International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com

ISSN No: 2456 - 6470 | Volume - 3 | Issue – 1 | Nov – Dec 2018

Survey on Security Threats in Cloud Computing

Deepak Kumar Malviya
M.Tech, Department of IT,
UIT BU, Bhopal, Madhya Pradesh,
India

Umesh Kumar Lilhore
Associate Professor, Department of AI,
SAGE University, Indore, Madhya Pradesh,
India

ABSTRACT

Cloud computing is a new and innovative technology, which serves resources as a service to cloud user. Cloud computing technology provides optimum utilization of computing resources in less cost, which attract organization to be part of cloud customer market. Day by day cloud users are getting increases. Cloud serves IaaS, PaaS, SaaS and DaaS as a service on various private public, community and hybrid cloud levels. On cloud data is stores over the network and this network is shared and access by various cloud users, so data security and privacy are key concerns. Due to shared architecture of cloud, security is always challenging job. Various security methods are suggested by cloud researchers to maintain security and privacy for cloud data. In this survey paper we are presenting a review of various cloud security threats and available methods for protection.

Key Words: *Cloud computing, Cloud security, threats, Cloud services*

1. INTRODUCTION

The term **"**Cloud Computing**"** is the computing services in Information Technology like infrastructure, platforms, or applications could be arranged and used through the internet [1]. Infrastructure upon which cloud is built upon is a large scaled distributed infrastructure in which shared pool of resources are generally virtualized, and services which are offered are distributed to clients in terms of virtual machines, deployment environment, or software. Hence it can be easily concluded that according to the requirements and current workloads, the services of cloud could be scaled dynamically. As many resources are used, they are measured and then the payment is made on the basis of consumption of those resources [12].

Cloud provides various facility and benefits but still it has some issues regarding safe access and storage of data. Several issues are there related to cloud security as: vendor lock-in, multi-tenancy, loss of control, service disruption, data loss etc. are some of the research problems in cloud computing. In this paper we analyze the security issues related to cloud computing model. The main goal is to study different types of attacks and techniques to securethe cloud model [2].

2. CLOUD COMPUTING

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP**'**s) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet [3].

2.1 SERVICE MODELS OF CLOUD COMPUTING-

Generally cloud services can be divided into three categories:

2.1.1 Software-as-a-Service (SaaS):

SaaS can be described as aprocess by which Application Service Provider (ASP) providedifferent software applications over the Internet. This makesthe customer to get rid of installing and operating theapplication on own computer and also eliminates thetremendous load of software maintenance; continuingoperation, safeguarding and support.

2.1.2 Platform as a Service (PaaS):

"PaaS is the delivery of acomputing platform and solution stack as a service withoutsoftware downloads or installation for developers, IT managers or end-users.

2.1.3 Infrastructure as a Service (IaaS):

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective isto make resources such as servers, network and storage morereadily accessible by applications and operating systems.

2.2 TYPES of CLOUD COMPUTING

2.2.1 Public Cloud:

A Cloud infrastructure provides too many customers and is managed by a third party and exists beyond the company firewall. Multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically provision resources.

2.2.2 Private cloud:

Private cloud can be owned or leased and managed by the organization or a third party and exist at on premises or off-premises. It is more expensive and secure when compared to public cloud.

2.2.3 Hybrid Cloud:

A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. These clouds would typically be created by the enterprise and management responsibilities would be split between the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services.

2.2.4 Community Cloud:

Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations.

3. SECURITY IN CLOUD COMPUTING

Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services have various cloud security issues. Each service model is associated with some issues. Security issues are considered in two views first in the view of service provider who insures that services provided by them should be secure and also manages the customer's identity management. Other view is customer view that ensures that service that they are using is securing enough [5].

3.1 SECURITY ISSUES IN CLOUD COMPUTING-

Following are the major security threats [3,5,6]:

3.1.1 Elasticity-

Elasticity is defined as the degree to which a system is able to adapt to workload changes by provisioning and deranged resources in an autonomic manner, such that the available resources match the current demand at any time as closely as possible. Elasticity implies scalability. It says that consumers are able to scale up and down as needed. This scaling enables tenants to use a resource that is assigned previously to other tenant. However this may lead to confidentiality issues.

3.1.2 Multi-Tennancy-

Multi-tenancy is a major concern in cloud computing. Multi-tenancy occurs when various consumers using the same cloud to share the information and data or runs on a single server. Multi-Tenancy in Cloud Computing occurs when multiple consumers share the same application, running on the same operating system, on the same hardware, with the same data-storage system and both the attacker and the sufferer are sharing the common server.

3.1.3 Integrity:

Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location.

