
Salim Ahmad\textsuperscript{1}, Sanjeev Kumar\textsuperscript{2} & S. P. Singh\textsuperscript{3}

\textsuperscript{1}Research Scholar, Department of Information Technology, Nims University Rajasthan – Jaipur, India.
\textsuperscript{2}Department of Information Technology, Nims University Rajasthan – Jaipur, India.
\textsuperscript{3}Department of Computer Engineering, Nims University Rajasthan – Jaipur, India.

Abstract

Cloud computing is a model and services that are delivered over the network, from business and technological aspect it can be an information technology service model whereby computing services which comprises of hardware and software are delivered on demand to particular customers over the network in a self-service technique, independent of device and location which represents a paradigm shift in Information Technology. The cloud can be used in a different service models comprising of SaaS, PaaS and IaaS which are abbreviated as (SPI) and deployment models like (Private, Public, Community and Hybrid) as well as technologies that supports the entire process of cloud computing. Therefore, an analytical review of various cloud security mechanism will help users, researchers and new entrant in adopting cloud. Since, the cloud technology been an internet based storage facility is prawn to many security challenges, thereby reducing the security challenges by most users if the mechanisms are well implemented and used. The main purpose of the research paper is to analyze and compare the various cloud computing security mechanisms for improved cloud adoption and usage. The paper also contains a review of a comprehensive literature related to cloud computing security mechanisms where various cloud computing security mechanism are respectively described, in order to help users in making a decision to move Information Technology Resources to the cloud environment. A descriptive research methodology is used as a method of investigation in the research.

Keywords: Cloud Computing, Security mechanisms, encryption, SSO, PKI, Authentication, Authorization.
I. Introduction

Cloud computing security, that is most of the times basically refers to as cloud security is a larger terms strategies, tools, applications, and controls that are put together in order to developed ways and or methods to safeguard virtualized IP, data/information, applications, services, as well as the related infrastructure of cloud computing. It is an integral part of general computer security, network security, and generally, the information security. (Wikipedia, 2019). The storage facilities that are provided by Cloud computing technology to users with abilities to store and process the various data in the cloud provider (CSP) data centers, are suspicious of various threats and attack that most of the users are concern about (MG Durga, 2014). Users or group of people make use of the cloud technology in a diversity of different service models that are available like the Software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) as well as various types of deployment models that includes private, public, hybrid, and community which cloud services can be access through. The security challenges related with cloud computing technology are issues concerning the following (Sofiane Hamrioui, et al. 2017): the security challenges from the cloud provider’s perspective; that is those companies providing software-, platform-, or infrastructure-as-a-service through the cloud technology and the security challenges from the various customer’s perspective; those users who make use of the data storage facilities on the cloud. However, the responsibility for ensuring the security is intact from both perspective are shared, both the users and provider’s need to guarantee that their infrastructure is secure and that the users’ data and applications are secure, and also the user must devise means or rather ways to ensure the applications they are used used updated security mechanisms to be protected like the Multi factor authentication and various measures which will be discussed in the next segment of the paper.

II. Related Literature Review

So many researches have been done with regards to cloud computing security issues and challenge to mention a few. (Al-Muslim W. and Li C, 2016) conducted a study on the user privacy and security in the cloud computing and they looked at the advantages of using cloud services which comprises of scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Moreover, they highlighted that Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains of using cloud services, organizations are slow in accepting it due to security issues and challenges related with it. Security is one of the major issues which hinders the growth of cloud computing and the main issue is lack of trust from both party because the idea of handing over data and information to another (third party) is seems difficult to the subscribers of cloud services; such that the client need to be cautious in accepting the risks of data breaches in this new environment. (Awodele O. et al, 2016) Looked at the big data, and cloud computing, issues. The main emphasis is on security issues in cloud computing considering at how important data is for effective administration of any business, therefore cloud computing security is developing at a rapid speed which includes computer security, network security, information security, and data privacy. Cloud computing plays a precisesignificant role in defending data, requests and the associatedstructure with the aid of strategies, skills, controls, and big data
implements. Additionally, cloud computing, big data and its uses, benefits are expected to signify the most encouraging innovative edges in science; it is consequently essential to defend such significant infrastructure.

Reference to (Shrinivas A, 2016) in an “Overview of Cloud Deployment Models and Security Issues in Cloud” emphasis that a cloud computing is a type of computing in which different business processes and data application and information can be stored in the servers owned by third party (cloud Providers) and accessing them through internet services to users, rather than saving and installing them in offices or personal computers. The software and other resources can also be shared on demand by users. It allows the users to do computing services without the need for them to buy and set up IT infrastructure. According to (Nikita G. and Toshi S, 2014) in their article Cloud Computing – SPI Framework, Deployment Models and Challenges, said the security of data is the key issue for any cloud computing deployment. The organization need to make sure that the data and information is effectively safe and secured by different effective techniques so that the data can be preserved confidentially. Implementation of effective data control mechanism helps to keep data safe and secure from strangers. It is better to choose deployment model in accordance with the needs and functionalities of clients. The overview of virtualization in cloud computing as discussed by (Nancy J., and Sakshi C, 2016) (virtualization) virtual machine, it is a machine that helps to develop the efficiency of cloud computing. With the help of virtualization, it is possible to work on multiple operating systems and applications concurrently over a single server; therefore virtualization increases the utility and flexibility of hardware. Reference (Chakradhara R., Mogasala L., and Ramesh K, 2013) in their paper Cloud Computing Services and Deployment Models, discussed seven security issues which one should discuss with a cloud-computing provider: It states some set of policies, technologies, and controls deployed to protect data, applications, and the related infrastructure of cloud computing. Clients and organizations use the Cloud in a variety of different service models and deployment models. The seven (7) security issues that need to be discuss between client and cloud provider are: Privileged user access, Regulatory compliance, Data location, Data segregation, Recovery, Investigative support, Long-term viability. Asking the issues is very essential because, determining data security is harder at present technological advance, so data security functions have become more critical than they have been in the past.

