International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

Cloud Computing Security: A Review

Ms. Naindeep[#1], Ms. Sakshi[#2]

[1]Department of Computer Science and Application,
Choudhary Devi LalUniversity (CDLU), Sirsa
[1]naina.sandhu2@gmail.com

[2]Department of Computer Science and Application
Choudhary Devi Lal University (CDLU), Sirsa
[2]sakshi24.dhingra@gmail.com

Abstract— The process of accessing applications on the Internet is called Cloud Computing. With Cloud Computing we can construct and maintain our application dynamically. It provides us online data storage & other infrastructure required for our applications. Cloud refers to any form of **Network (public or private)** which is present at remote location. Almost all types of applications (Email, Video Conferencing, game etc.) execute in the cloud. Cloud Computing provides us facility to access any kind of information at any time. We only need an Internet connection for accessing different types of resources and services available on the cloud. Cloud environment provides virtual hardware and software to its user. This paper provides review of different security aspects of cloud data storage.

Keywords— Cloud Computing, Cloud Storage, Cloud computing Security

I. INTRODUCTION

Cloud refers to any form of Network (public or private) which is present at remote location. Almost all types of applications (Email, Video Conferencing, game etc.) execute in the cloud. Cloud Computing [1] provides us facility to access any kind of information at any time. The cloud computing provides different services to their clients called front end and the cloud itself refer as back end that provides such services to the clients [2].

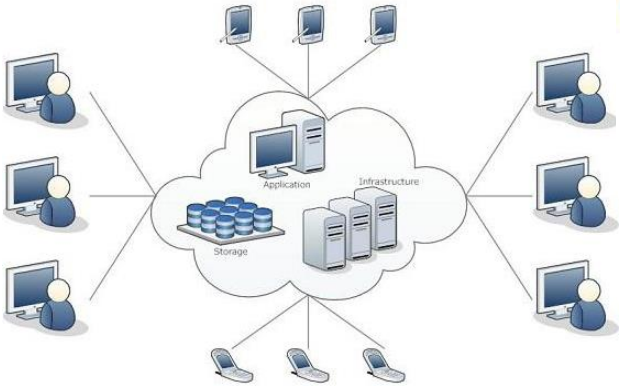

Figure 1: Cloud Computing

The basic concepts of back end (Cloud) and front end (clients) is shown in figure 1 above.

Cloud Computing provides multiple features to its users. Some popular features provided by cloud computing are explained below and shown in figure 2 below:

▪ Construct & maintain the applications dynamically at any time.

▪ User need not to install any specific software to access the cloud application. Users only need to connect with internet and authenticate them on the specific cloud.

▪ Any type of user can access applications provided on the cloud.

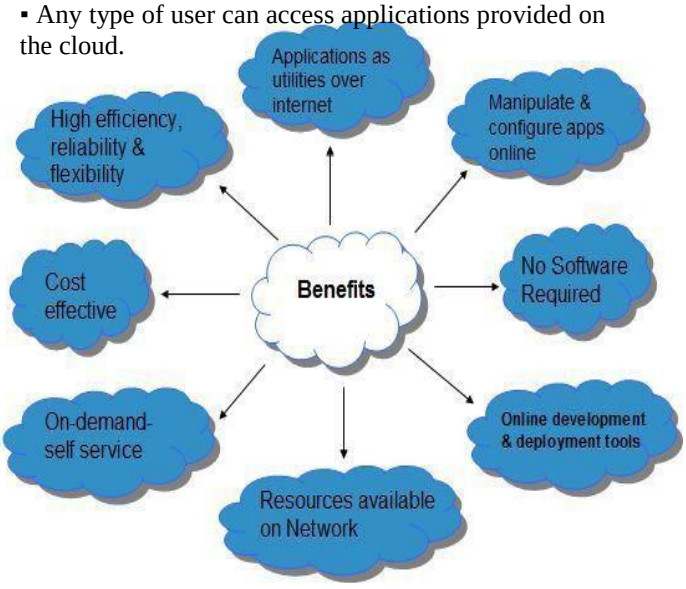

Figure 2: Features of Cloud Computing

▪ Using **Platform as a Service model**[3] the Cloud environment provides online application and software development.

▪ A user can access Cloud resources available over the network on any form of platform. Thus we can say that cloud computing provides platform independent access to cloud resources.

▪ The operating cost of Cloud Computing is not very high.
▪ Cloud Computing provides efficient load balancing so that each server on the cloud provides reliable & fast services to their clients.

