Cloud Computing Security: A Review

[1]Nidhi Dahiya, [2]Mrs. Sunita Rani
[1]Student, [2]Astt. Proff.
[1]Department of Computer Science
[1]BPSM University, Khanpur Kalan, Sonipat(Haryana), India

***Abstract*— The process of using a network to store, manage, and process data, of remote servers hosted on the Internet to instead of a local server or a personal computer. With Cloud Computing we can construct and maintain our application dynamically. It provides us online data storage & other infrastructure required for our applications. We only need an Internet connection for accessing different types of resources and services available on the cloud. This paper will give a review about different security aspects of Cloud environment that provides virtual hardware and software to its user. In this review we will discuss the security of data. By using cryptographic encryption algorithms Cloud service providers (CSP) can provide a level of privacy and security to the cloud users. By following query any user can access the data from the cloud servers through decryption.**

***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].
The basic concepts of back end (Cloud) and front end (clients) and cloud infrastructure is shown in Figure 1 below.
Cloud Computing provides multiple features to its users. Some popular features provided by cloud computing are explained below and shown in figure 2 below: Many email services which are web based like Gmail and Hotmail deliver a cloud computing service: If any user want to access his email then he only need a internet connection and a web service regardless of what kind of hardware is on that particular computer. The emails are hosted on Google's and Microsoft's servers, rather than being stored locally on the client computer. Now a day's many other services are present like twitter Skype, media services(YouTube, voot)etc which are a example of cloud services.

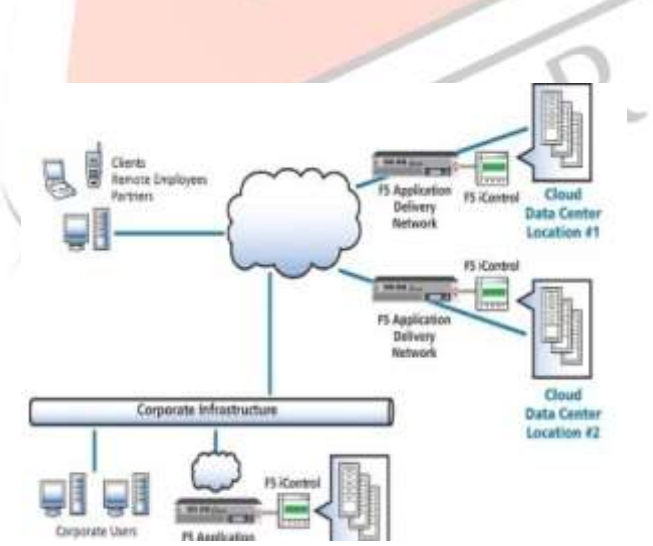

Fig.1: Cloud Comupting [17]

\

▪ 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.

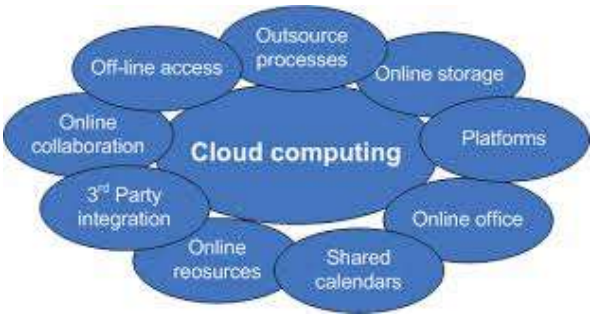

Fig. 2: Features of Cloud Computing

▪ 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[18]:

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[21].

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[18].

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[18].

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. "The main purpose of author is to authorize access to remotely-stored data to the users". so that all the data can be saved with authenticity.

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 uses some set of rules that is used to provide security and also to abstain the integrity called correctness of data. They also provide security against different hackers on the Internet that can be harmful for our data.

In 2012, Abbas Amini [9] proposed secure storage system for cloud computing. in their paper they uses algorithm for maintaining of accuracy of data as well as to enhance security.and for this they had used RSA Algorithm. And one other algorithm they have used is AES algorithm to keep secrecy of the client data storage".

In 2013, Sajjad Hashemi [10] proposed different security challenges for cloud data storage. "He also suggests various concepts to increase the security of data storage in the cloud computing systems". He uses algorithm acc to problem or challanges faced in security .for example he uses AES,DES.