3.1.4 Insider & Outsider Attacks-

Cloud model is a multitenant based model that is under the provider's single management domain. This is a threat that arises within the organization. There are no hiring standards and providers for cloud employees. So a third party vendor can easily hack the data of one organization and may corrupt or sell that data to other organization.

3.1.5 Confidentiality:

Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers are not encrypting their communications.

3.1.6 Availability:

Availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that **companies have business continuity plans (BCP‟s) in order for th**eir systems to have redundancy.

4. RELEATED WORK

Although cloud service providers can provide benefits consumers, security risks play a major role in the cloud computing environment. Users of online data sharing or network facilities are aware of the potential loss of privacy [8]. According to a recent IDC survey [3], the top challenge for 74% of CIOs in relation to cloud computing is security. Protecting private and important information such as credit card details or patients' medical records from attackers or malicious insiders is of critical importance [5].

Moving databases to large data enters involves many security challenges [7] such as virtualization vulnerability, accessibility vulnerability, privacy and control issues related to data accessed from a third party, integrity, confidentiality, and data loss or theft.[1] Present some fundamental security challenges, which are data storage security, application security, data transmission security, and security related to third-party resources.

In different cloud service models, the security responsibility between users and providers is different. According to Amazon [8], their EC2 addresses security control in relation to physical, environmental, and virtualization security, whereas, the users remain responsible for addressing security control of the IT system including the operating systems, applications and data.

According to [3], the way the responsibility for privacy and security in a cloud computing environment is shared between consumers and cloud service providers differs between delivery models. In SaaS, cloud providers are more responsible for the security and privacy of application services than the users. This responsibility is more relevant to the public than the private cloud environment because the clients need more strict security requirements in the public cloud. In PaaS, users are responsible for taking care of the applications that they build and run on the platform, while cloud providers are responsible for protecting one user's applications from others. In IaaS, users are responsible for protecting operating systems and applications, whereas cloud providers must provide protection for the users' data [7].

[5] claim that the levels of security issues in IaaS are different. The impact of security issues in the public cloud is greater than the impact in the private cloud. For instance, any damage which occurs to the security of the physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems. In the cloud environment, the physical infrastructure that is responsible for data processing and data storage can be affected by a security risk. In addition, the path for the transmitted data can be also affected, especially when the data is transmitted to many third-party infrastructure devices [11]. As the cloud services have been built over the Internet, any issue that is related to internet security will also affect cloud services. Resources in the cloud are accessed through the Internet; consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through networks which may be insecure. As a result, internet security problems will affect the cloud, with greater risks due to valuable resources stored within the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used in the Internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud. Data confidentiality of the cloud through the Internet by hackers and cybercriminals needs to be addressed and the cloud environment needs to be secure and private for clients [6].We will address three security factors that particularly affect single clouds, namely data integrity, data confidentiality, and service availability.

5. TECHNIQUES TO SECURE DATA IN CLOUD

5.1 Authentication and Identity-

Authentication of users and even of communicating systems is performed by various methods, but the most common is cryptography. Authentication of users takes place in various ways like in the form of passwords that is known individually, in the form of a security token, or in the form a measurable quantity like fingerprint. One problem with using traditional identity approaches in a cloud environment is faced when the enterprise uses multiple cloud service providers (CSPs). In such a use case, synchronizing identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution.

5.2 Malware-injection attack solution-

This solution creates a no. of client virtual machines and stores all of them in a central storage. It utilizes FAT (File Allocation Table) consisting of virtual operating systems. The application that is run by a client can be found in FAT table. All the instances are managed and scheduled by Hypervisor. IDT (Interrupt Descriptor Table) is used for integrity checking.

5.3 Data Encryption-

If you are planning to store sensitive information on a large data store then you need to use data encryption techniques. Having passwords and firewalls is good, but people can bypass them to access your data. When data is encrypted it is in a form that cannot be read without an encryption key. The data is totally useless to the intruder. It is a technique of translation of data into secret code. If you want to read the encrypted data, you should have the secret key or password that is also called encryption key.

5.4 Information integrity and Privacy-

Cloud computing provides information and resources to valid users. Resources can be accessed through web browsers and can also be accessed by malicious attackers. A convenient solution to the problem of information integrity is to provide mutual trust between provider and user. Another solution can be providing proper authentication, authorization and accounting controls so the process of accessing information should go through various multi levels of checking to ensure authorized use of resources. Some secured access mechanisms should be provided like RSA certificates, SSH based tunnels.

5.5 Availability of Information (SLA) –

Non availability of information or data is a major issue regarding cloud computing services. Service Level agreement is used to provide the information about whether the network resources are available for users or not. It is a trust bond between consumer and provider. A way to provide availability of resources is to have a backup plan for local resources as well as for most crucial information. This enables the user to have the information about the resources even after their unavailability.