Along with different features provided by cloud there are some drawbacks of using cloud computing. Some common risks associated with cloud computing are explained below:

SECURITY & PRIVACY OF CLIENTS DATA
The main risk associated with cloud is that client's data is available to third party. We need extra care while storing our important data on the cloud.

PORTABILITY (LOCK-IN) PROBLEM
The Cloud Service Provider (CSP) provides poor portability facility therefore clients are locked with one specific CSP & depend upon them for all kind of services.

INSECURE OR INCOMPLETE CLIENT'S DATA DELETION
When client delete some data from cloud then it is possible that data may not be deleted because duplicate copies of data may exist on the cloud.

From the above discussion we find that one of the main challenges related to cloud computing called data security of multiple clients. In this paper we present review of different security mechanism applied for cloud data storage security.

II. LITERATURE REVIEW

In the past several other works are performed for the cloud data security. The literature reviews of some of these works are explained below:

In 2009, Mohammed Abdelhamid [4] proposed multiple techniques based on RSA algorithm to enhance users' privacy. "His proposal is to authorize access to remotely-stored data to the users".

In 2010, S Subashini and V Kavitha [5] proposed a dynamic framework of security by different methods and techniques, Different part provides different types of security.

In 2010, M. Ahmed et al. [6] described the accuracy of various security issues related to clients and cloud resources. Their main aim to secure the cloud resources and client's data that is available on cloud server.

In 2011, V. Krishna Reddy and Dr. L. S. S. Reddy [7] proposed the architecture of different level of cloud security. Their main aim to secure the cloud resources and client's data that is available on cloud server.
They also provide study of different types of services provided by the cloud servers such as software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS)".

In 2011, Syam Kumar P and Subramanian R [8] proposed Elliptical Curvlet Cloud and sobel sequence for security of client data and cloud resources. "This protocol provides integrity (correctness) and secrecy of data. They also provide security against different hackers on the Internet.

In 2012, Abbas Amini [9] proposed secure storage system for cloud computing. "Their paper use RSA algorithm for cloud data integrity, and they also use AES algorithm to achieve secrecy of the client data storage".

In 2013, Sajjad Hashemi [10] proposed different security challenges for cloud data storage. "He also suggests different concepts to enhance the security of data storage in the cloud computing systems".

In 2014, Swarnalata Bollavarapu and Bharat Gupta [11] proposed cloud computing data storage system security for client's data. "This system uses different algorithms such as RSA, RC4 and ECC for encryption & decryption techniques".

In 2015, Dr. Salim Ali Abbas, Amal Abdul Baqi Maryoosh [12] provided an effective, flexible and secure method to impart security of clients' data and cloud resources. They also provide Elliptic Curve Cryptography algorithm for data correctness and security.

III. CLOUD COMPUTER SECURITY

The general aim of security is to provide user insurance that his/her data is free from any kind of danger. Using this general objective a secure system safeguards any kind of data or resources from unauthorized persons or hackers [23]. Therefore to attain the proper level of security, multi-level security mechanism must be implemented in an organization to protect its assets, resources and clients' data. According to Whitman [23] different security levels that an organization must have are explained below:

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

1. **Personnel Security**: With personnel security an organization appoint authorized individual or group of individuals for accessing and allocating all the organization resources and data.

2. **Information Security:** With information security an organization can safeguard and protect the confidentiality and correctness (integrity) and assets information for processing and storage.
3. **Physical Security:** With this security an organization can protect its physical assets and other essential properties from unauthorized access and misuse.

4. **Network Security:** With network security an organization protects its networking components & connections. It also protects organization contents that are transferred through networks.

5. **Operations Security:** With operational security an organization protects the information of all transactions and operations performed regularly.

6. **Communications Security:** With communication security an organization protects various technologies, communications media and their content from unauthorized access.

All the above security levels are integrated in an organization as shown in figure 3 below to protect its storage, data and resources from unauthorized users.

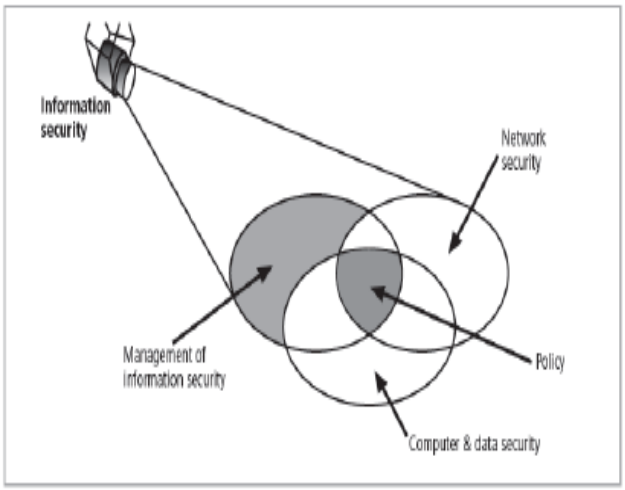

Figure 3: Multi-level security Components

IV. Cloud Security Principles

Ramgovind, Eloff, & Smith defined six cloud computing security principles [13]:

1. **Identification& Authentication:** The main purpose is to identify the users requesting access and their access priorities, then check permissions. This process is the same in cloud computing, regardless of the type or delivery model. Verifying and validating cloud users is done at this stage using security checks for usernames and passwords linked to the cloud profile.

