Cloud Security Threats & Frameworks: A Survey

Dr. Anurag Rai[1]
Director – Admin and Research,
JBIT, Dehradun[1]

Amit Saxena[2]
PhD Research Scholar, UTU,
Dehradun[2]

Dr. Manish Manoria[3]
Director, Sagar Institute of Research
& Technology, Bhopal[3]

Abstract: **Cloud is the pay per use model of providing Services and Resources to the Users without minimal Service Provider interaction. This model had revolutionized the domain of Computing as it leads to optimal utilization of shared Resources and other computational capabilities. As the Resources and Computing Capabilities in Cloud environment are very large, as well as the Load and User count is large, this leads to an opportunity for Hackers and unauthorized Users to avail the Services and access Resources for their own cause through unfair means. A lot of Security Threats, Attacks, Issues and Vulnerabilities currently exist in the Cloud environments. They degrade the performance of the Systems to a great extent. So, such issues are required to get resolved at the earliest to ensure the effectiveness and efficiency of the Cloud environment. There are various approaches to handle the above stated issues, leading to the optimal utilization of computing capabilities and effectiveness of the Cloud system. This paper provides a brief overview about the various proposed and implemented schemes that can act as a Solution for handling the various issues related to Cloud Computing, especially Cloud Security.**

Keywords: Cloud Computing, Cloud Security, Cloud Security Issues, Cloud Security Framework, Cloud Computing Threats, etc.

I. INTRODUCTION

Cloud Computing cannot be defined before knowing its few important attributes such as:
Multi - Tenancy: It means that the Cloud Computing uses shared resources instead of dedicated resources at different level such as host level, network level and application level [13].
Massive Scalability: It defines that the Cloud Computing can provide the ability to scale 'n' number of systems, and also its space [13].
Elasticity: Users can occupy and un-occupy any number of resources as per their need and convenience [13].
Pay As You Go: This is the foremost attribute of Cloud Computing as it let the user pay for only the services they are taking and nothing else [13].
Assembling of Resources: Users can arrange and manage additional resources, such as processing capabilities, network resources and storage [13].

Now, CLOUD COMPUTING is defined as "Cloud Computing is nothing but a parallel and distributed system which consists of numerous software, virtualised computers which are interconnected, storage, etc. which can be directly in access to the user for which the user needs to pay for only the facilities they opt for". Thus by this feature, the Cloud Computing Model is becoming popular in IT as it lets the user have hands on special databases at a very minimal cost [13].

Cloud Services

The major services offered by Cloud Computing are:
PaaS: Platform as a service-In this the vendor offers a development environment to application developers, toolkits and standards of development. It then receives the payment for the services they provide [2].
SaaS: Software as a service-In this the customer do not buy any software and then load it in the computer and do capital expense (CapEx),instead the user rents the software for use from the cloud and use it on operational expense(OpEx).The user can sometimes have access to free services for limited period of time [2].
IaaS: Infrastructure as a service-In this the vendor provides the entire infrastructure for a customer to run its applications. IaaS offers scalability and best of the technology and resources to its user [2].

Types of Cloud

There are mainly four types of cloud:
Private Cloud: It is a cloud infrastructure which is solely operated by a single organisation [15].
Public Cloud: In this type of cloud, customers or users from different organisation are mixed together and they use the same cloud or network [15].
Community Cloud: This type of cloud is shared by a community or group of organisations with a common goal [15].
Hybrid Cloud: Combination of public / private cloud [15].
Thus we can say that Cloud Computing comes with a lot of advantages:
* The cost of services have been reduced which leads to low cost of managing and maintaining IT systems.
* The data doesn't face any loss and thus by securing data loss the continuity of any business can be maintained.
* Storage capacity is also beyond measure which is again an advantage as it doesn't restrict the users about being worried for the storage space in the system.
* The user can anytime, anywhere access the cloud and its services which is an irreplaceable feature of Cloud Computing.

However anything which comes with so many advantages has some or the other kind of disadvantages related with it too:
* Security and Privacy are the most concerned area of any user of Cloud Computing, as there are many hackers

present on the Cloud Server which may replace or extract the data from the cloud.
* There is no concept of data transferring in cloud and it is a big bottleneck for the Cloud System.
* Accessibility of data 24x7 sometimes become a problem as the site may go offline or unreachable.

II. ISSUES IN CLOUD COMPUTING

There are few important issues related to Cloud Computing, such as:
Availability: It means providing the users with the needful services from any place [7].
Confidentiality: It can be defined as to keep the user data safe in its environment [7].
Access Control: It assures that only the authorised user can access the data from the cloud [7].
Data should not be changed by any illegal user, data loss, data leakage happens when data reaches in wrong hand, data locations are not known to the user, secure data transfer, etc [7].
Storage related Issues: They may arise as the data stored on the cloud is firstly fragmented and then stored at different locations on the cloud, if any such one location crashes, the complete data can never be recovered in that case [7].
There are certain loophole in policies of cloud management which results into lack of user control, unauthorised usage of data on the cloud, data standards are not maintained and also the handling of data.
Security Issues: They are due to unauthorised login, no data backup, Lack of Customer Trust, etc [7].
Attacks: They are the major issues in Cloud Computing [7]:
* **Denial of Service:** When a user makes too many requests to the cloud server, then DoS occur.
* **Cookie Poisoning:** The unauthorised users try to manipulate the cookie for having data access.
* **Encryption Attack:** The encrypted data is tried to be decoded by the attackers.
* **Sniffer Attack:** Sniffers actually track the entire data.

