Assessment of Security Issues in Cloud Computing

Zahra Jabeen, Mohd. Suaib

ABSTRACT--- A computing model in which the computing resources such as hardware, software and data are provided as a service via web browser or light-weight desktop machine on the internet is termed as Cloud computing. This computing model demolishes the requirement of keeping the resources of computer locally hence reducing the cost of worthy resources (Llorente, Montero & Moreno, 2012). A typical cloud is affected by various security concerns such as Temporary Denial of Service (TDOS) attacks, hijacking session issues, flashing attacks and theft of user identity. The motto of this study is to overcome the research gap between the cloud security constraints and the existing security danger. An investigation into the present cloud service models, presently applied security measures, security standards and their level of flawless shielding has been done. This thematic study helped in disclosing various security issues and their counter measures whereas the empirical study facilitated in acknowledgement of the botherings of users and security analysts in regards to those solution strategy. The empirical methods used in this research were interviews and questionnaires to justify the theoretical findings and to gain the originality of practitioners dealing with cloud security.

Keywords— Computing, security, cloud data breaching, theft of user's identity, hijacking session, flashing attacks.

1. INTRODUCTION

Cloud computing hosts and delivers the assorted processed work that is sent over the servers of internet. It is an appearing prototype which is multiplying its importance both in IT and business areas. It permits easy on request network access to a shared pool of customizable computing resources on rent. The services offered like processing and storage are operated with the use of web servers available as 'cloud 'and the GUI that is conveyed by the customer's browser. This technology was brought around 60's and has been progressive in its use from last decade.

Knowledge of varied assorted technologies like virtualization has brought cloud beside various services that may be chop-chop provisioned over the net with lowest attempt.

Concern of security risks in cloud atmosphere may be divided on the idea of various parts of cloud.

2. CLOUD DEPLOYMENT METHOD

• **Public Clouds** Providing services to the general public as an entity is dealt by this. Service provider positions the infrastructure on it's own end to choose all the activities of the cloud together with the owner and it's managerial rights. As a security prospect public clouds are not considered safe because the data is accessible to all public and there is no contract agreement with the provider. It's a mini projector aligned with a camera and a smart phone, which is subsequently connected to Cloud.

• **Private Clouds** Services provided to a specific organization wherever sharing of resources isn't required with different organizations is done here. Cloud resources are used strictly for one organization. Managed by a third party or an organization it could or could not be available at provider side. It is thought-about trusted as user encompasses complete management on the provided service and integrity parameters of data beside the network route [1].

• **Community Clouds** Services are offered to a bunch of organizations having identical deployment features as private clouds. It is essentially the private cloud for the cluster of organization with the general public cloud characteristics. Organizations in this cloud have trustworthy customers and are part of the community as in the private cloud.

• **Hybrid Clouds** A combination of all of the above stated clouds. These contain features and benefits of each introduced deployment model. Hybrid clouds have social control rights on organization and owners likewise as on third party supplier aspect. Either side can have their location. Trusted as well as untrusted users can be found in this deployment method. Restricted access of the private and community component resources is allowed to the untrusted users.

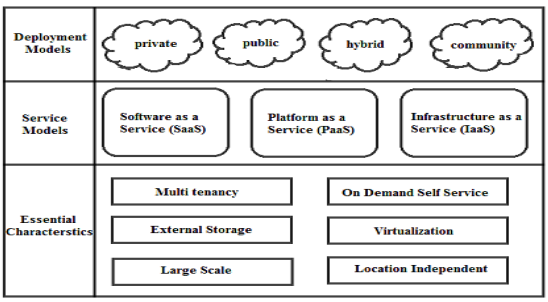

Figure 1. Cloud Deployment Models.

3. CLOUD SERVICE MODELS

A brief introduction about several models for cloud services are given below:

- **SAAS** A feature that is present for users to use the applications, that are available on the cloud infrastructure of service providers with the intention to provide access to users by different user end

Revised Manuscript Received on August 19, 2019.

