth quick etc. is also breaking the data availability.

2) Virtualization Availability

- In VM migration, the unnecessarily virtual machine has to move from one physical server to another server. At this time high availability is required to store data properly. The hypervisor or VMMs may fail/crash due to some reason which affected all VM machine running into the server. Such a situation must be solved or recovered by CSP.

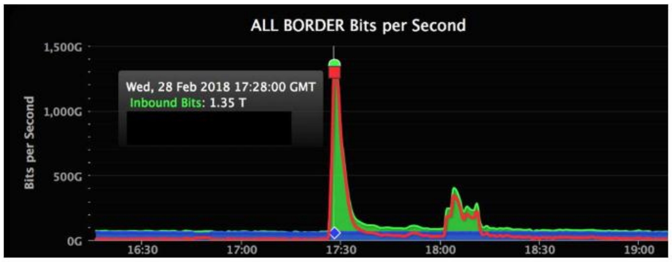

Figure 1. High Traffic on GitHub Server due to DDOS Attacks.

IV. Conclusion and Future Scope

Challenges related to security of cloud environment are addressed in this paper. Basic understanding of security defects in cloud computing environment and its awareness is discussed in the paper. Threat of various attacks occurring on cloud data and virtual environment has been conveyed. Many techniques and algorithms have been proposed to secure data and virtualization on cloud platform. Hence, security defects and the challenges in cloud-based systems needs to be understood and considered clearly. There is still a scope of improvement, as threats and challenges in the domain of security of cloud-platform is increased.

References

[1] Dean, Jeffery, S. Ghemawat, *“Map Reduce Simplified Data Processing on Large Clusters”*, OSDI, **2008**.

[2] Chen, Deyan, and Hong Zhao, *"Data security and privacy protection issues in cloud computing"*, In the Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering**,** Vol. **1,** pp. **647-651, 2012.**

[3] T. Chou, *”Security threats on cloud computing vulnerabilitie”,* International Journal of Computer Science & Information Technology **5,** no**. 3 ,**p: **79**, **2013**.

[4] S. Nuno, K. Gummadi, and R. Rodrigues. *"Towards Trusted Cloud Computing."* HotCloud 9, no. **9**, p:**3**, **2009**.

[5] S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury, and P. Sarkar, *"Cloud computing security challenges & solutions-a survey"*, In the Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp**. 347-356, 2018**.

[6] Goyal, Sumit. *"Public vs private vs hybrid vs community-cloud computing: a critical review."* , International Journal of Computer Network and Information Security 6, no. **3**, p: **20**, **2014**.

[7] J. Wayne, and T. Grance. *"Guidelines on security and privacy in public cloud computing."* , 2011.

[8] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. B. Fernandez. *"An analysis of security issues for cloud computing."* Journal of internet services and applications 4, no. **1**, p**:5**, **2013**.

[9] Mahalakshmi, B., and G. Suseendran. *"An Analysis of Cloud Computing Issues on Data Integrity, Privacy and Its Current Solutions."* In Data Management, Analytics and Innovation, Springer, Singapore, pp. **467-482**., **2019**.

[10] W. Hanqian, Y. Ding, CH. Winer, and L. Yao, *"Network security for virtual machine in cloud computing",* In the Proceedings of the 2010 5th International Conference on Computer Sciences and Convergence Information Technology, Seoul, pp. **18-21**.

[11] Q. Wang, C. Wang, L. Jin, R. Kui, and L. Wenjing. *"Enabling public verifiability and data dynamics for storage security in cloud computing."* In European symposium on research in computer security, Springer, Berlin, Heidelberg, pp. **355-370, 2009**.

[12] Z. Kazi, and S. Vrbsky. *"Security attacks and solutions in clouds."* In Proceedings of the 2010 1st international conference on cloud computing, pp. **145-156**.

[13] J. Sen, *"Security and privacy issues in cloud computing."* In Cloud Technology: Concepts, Methodologies, Tools, and Applications, IGI Global pp. **1585-1630**., **2015**.

[14] S. Aguru, and B.MadhavaRao *“Data Security In Cloud Computing Using RC6 Encryption and Steganography Algorithms”* In International Journal of Scientific Research in Computer Science and Engineering, Vol.**07**, Issue**.01,** pp.**6-9**, **2019.**

[15] Y. Patil, and P. Deshmukh *“A Review: Mobile Cloud Computing: Its Challenges and Security”* In International Journal of Scientific Research in Network Security and Communication, Vol.**06**, Issue.**01**, pp.**11-13, 2018**.

Authors Profile

Mrs Foram Suthar pursed Bachelor of Engineering from Shankersinh Vaghela Bapu Institute of Technology, Gujarat, India in 2014 and Master of Technology from Nirma University in year 2016. She is currently pursuing Ph.D. from Indus University and working as an Assistant Professor in Department of Computer Engineering, Indrashil Institute of Science and Technology, Gujarat, India since 2016. She has published more than 4 research papers in reputed international journals and presented one paper at Springer international conference. Her main research work focuses on Cryptography, Cloud Security, Cloud Computing. She has more than 3 years of teaching experience.

Dr. Samrat.V.O.Khanna is former director of IICT, Indus University. He pursed Master of Technology in Information Technology Department. He has published more than 60 research papers in reputed international journals. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security, Mobile Computing, Web Technology based education. He has 17+ years of teaching experience.

Mr Jignesh Patel pursed Bachelor of Engineering from North Gujarat University, Gujarat, India in 2008 and Master of Engineering in 2013. He is currently pursuing Ph.D. from Indus University and currently working as Assistant Professor in Department of Computer Engineering, from Indus University, Gujarat, India. He has published more than 8 research papers in reputed international journals including conference like Springer. His main research work focuses on IoT based system, Cloud Security, Cloud Computing. He has 8+ years of teaching experience.