III. THREATS IN CLOUD COMPUTING

Threats are the major issues that require immediate solution; otherwise they may lead to severe damage and degradation of Cloud Environment, Resources, Services, Components, etc., thereby degrading the Quality of Service and Performance of the Cloud Computing Environment [8].
The common Threats in Cloud Computing include:
Vulnerability in Virtualisation: This is one of the important parts of the CC, whose job is to isolate different items working on the same physical machine [8].
Fault Tolerance & Service Availability: The data are stored on the cloud server and managed by others, however there may occur instances when this data is unavailable to the user due to system failure, etc [8].
Data Migration: The data stored on the server of the cloud is moved from one cloud server to the other; however the user who adopts CC doesn't want this to happen so that the security of the data is maintained [8].
Load Balance: The concept of handling the load is mandatory in CC so that the failures can be avoided [8].
Data Confidentiality and Integrity: The data is stored on the cloud server on which different operations and modifications keep on taking place; to maintain the security and integrity of user's data only authorised access should be provided to enter the cloud server [8].
Interoperability: It is required to share applications among clouds and perform operations on different clouds simultaneously [8].
Scalable Data Storage: A cloud allows its user to put their data on the cloud and need not worry about its storage and backup as 2 basic features for the data is its security and reliability. The user should be able to access its data anywhere and anytime [8].
Latency and Motility of Data: Here latency means delay before a transfer of data begins following an instruction for its transfer. And data motility is a threat which is caused due to transferring of data from one cloud to other for storage and leaving some remnants behind which can be used by unauthorised users to tamper the security [8].

IV. RELATED WORK

The above mentioned threats and many more other threats challenges the security of the cloud server and for maintaining a secure environment of cloud server various Security Models have been proposed, such as:
Separation Model: In this model the main focus is laid on to separate the storage area and processing part of the cloud server to avoid data loss, data integrity, etc. which also increases the access speed of cloud and make it more successful [8].
Availability Model: The data is kept on separate places, one for processing and for storage. To make sure that the data is available to its user all the time for processing, two or more autonomous data processing services A & B is there and two data storage A & B respectively. Both cloud storage services are connected to services of replication between them [8].
Migration Model: The data is migrated between the different Cloud Storage Service such as A & B using the migration service of this model, and when the data is migrated from Cloud Storage Service A to Cloud Storage Service B, it is made sure that the data is secured and safe by cloud provider [8].
Tunnel Model: In this model a Tunnelling Process is activated between the Data Processing Service and Data Storage Service, which works as a communicator between the DPS & DSS. The tunnel helps in manipulating and retrieving the data [8].
Cryptography Model: It is an enhanced version of Tunnel Model with an additional function. The tunnelling provides an interface between Storage and Processing [8].
The data goes through the Tunnel and then the cryptography works which encrypts the data into a cipher text to which only an authentic user has its access on. Authenticate user can decrypt the cipher data, using public/private key [8].

The Cloud Multiple Tenancy Model of NIST: It basically means to allow multiple applications of Cloud Providers presently running in a server to offer Cloud services to users. MVMs are used to share resources among users [9].

The Cloud Risk Accumulation Model of CSA: As the different layers of clouds are built on each other ie PaaS is built on IaaS and SaaS is built on PaaS, this shows the relationship among services of the cloud [9].

* IaaS layer provides functionality to the user for maintaining the security of data, applications, OS, etc [9].
* PaaS layer provides the development power of customised applications based on PaaS platform [9].
* SaaS layer provides the most highly integrated service and security among all the three service layers [9].

The Mapping Model of Cloud, Security and Compliance: This model compares and checks recent good methods to find out the spaces between cloud architecture and framework and compliance framework and the corresponding security control strategies of Cloud Service Provider. It contributes to determine the situations to accept or refuse the security risks of Cloud Computing [9].

Multi Cloud Database Model: Multi Cloud database model represents Cloud Service Providers with multiple storage of data. This model doesn't assure the security of single cloud database, instead security and privacy of data is maintained by shared database by cloud provider which reduces the security risks in Cloud Computing. This model replicates data secretly to increase the privacy and security of data [8].

Jericho Forum's Cloud Cube Model: This model describes the concept of the cloud using the figures for describing the security attributes. There are various model's parameter described in this model which actually represent the cube formation and thus called as the Cube Model [9].

*** Internal / External:** It just describes the location of the data stored in the system. If the data is stored within the data owner's boundary, it is termed as Internal else External [9].

*** Proprietary / Open:** If the services provided by the cloud belongs to a particular organisation or there is a CSP having the ownership, then its Proprietary in nature otherwise it is termed as Open [9].