Zahra Jabeen, Integral University, Kursi Road, Lucknow (jabeenmte@iul.ac.in)

Mohd. Suaib, Integral University, Kursi Road, Lucknow (suaib@iul.ac.in)

applications or by the using web-based clients. In this kind of service user don't have to be compelled to be troubled regarding cloud infrastructure, its network, in operation systems its storage or capabilities of application and their configuration.

- **PAAS** Platform as a Service is capable to assign an application created by the consumer by using any programming. It's usually done on basis of pay per use. A cloud is an infrastructure, which is combination of software and hardware having five basic features of cloud computing which can be stated as abstraction layer and physical layer. The end that contains all the hardware resources is termed as physical layer. All these resources are accountable to finish storage, computing and network services whereas on the reverse side the abstraction layer consists of software deployment in the physical layer. A brilliant factor is that user does not manage the infrastructure in fact he has the management on his deployed applications and even he can change the configuration of the application.

- **IAAS** Through this model the liberty to access processing, storage, networks and many other fundamental resources is given to consumer to use them as platform for deployment of software and other applications. Client is never allowed to manage cloud infrastructure however still relish the freedom to manage the functions and options of operation.

Figure 2. Cloud Service Models.

4. RELATED WORK & RESULTS

Sudhansu et al. recommended two algorithms for Data Security. In the proposed model, RSA algorithm is used for secure Communication and Encryption. Digital signature and hiding key information basically uses MD5 hashing.

Asif et al. recommended a new encryption algorithm for Cloud Data security. A proposed hybrid approach uses a compression data method to minimize the original data size and then ASIF Encryption Algorithm gives encrypted data. It reduces the size of data thus requires less storage space because of Data Compression method. This Algorithm performs multiple rounds based on the length of the key. It generates a random key in each round and also selects the key randomly in each round to encrypt the data. Matrix techniques are used for encryption.

Santosh et al. recommended technique for Cloud Storage Security known as Partitioning. Third Party Auditor is responsible for partitioning the data then secret key is generated for each partition proceeding to encrypt each partition using the respective keys, sending partition at appropriate cloud server. Encryption and decryption is done using RSA algorithm. This proposed technique has taken more time for encryption and decryption.

Manikondan et al. recommended Arocrypt Symmetric encryption algorithm to make sure cloud data is secure. Plain text is transformed into ASCII values. A square matrix is formed based on the number of characters in the plaintext. The square matrix is divided into three matrices called upper (UMAT), lower (UMAT) and diagonal (DMAT) matrix. Different keys encrypt the matrices. Based on encrypted value another square matrix is constructed. But, only the Cloud Service Provider side performs encryption.

Sunitha rani et al. recommends Data Security methodology which is used with three encryption algorithms for data encryption. Plain text is encrypted by the ceaser cipher at first. Then the encrypted result is again encrypted by RSA substitution algorithm and finally received result is again encrypted by the monoalphabetic substitution method. Presented technique takes more time to encrypt the data one by one by three algorithms.

Priya et al. combined Ceaser cipher and Attribute Based Cryptography (ABC) to propose symmetric algorithm thus improving cloud data storage end data security. This methodology contains three level encryption to encrypt the data. So, this methodology takes more time to encrypt the data and concentrate only on cloud storage data.

Pedro Costa et al described that in spite of the vast cloud concept adoption, most Decision Makers (DM) in IT industry have expressed doubts and concerns about how, what and when should migration be made to the cloud as there are no strict standards in adopting cloud computing. Hence stating their hindrances as "DM cannot evaluate Cloud services in IT organizations" and proposing a solution with a set of thirty measurement criteria measured on two cloud services; Microsoft Office 365 and Google Apps [2].

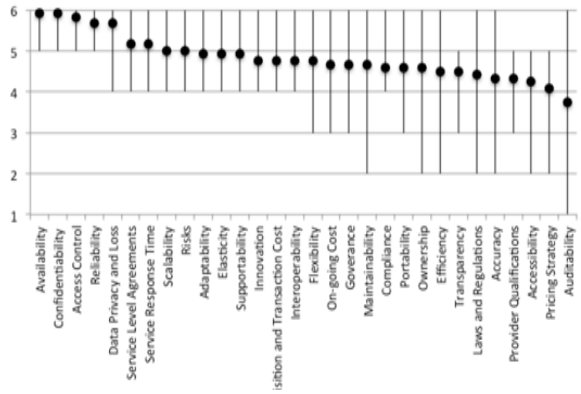

Figure 3. Measurement Criteria for cloud computing.