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 R. Velumadhava Rao, K. Selvamani [12] identify various Data Security Challenges and its Solutions in Cloud Computing. the main purpose of this practical examination to enhance security of data so that can maintain integrity.

In 2015, Dr. Salim Ali Abbas, Amal Abdul Baqi Maryoosh [13] 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.

In 2016 AL-Museelem Waleed, Li Chunlin [14] provided assessment how the lack of security is affecting user's data and cloud resources. UEC (Ubuntu Enterprise Cloud) is used in this to solve problem of secrecy of authenticity. The algorithm they have used involves encrypting and decrypting data to ensure privacy and security integrity in the cloud**.**

III. PROBLEM DEFINITION

Cloud Computing is not secure computing model because there are many data security challenges. The data security is provided to the data which is stored in storage cloud by using the various encryption technique. But still there is a loophole through which the data integrity can be stalked i.e when data is transferring from the storage cloud to computational cloud for processing. So, in this thesis we are going to secure data in this stage to make the cloud computing more reliable technology for customers. There May be a problem when a unauthorized user try to access the cloud at first time cloud may ignore that request but for multiple time there is problem to ignore each and every time. so in this we have to find out the user or request which is coming again and again and also unauthorized.
for doing this there may be another problem arise which is to remember IP Address or Mac address of that machine so that we can block them. for this purpose we will use AES and DES and RSA along with homomorphic tokens.

IV. RISK AND SECURITY CONCERN

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 [15]. 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 [15] different security levels that an organization must have are explained below [19].

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[18].

2 **Eavesdropping:** An unauthorized user can access the data because of interception in network traffic, it may result in failure of confidentiality. The Eavesdropper secretly listen the private conversation of others. This attack may done over email, instant messaging, etc[19]

2. **Information Security:** With information security an organization can safeguard and protect the confidentiality and correctness (integrity) and assets information for processing and storage[19].

3. **Physical Security:** With this security an organization can protect its physical assets and other essential properties from unauthorized access and misuse.

4. **Network Level 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.

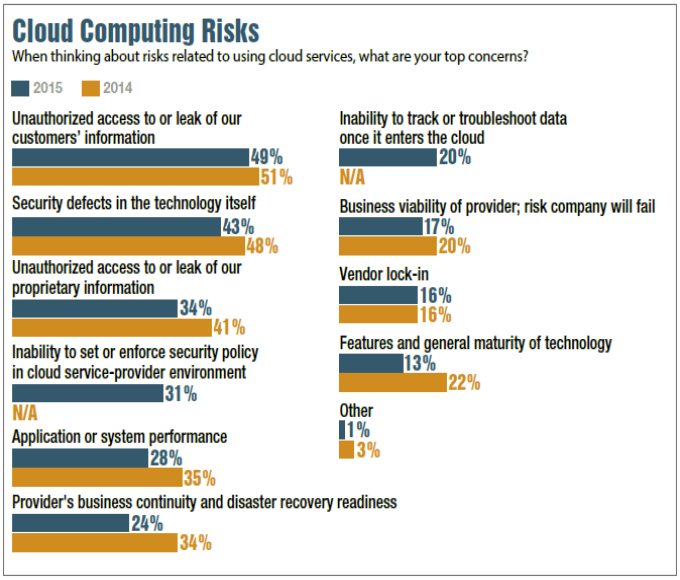

Fig. 3: Level of Risk [21]

V. CLOUD SECURITY PRINCIPLES

A cloud computing security principle determines the rules for imparting security of cloud data. Six cloud computing principles defined by Ramgovind, Eloff, & Smith are explained below [16]:

1. **Authorization:** Authorization preserves referential integrity in cloud environment. With this rule only authorized person access the cloud resources. All the unauthorized persons are denied for cloud services and resources[18].

2. **Integrity:** The integrity maintains the correctness of information stored on cloud servers. It follows ACID (Atomicity, Consistency, Isolation and Durability) property which maintains the integrity of cloud data[10].

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 we are working in a public cloud because there are chances that can affect integrity of data. Emphasizing confidentiality and protection of users' data and profiles at all levels will enforce information security principles at different levels of cloud applications.

4. **Non-repudiation:** With this principle security of cloud data is maintained by some Security protocols and token provisioning for transmission of data on cloud server to client and vice versa. To maintain non-repudiation different concepts are applied such as digital signatures, confirmation acknowledgement etc.