*** Perimeterised / De-Perimeterised:** This is just a parameter to define the architectural condition of the security protection of any application/data that if it is inside the boundary and secured or not [9].

*** Insourced / Outsourced:** Insourced means that the services presented by the cloud are done by its own employees whereas outsourced means that the cloud service is presented by any third party [9].

Private Virtual Infrastructure: This model was proposed keeping the data risks in mind. PVI thus focuses on security of data while transferring of data. It focuses mainly on the transfer stage. This model is made of two layers-PVI layer and Cloud Fabric Layer [10].

*** PVI Layer:** The information owner controls the security of data centre through firewall, intrusion detection system, etc to maintain the confidentiality of data [10].

*** Cloud Fabric Layer:** Cloud fabrics are controlled by CSP which maintain the physical (infrastructure security) and logical security (authentication, encryption, passwords, etc.) of data. Various security tools are also used to maintain the data security in the cloud [10].

Another security tool is Locator Bot Provider which provides details of all activities by monitoring the cloud security even at the destruction stage of data [10].

Privacy-Preservation Public Auditing: This model is implemented to ensure the security of data in the storage stage where data and metadata are held for future use. Three entities are collaborating together to achieve the required output [10]:

* Cloud User
* Cloud Server
* Cloud Service Provider

Third Party Auditor (TPA) is focal point as he has expertise and experience in auditing the data and from these audit reports the security of data can easily be done by tracing the path of data on the cloud [10].

Cloud Data Storage Security Scheme: The main focus of this Model is on the Data Storage Security.

V. CONCLUSION

Cloud Computing had revolutionized the Model for providing Services, Resources and Data to multiple Users in a shared manner, such that the Utilization of the Resources increases to the Optimum. It is very easy to acquire the Services of Cloud, as it is totally dependent on Internet, which in common for all in today's world.

But, Cloud Computing is also facing certain issues that need immediate resolution to ensure the Performance of the System. One of the major issues is Security. In this paper, we had discussed various Issues, Vulnerabilities and the Solutions that had already been proposed by other Researchers in this regard. Still, many Researchers, Professionals and Computer Scientists are working in this domain to develop some other Solutions for handling these issues in an efficient and effective manner.

REFERENCES

[1] V. Chang, M. Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Services Computing, IEEE, 2015
[2] Er. F. B. Shaikh, S. Haider, "Security Threats in Cloud Computing", Proceedings of the 6th IEEE International Conference on Internet Technology and Secured Transactions, December, 2011
[3] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, B. S. Lee, "Trust Cloud: A Framework for Accountability and Trust in Cloud Computing", Proceedings of the World Congress on Service, IEEE, 2011
[4] M. Theoharidou, N. Papanikolaou, S. Pearson, D. Gritzalis, "Privacy, Risk, Security, Accountability in the Cloud", Proceedings of the IEEE International Conference on Cloud Computing Technology and Science, 2013
[5] K. Hashizume, D. G. Rosado, E. F. Medina, E. B. Fernandez, "An Analysis of Security Issues for Cloud Computing", Springer Journal of Internet Services and Applications, 2013
[6] I. M. Abbadi, M. Alawneh, "A Framework for establishing Trust in the Cloud", Elsevier Journal of Computer and Electrical Engineering, Volume 38, 2012

[7] H. Takabi, J. B. D. Joshi, "Security and Privacy Challenges in Cloud Computing Environments", IEEE, 2010
[8] A. K. Gaur, P. Rana, V. Sharma, "A Parametric Analysis of Cloud Computing Security Models and Threats", International Journal of Computer Applications (IJCA), Volume 133, Number 13, Page 27 – 32, January 2016
[9] J. Che, Y. Duan, T. Zhang, J. Fan, "Study on the Security Models and Strategies of Cloud Computing", International Conference on Power Electronics and Engineering Applications, Page 586 – 593, Elsevier, 2011
[10] N. Mazher, I. Ashraf, "A Survey on Data Security Models in Cloud Computing", International Journal of Engineering Research and Applications (IJERA), Volume 3, Issue 6, Page 413 – 417, November – December 2013
[11] A. Singh, Dr. M. Shrivastava, "Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology (IJIET), Volume 1, Issue 4, Page 321 – 323, April 2012
[12] X. Jing, Z. J. Jun, "A Brief Survey on the Security Model of Cloud Computing", 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, IEEE, 2010
[13] E. M. Mohammed, H. S. Abdelkader, "Enhanced Data Security Model for Cloud Computing", International Conference on INFOrmatics and Systems (INFOS), May 2012
[14] Tamanna, R. Kumar, "Secure Cloud Model using Classification and Cryptography", International Journal of Computer Applications (IJCA), Volume 159, Number 6, Page 8 – 13, February 2017
[15] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", Special Publication, National Institute of Standards and Technology, US
[16] S. Ajoudanian, M. R. Ahmadi, "A Novel Data Security Model for Cloud Computing", IACSIT International Journal of Engineering and Technology, Volume 4, Number 3, Page 326 – 329, June 2012