From all the related works reviewed, one dominant problem is the issue of security associated with the cloud computing technology and which cannot be overemphasized. Therefore, the paper reviewed and explains various cloud security mechanisms in order to reduce such challenges and even eliminate it so as to improve implementation and usage.

III. Cloud Computing Security Mechanisms

Cloud Security Mechanism: are some set of fundamental cloud security mechanism that can be used to counter the security threats while accessing Data and or Information in the cloud/internet (G. Jasper W. Katherine et al, 2014) each and every user will have to provide his identity before the CSP will allow or grant access to that particular data
stored in the cloud. There are lots of security mechanism for cloud computing users but discussions will be restricted to Four (4) most commonly used, which consist of Encryption, Public Key Infrastructure, Single Sign On and Identity and Access Management.

- **Encryption**

Encryption as a cloud security mechanism is a digital coding system that is dedicated in preserving the confidentiality and integrity of Data, however if plain text data is applied, the data is then been paired with string of character called encryption. The following graphical representation clearly shows the concept of Encryption.

Figure 1: Cloud Security Mechanism- Encryption

![Encryption Diagram]

Source: Adapted from google.com

Therefore, the difference between Encryption and Decryption is that: Encryption is the process of converting the Plaintext into Cipher text. While: Decryption is the process of converting Cipher text into plaintext. So that, the receiver will receive the confidential message.

There are two (2) types of Encryption; Symmetric Encryption uses same key for both encryption and decryption which is sometimes known as Public Key Cryptography. And Asymmetric Encryption uses different keys that is Private Key and Public Key is also known as Public Key Cryptography.

- **Public Key Infrastructure (PKI)**

Public Key Infrastructure it is also sometimes known as Asymmetric encryption because it uses two keys both Public key and Private Key. However, there are different ways in which messages can be used in PKI or Public Key Cryptography that is sending Data to receiver in a confidential manner. These are Encrypted Messages, Signed Messages and Signed and Encrypted Messages by making use of the following PKI entities Certificate Authorization (CA), Registration Authorization (RA), Subscriber, Relying Party and Repository.
- **Single Sign-On (SSO)**

The SSO cloud security mechanism enables one cloud service user to be authenticated by a Security Broker which establishes a security context that is persisted while the cloud service user accesses other cloud services of cloud-based IT resources. Otherwise, the cloud service user would need to re-authenticate itself with every subsequent request. The SSO mechanism essentially enables mutually independent cloud services and IT resource to generate and circulate runtime authentication and authorization credential to each cloud user for efficient security.

- **Identity and Access Management (IAM)**

Identity and Access Management cloud security mechanism comprises the element and policies necessary to control and track user identities and access privileges for IT resources, environment and systems. Therefore, IAM cloud security mechanism occurs as a system that includes four (4) main components as follows:

1. **Authentication**: User name and password combination are the most common forms of user authentication managed by IAM systems, which can also supports digital signatures, digital certifications, biometric hardware (finger prints), specialized software (voice analysis). The below figure shows how authentication takes place using the client/user exchanging the security keys with the Cloud Provider Interface, where the client is authenticate through the cloud server.

![Cloud Security Mechanism - Client/User Authentication](image)

**Source:** Adapted from wikepedia.com

2. **Authorization**: The authorized components defined the character granularity for access controls and oversees the relationship between Identities, access control rights and IT resource availability.
3. **User Management**: In this instance it is associated to the managerial competence of the system; the user management program is answerable for producing different user characteristics and admittance groups, resetting passwords, defining password policies and managing privileges.

4. **Credential Management**: This system established identity and access control rules for defined user accounts, which mitigate the threat of insufficient authorization. The AIM mechanism is primarily used to counter insufficient authorization, denial of services and overlapping trust boundaries threats.

**IV. Methodology**

The paper is basically based on analytical review, that’s extracted from mainly the secondary sources comprising of (internet resources, published and unpublished journals, ebooks and many others) as the research methods of obtaining relevant data and information with regard to the topic of the research, in order to review and analyses some cloud computing security mechanism. That despite the problems or challenges associated with the general cloud computing technology; if these mechanisms are followed and implemented it will have a significant impact to users, thereby improving the level of implementation in general.

**V. Conclusion**

Conclusively, it can be said that despite the security challenges and issues that hinder users in making use of the cloud technology, it also affect the development and rapid growth of the technology. These issues and challenges can be reduced to its minimal level if not totally eliminated. Therefore, some basic cloud computing security mechanism like encryption, public key infrastructure, single sign-on, identity and access management that comprises of user account authentication, authorization, user management and credential management are all analyzed and discussed in the paper. So that, those cloud security challenges that affect adoption, growth and implementation of the cloud technology will be addressed, reduced drastically and ensure proper implementation and usage so as to allow users harness the numerous benefits associated with the general cloud computing technology.

**References**