5. TRIGGERS FOR DATA SECURITY THREATS AND ISSUES

The crucial detection of the analysis done for the possible causes of data security threats are as discussed:

- Malicious insiders who have access to the sensitive information. They could steal the available information and perform any number of malicious activities or sell the data to other parties. Incidents reported since 2001 about data breaches are many in numbers which are as a result of malicious insiders.

- Absence of security measures and related tools at consumers end has raised accessibility and use of personal Webmail, social media and alternative sites which affect the safety of their browser, its underlying platform, and cloud service accounts. Solutions provided by Traditional antivirus and firewalls are not sufficient to provide protection to consumer end. [3].
- Cloud service provider's environment should not offer lack of understanding. If cloud consumers are unaware of providers' environment such as their hardware, software detail and VMware then security might be at risk.
- Without trusting the provider an Organization must not rush to adopt cloud technologies. Data security threats signifies lack of trust as it's major cause. Organization must assess their capabilities, procedures and policies before selecting a cloud service provider.
- The providers and the consumers should not offer lack of transparency in between. They must maintain transparent and strong relationship among themselves. [4].
- Variety of data security threats are exposed by organizations while relying on a weak set of interfaces. Cloud clients need to interact and manage with their providers using those set of interfaces. Hence the security of the cloud services is dependent upon the security of those basic interfaces.
- An assumption kept in mind while designing privacy rules is that protecting privacies are most reasonable at the ends. Privacy protection procedures and mechanisms are not completely exercised before defining the rules of privacy. Therefore cloud service providers assume that both ends are protected against privacy. [5]
- Poorly framed service level agreement (SLA). The existing SLAs only discuss about the services that are provided and if the services do not meet the agreement then the waivers given. Many other issues should also be discussed by SLA like methods, policies and their implementations.

6. CONCLUSION

The overall objective of this research study is to have a reflective manner towards the conclusions and results extracted from various group projects to use it in a way of improving teaching and learning methods.

A cloud serves various kind of service to its users each time such as spreadsheet applications, database services and word processing. The diversity reflected in the service shows a giant obstacle in implementing a mechanism for strong security. New cloud service model known as Dedicated cloud‖ has been proposed in this some research works to enhance the security of the cloud [6]. Whenever a user commands to a cloud, it contains a binary code to which the cloud server acts accordingly after understanding. If a single service is delivered by cloud server but on large scale, we may acknowledge in regards to all the valid commands to the cloud server. Hence, the cloud server will be interrupted for any invalid or bulk command that might have been sent to it. This ensures simplicity, scalability, troubleshooting, maintainability and would also assure the security of cloud automatically by integrating the cloud services into security itself. [7]

REFERENCES

1. Akshay Agarwal, Aravinth Subramanian,
2. 3rd National Conference on "Recent Innovations in Science and Engineering", May 6, 2017.
3. Nishantraj Pandey, Ranjeet Daroga International Journal of Scientific and Research Publications, Volume 5, Issue 5, May 2015 3 ISSN 2250-3153
4. Prof. Mr. D.S. Patil1, Mr. Shahak Patil, "IJRITCC | May 2014".
5. Karan Jeet Singh, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-4, Issue-5)
6. Dr. Ashwani Kush, *978-1-4673-7231-2/15/$31.00 ©2015 IEEE*
7. Mayank Kumar Jain, Shivani Shrivastri, Ratan Singh Computer Science and Engineering, RGPM Bhopal India
8. Shahbaz Pervez, Gasim Alandjani , Qurrat Ulain, Yanbu University College, Kingdom of Saudi Arabia, Information and Computer Technology Department, Department of Computer Science, COMSATS Institute of Information Technology Wah Campus Pakistan
9. Various Internet Sources like www.researchgate.net, dspace.hb.se, link.springer.com, www.inase.org etc