Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 5, May-2016

Cloud Computing Security: A Review

Swati Mehta[#1], Raman Chawla[#2]

[1,2]Department of Computer Science

[1,2]N C College of Engineering, Israna

Haryana, India

[1]swtmehta92@gmail.com

[2]ramanchawla.cs@ncce.edu

Abstract— Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online. It offers online data storage, infrastructure and application. The term Cloud refers to a Network or Internet. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud. Cloud computing is highly promising technology because of its unlimited resource provisioning and data storage services which help us in managing the data as per requirements. But this area is still suffering problem of secure storage and communication of data inside the cloud and in between clouds also. Due to the use of internet and vital remote servers to maintain the data and applications, the cloud computing environment becomes open for the attackers to attack on the user data and communication services. This paper provides review of different security aspects of cloud data storage.

Keywords— ***Cloud Computing, Cloud Storage, Cloud computing Security***

I. INTRODUCTION

Cloud computing [1] comprises of 2 components —the front end and the back end. The front end includes client's devices and applications that are required to access cloud. And the back end refers to the cloud itself. The whole cloud is administered by a central server that is used to monitor client's demands (Fig 1).

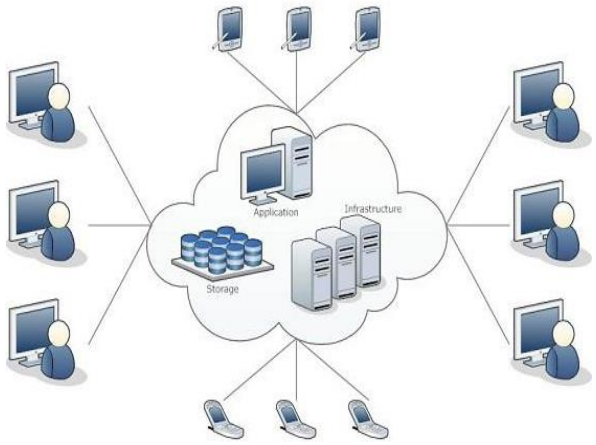

Figure 1: Cloud Computing

Cloud Computing has numerous advantages [2]. Some of them are listed below:

- One can access applications as utilities, over the Internet.
- Manipulate and configure the application online at any time.
- It does not require to install a specific piece of software to access or manipulate cloud application.
- Cloud Computing offers online development and deployment tools, programming runtime environment through **Platform as a Service model**.
- Cloud resources are available over the network in a manner that provides platform independent access to any type of clients.
- Cloud Computing offers **on-demand self-service**. The resources can be used without interaction with cloud service provider.

▪ Cloud Computing is highly cost effective because it operates at higher efficiencies with greater utilization. It just requires an Internet connection.
▪ Cloud Computing offers load balancing that makes it more reliable.

Although Cloud Computing is a great innovation in the world of computing, there also exist downsides of cloud computing. Some of them are listed below [2]:

SECURITY & PRIVACY
It is the biggest concern about cloud computing. Since data management and infrastructure management in cloud is provided by third-party, it is always a risk to handover the sensitive information to such providers. Although the cloud computing vendors ensure more secure password protected accounts, any sign of security breach would result in loss of clients and businesses.

LOCK-IN
It is very difficult for the customers to switch from one **Cloud Service Provider (CSP)** to another. It results in dependency on a particular CSP for service.

ISOLATION FAILURE
This risk involves the failure of isolation mechanism that separates storage, memory, routing between the different tenants.

MANAGEMENT INTERFACE COMPROMISE
In case of public cloud provider, the customer management interfaces are accessible through the Internet.

INSECURE OR INCOMPLETE DATA DELETION
It is possible that the data requested for deletion may not get deleted. It happens either because extra copies of data are stored but are not available or disk destroyed also stores data from other tenants.

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. In this paper we present review of different security mechanism applied for cloud data storage security.

II. LITERATURE REVIEW

Several works related to our work, which presents the security of data in cloud computing as follow:

In 2009 Mohammed Abdelhamid [4] proposes techniques to enhance users' privacy based on RSA algorithm. This proposal allowing users to authorize access to their remotely-stored data.

In 2010 S Subashini and V Kavitha [5] proposes a security framework by different methods provided dynamically, that one of the components of this framework refers to provide data security by storage and access to data based on meta-data, which is similar to storing related data in different areas based on metadata, and if the destruction of user data takes place, it can be retrieved. Each part of the framework in "security as a service" is provided for practical applications by providers of security as a layer or multiple layers of required applications.

In 2010 M. Ahmed et al. [6] described the accuracy of certain security issues related to cloud computing have examined and its aim is to explore and establish a secure channel for communication INO with the CSP, while the reliability and confidentiality of information is maintained. In addition, they have compared the provided protocol by the SSL of the activities associated with the work, along with the trustworthy security way to securing data.

In 2011 V. Krishna Reddy and Dr. L. S. S. Reddy [7] proposed the security problems at different levels of the architecture of cloud computing services have been studied. Security of customer-related data is a substantial need for services which is provided by each model of cloud computing. They have studied matters of on-going security software as a service (SaaS), platform as a service (PaaS) and Infrastructure as a Service (IaaS). This paper focuses on the use of cloud services and security for working cross-domain Internet connected.