2 **Authorization:** Authorization in cloud computing guarantees that referential integrity is preserved. It targets control and privilege processes that stream within cloud computing.
3 **Confidentiality:** Confidentiality is a core requirement to maintain control over the data of many organizations that may be located across several distributed databases. Confidentiality is a must when shifting to public cloud. Emphasizing confidentiality and protection of users' data and profiles at all levels will enforce information security principles at different levels of cloud applications.

4 **Integrity:** The integrity of information which requires Atomicity, Consistency, Isolation and Durability (ACID) properties must be enforced across all cloud computing delivery models.

5 **Non-repudiation:** Security protocols and token provisioning for data transmission, such as using digital signatures, timestamps and confirmation receipts services, should be applied to maintain non-repudiation.

6 **Availability:** When choosing among private, public or hybrid cloud vendors and making further decisions concerning delivery models, availability factors for the different vendors must be considered. This should be part of the SLA, possibly the most important document to be executed. It should define in detail the availability of cloud resources and services to be maintained between the provider and client.

The illustration below in figure 4shows a visual representation of the information presented above for different configurations.

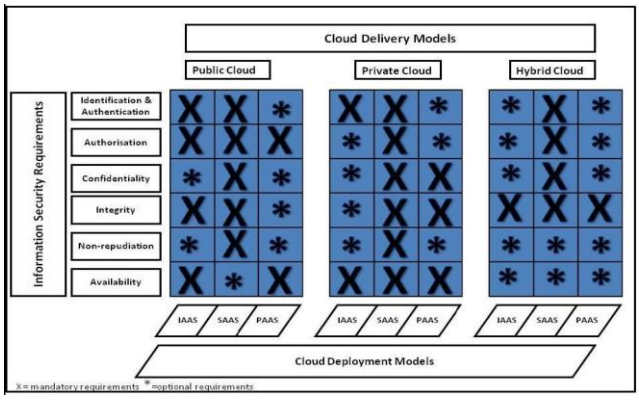

Figure 4: Cloud Computing Security Requirements

V. CONCLUSION

Cloud refers to any form of Network which is present at remote and distance location. Almost all types of applications such as Email, Video Conferencing, game etc. execute in the cloud. Cloud Computing provides us facility to access any kind of information at any time. The cloud computing provides different services to their clients called front end and the cloud itself refer as back end that provides such services to the clients. One of the main challenges related to cloud computing called data security of multiple clients.This paper provided review of different security aspects of cloud data storage.

REFERENCES

[1] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, "Cloud Computing, A Practical approach"

[2] B. Hayes, "Cloud Computing," *Commun. ACM*, vol. 51, no. 7, pp. 9–11, Jul. 2008.

[3] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," *NIST special publication*, vol. 800, no. 145, p. 7, 2011.

[4] Mohamed Abdelhamid, PhD thesis, "Privacy-preserving Personal Information Management", School of Computer Science, McGill University, Montreal, August 2009.

[5] S Subashini, V Kavitha, "A survey on security issues in service delivery models of cloud computing", Network and Computer Applications, Elsevier, Vol. 34, pp. 1-11, 2010.

[6] Mahbub Ahmed, Yang Xiang, Shawkat Ali, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp.723-730, 2010.

[7] V. Krishna Reddy, Dr. L. S. S. Reddy, "Security Architecture of Cloud Computing", International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

[8]. Syam Kumar P and Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

[9] Abbas Amini, MSc thesis, "Secure Storage in Cloud Computing", Department of Informatics and Mathematical Modelling (IMM), the Technical University of Denmark, May 2012.

[10] Sajjad Hashemi, "Data Storage Security Challenges in Cloud Computing", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.

[11] Swarnalata Bollavarapu and Bharat Gupta, "Data Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.

[12] Dr. Salim Ali Abbas, Amal Abdul Baqi Maryoosh, "Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography", Journal of Computer Engineering, Volume 17, Issue 4, Ver. I (July – Aug. 2015), PP 48-53.