6. CLOUD COMPUTING SECURITY STANDARDS

Standards for security define procedure and processes for implementing a security program. To maintain a secure environment, that provides privacy and security some specific steps are performed by applying cloud related activities by these standards. A concept called **“**Defence in Depth**”** is used in cloud to provide security. This concept has layers of defence. In this way, if one of the systems fails, overlapping technique can be used to provide security as it has no single point of failure. Traditionally, endpoints have the technique to maintain security, where access is controlled by user.

6.1 Open Authentication (OAuth)-

It is a method used for interacting with protected data. It is basically used to provide data access to developers. Users can grant access to information to developers and consumers without sharing of their identity. OAuth does not provide any security by itself in fact it depends on other protocols like SSL to provide security.

6.2 Security Assertion Markup Language (SAML)-

SAML is basically used in business deals for secure communication between online partners. Itis an XML based standard used for authentication, authorization among the partners. SAML defines three roles: the principal (a user), a service provider (SP) and an identity provider (IDP). SAML provides queries and responses to specify user attributes authorization and authentication information in XML format. The requesting party is an online site that receives security information.

6.3 SSL/TLS-

TLS is used to provide secure communication over TCP/IP. TLS works in basically three phases: In first phase, negotiation is done between clients to identify which ciphers are used. In second phase, key exchange algorithm is used for authentication. These key exchange algorithms are public key algorithm.

The final and third phase involves message encryption andcipher encryption.

6.4 Open ID-

Open ID is a single-sign-on (SSO) method. It is a common login process that allows user to login once and then use all the participating systems. It does not based on central authorization for authentication of users.

7. CONCLUSIONS AND FUTURE WORK

One of the biggest security worries with the cloud computing model is the sharing of resources. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues and research challenges in cloud computing. Data security is major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. This paper has highlighted all these issues of cloud computing. We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture. As the development of cloud computing technology is still at an early stage, we hope our work will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

REFERENCES

1. Nikhit Pawar, Prof. Umesh Kumar Lilhore, Prof. Nitin Agrawal "A Hybrid ACHBDF Load Balancing Method for Optimum Resource Utilization In Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology,2017 IJSRCSEIT, Volume 2, Issue 6, ISSN : 2456-3307, 2017, PP 367-373.
2. M. A. AlZain, B. Soh and E. Pardede, A New Approach Using Redundancy Technique to Improve Security in Cloud Computing, Proceedings of The 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec12), IEEE, Kuala Lumpur, Malaysia,2012, pp. 230-235.
3. Umesh Lilhore, ,Dr Santosh Kumar, ”Advance anticipatory performance improvement model, for cloud computing”, International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 02, Issue 08; August - 2016 [ISSN: 2455-1457], PP 210-2014.
4. M. A. AlZain, B. Soh and E. Pardede, A new model to ensure security in cloud computing services, Journal of Service Science Research, 4 (2012), pp. 49-70.
5. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, Provable data possession atuntrusted stores, Proceedings of the 14th ACM conference on Computer and communications security, ACM, 2007,pp. 598-609.
6. H. Attiya and A. Bar-Or, Sharing memory with semibyzantineclients and faulty storage servers, Proceedings The 2003 22nd International Symposium on Reliable Distributed Systems, 2003, pp. 371-378.
7. A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, DepSky: dependable and secure storage in a cloud of-clouds, Proceedings of the sixth conference onComputer systems, ACM, 2011, pp. 31-46.
8. Nuaimi, K.A. Al Ain. Mohamed, N. Nuaimi, M.A and Al Jaroodi, J.,“A Survey of Load Balancing in Cloud Computing: Challenges and Algorithms”, Published IEEE Network Cloud Computing and Applications (NCCA)Second Symposium , 2012.
9. 2. Olivier Beaumont, Lionel Eyraud Dubois, Hubert Larchevque, “Reliable Service Allocation in Clouds”, IEEE 27thIEEE International Parallel & Distributed Processing Symposium (IPDPS) 2013.
10. P. Varalakshmi, Aravindh Rama swamy, A swath Bala Subramanian and Palaniappan Vijay Kumar, “An Optimal Workflow Based Scheduling and Resource Allocation in Cloud”, Springer, pp 411-420, year 2011.
11. Rohit O.Gupta and Tushar Champaneria, “A Survey of Proposed Job Scheduling Algorithms in Cloud Computing Environment”, International Journal of Advanced Research in Computer Science and Software Engineering, PP 782-790, year 2014.
12. K. Birman, G. Chockler and R. van Renesse, Toward a cloud computing research agenda, SIGACT News, 40(2009), pp. 68-80.