In 2011 Syam Kumar P and Subramanian R [8] propose an effective and safe protocol by use ECC and Sobol sequence. This protocol provides integrity and confidentiality of data. Moreover, their system also supports dynamic data operations, which performed by the user on data stored in cloud while maintaining same security assurance.

In 2012 Abbas Amini [9] propose system for secure storage in cloud computing. This proposal use RSA algorithm for data integrity, and use AES algorithm to achieve confidentiality of the stored data.

In 2012 K.Govindaand Dr. E. Sathiyamoorthy [10] proposes a manner of secure data storage and identity anonymization in private cloud by use GDS (Group Digital Signature). They use the concept of key exchange with Diffie-Hellman protocol and strong RSA algorithm for the keys generation in addition to the process of signature, encryption and decryption.

In 2014 Swarnalata Bollavarapu and Bharat Gupta [11] propose data storage security system in cloud computing. This system use algorithms like RSA, ECC and RC4 for encryption and decryption techniques.

III. CLOUD COMPUTER SECURITY

The general definition of security is "the quality or state of being secure—to be free from danger" [12]. This implies that the objective is to protect the target from those who would, intentionally or unintentionally, do it harm. In fact, in order to achieve the proper level of security, an organization would require a multilayered system that guards the organizations entity, its resources, assets, and people. Whitman and Mattord believe that an organization should have the following security layers:

3.1 **Physical Security:** is required to defend property and physical assets from unauthorized access and misuse of physical items, objects, or areas.

3.2 **Personnel Security**: **is** required to guard the individual or group of individuals authorized for access to the organization and its operations.

3.3 **Operations Security:** is required to protect the information of a certain operation or sequence of operations or activities, including the logistics methodology.

3.4 **Communications Security:** is required to guard communications media, technology, and content from unauthorized access.

3.5 **Network Security:** is required to defend networking components, connections, and the content they manipulate.

3.6 **Information Security:** is required to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission.

All of these overlap and are part of information security, and policy must include and cover them all [12] as shown in figure 2 below.

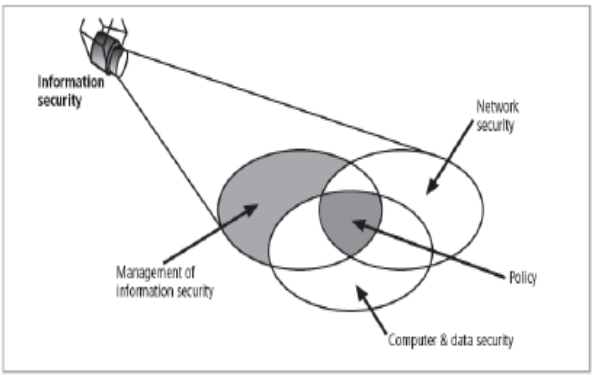

Figure 2: Components of Information Security

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 3 shows a visual representation of the information presented above for different configurations.

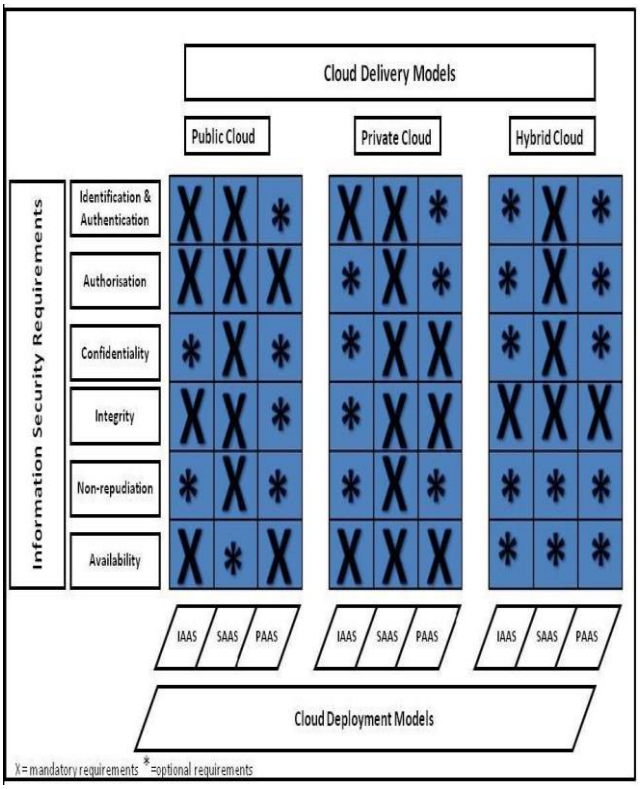

Figure 3: Cloud Computing Security Requirements

V. CONCLUSION

Cloud computing is an Internet-based computing, where shared resources, software and information, are provided to computers and devices on-demand. It provides people the way to share distributed resources and services that belong to different organization. Since cloud computing uses distributed resources in open environment, thus it is important to provide the security and trust to share the data for developing cloud computing applications. Cloud providers need to safeguard the privacy and security of personal data that they hold on behalf of organizations and users. This paper provides 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", Interna

[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] K.Govinda and Dr.E.Sathiyamoorthy, "Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud", Published by Elsevier Ltd., Procedia Technology, April, 2012.

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

[13] 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.

[14] G. Reese, *Cloud application architectures: [building applications and infrastructure in the Cloud]*. Sebastopol, CA: O'Reilly Media, Inc, 2009.

[15] J. W. Rittinghouse, *Cloud computing: implementation, management, and security*. Boca Raton: CRC Press, 2010.