5. **Availability:** Another cloud security principle is availability of cloud vender. We must choose cloud vender among public, private, or hybrid cloud vendors according to facility and security required for our data. If specific cloud vendor is currently not available then wait for some time or choose the vendors that provide maximum security of client's data and resources.

The six cloud computing security principles for different configuration are shown in figure 4 below.

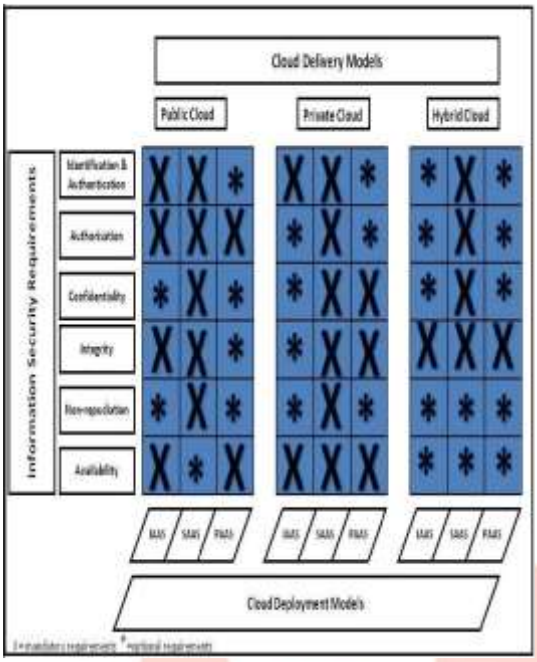

Fig. 4: Principles of Cloud Computing Security

6. **Identification & Authentication:** With this security principle we must identify the client making requests and their access privileges. If any client is not assigned to any service then he is denied for that service. The client authentication by username and password are also validated before accessing to any cloud service. The identification and authentication is the essential security principle for all types of clouds.

VI. 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. This Review paper give a view or idea about the problems that can be occur in a cloud computing system at multiple security issues. In this review paper we have discuss the security aspect of cloud. As well as we make the problem formulation of security.

REFRENCES

[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] ShankarNayak Bhukya, Dr.Suresh Pabboju ,Dr. K Venkatesh Sharma,"Data Security in Cloud Computing and Outsourced Databases", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016 978-1-4673-9939-5/16/$31.00 ©2016 IEEE.

[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.

[13] 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.

[14] AL-Museelem Waleed, Li Chunlin, "User Privacy and Security in Cloud Computing", International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352.

[15] M. E. Whitman, Principles of information security, 4th ed. Boston, MA: Course Technology, 2012.

[16] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in Cloud computing," in *Information Security for South Africa (ISSA), 2010*, 2010, pp. 1–7.

[17[Mr.V.Biksham, Dr. D.Vasumathi," Query based computations on encrypted data through homomorphic encryption in cloud computing security", International Conference on Electrical, Electronics, and ptimization Techniques (ICEEOT) - 2016 .978-1-4673-9939-5/16/$31.00 ©2016 IEEE

[18]Ahmed Albugmi,Madini O, Alassafi Robert Walters, Gary Wills," Data Security in Cloud Computing ,978-1-5090-1306-7/16/$31.00 ©2016 IEEE"
[19] R. Charanya1, M.Aramudhan2, K. Mohan3, S. Nithya4"Levels of Security Issues in Cloud Computing" ISSN : 0975-4024 Vol 5 No 2 Apr-May 2013 1912 International Journal of Engineering and Technology (IJET).

[20] Mrinal Kanti Sarkar,Sanjay Kumar," A Framework to Ensure Data Storage Security in Cloud Computing",978-1-5090-1496-5/16/$31.00 © 2016 IEEE.

[21] https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/

[22] ShankarNayak Bhukya, Dr.Suresh Pabboju ,Dr. K Venkatesh Sharma,"Data Security in Cloud computing and Outsourced Databases", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016 978-1-4673-9939-5/16/$31.00 ©2016 IEEE.

[23]Z.C Nxumalo, P. Tarwireyi, M.O Adigun ," Towards Privacy with Tokenization as a Service", Department of Computer Science,University of Zululand ,Empangeni, South Africa -978-1-4799-4998-4/14/$31.00 ©2014 IEEE.