RNI: MAHENG/2016/68030 Vol. 4 Issue 5 Sep.-Oct. (2019): Page No.13-16 ISSN: 2456-5342 (print)

MAHATMA GANDHI MISSION MGMUNIVERSITY
MGM's JAWAHARLAL NEHRU ENGINEERING COLLEGE

VISTA INTERNATIONAL JOURNAL ON ENERGY, ENVIRONMENT & ENGINEERING

VISTA

# A survey on data security mechanisms in cloud computing

**Ajinkya A. Waghmare and Nitin R. Yadav***

Department of Master of Computer Applications,
MGM's Jawaharlal Nehru Engineering College, Aurangabad

**Corresponding author email :** nitinyadav@jnec.ac.in, Mob.: +91-9860841255

## ABSTRACT

This paper analyses the basic problem of data security in cloud computing. Cloud computing provides the way to share distributed resources and services of different organizations or sites that belong to cloud, meanwhile computing share distributed resources via network in the open environment as a result it makes security problems.

***Keywords :*** *Cloud computing, Data Security, Steganography, Encryption, Data-At-Rest and Data-In-Transit*

## 1.Introduction :

Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet). Cloud computing gives one to access to storage, database and a broad set of application services over the internet. With the growing use of cloud computing, Data security becomes most vital issue in cloud computing. Some important security services including authentication, encryption and decryption and compression are provided in Cloud computing system. Cloud computing has two modes to provide data security.

### 1.1 Data-At-Rest :

Data is at rest when it stored on a hard drive. In this state information is primarily protected by firewall and antivirus programs. Organization needs additional layers to protect data from intruders. Encrypting hard drives is one of the best ways to safeguard the security of data at rest. Carelessness is one of the major causes of leak today and one of the significant dangers to data at rest.

### 1.2 Data-In-Transit :

Data in Transit is data that communicated from one device to another. This is an information security concept that is used to identify data that requires encryption. Data in transit is a term used to describe data that is in transfer through network (cellular, Wi-Fi, or other network) or is located in RAM. Data in transit is also referred as data in motion or data in flight.

## 2. Literature Review :

Scientist team had proposed the protection method and approaches for reducing risk and threads and used Data-In-Transit and Data-At-Rest for data security aspects [1]. Team of researchers had proposed that data owners can remotely store their data in the cloud [2]. A brief introduction of cloud computing had been given along with its type and security issue and approaches to secure data in the cloud environment [2].

Scientist had proposed that the advantage of reducing cost by sharing computing and storage resources combined with an On-demand provisioning mechanism relying on a pay-per-use business model [3] and explained that how security trust and privacy issues occur in the context of cloud computing and discussed data accessibility aspects. Scientists are working on leakage-resilient authentication and data management system since it can be regarded as a prominent solution for secure cloud storage [4].

The different security techniques and challenges from both software and hardware aspects are to be considered for protecting data in cloud. This enhances the data security and privacy protection for the trustworthy cloud environment.

## 3. Cloud Security Mechanism :

Cloud security is used to secure the cloud data. The cloud security has various mechanisms, they are as follows:

- Encryption
- PKI (Public Key Infrastructure)
- SSO (Single Sign On)
- IAM (Identify and Access Management)
- Steganography

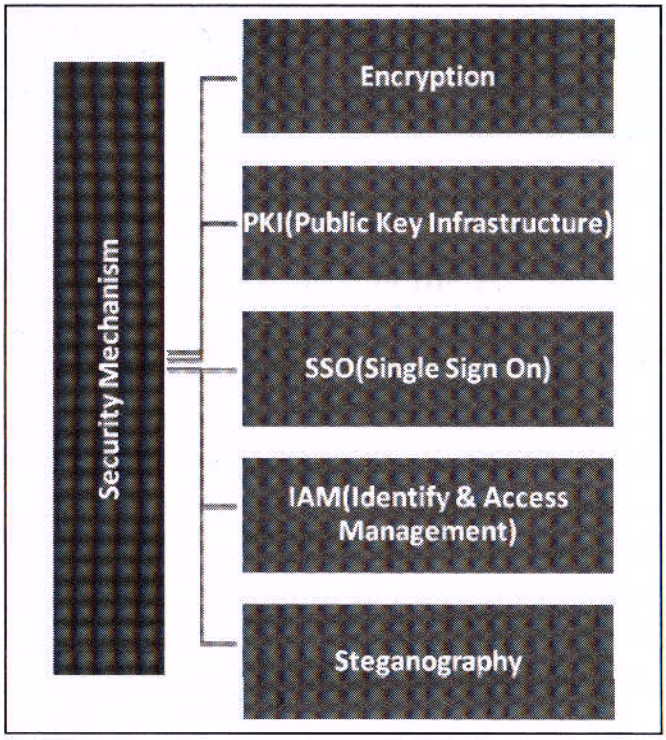


**Fig. 1 Security Mechanism**

### 3.1 Encryption :

Data encryption translates data into another form, or code, so that only authorized people can access to a secret key (formally called a decryption key) and they can read it. Encrypted data is commonly referred to as cipher text, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption [5].

#### a) Symmetric Encryption :

A single key is used to encrypt and decrypt the message sent between two parties. Symmetric encryption is fast, and this type of encryption is effective only when the key is kept absolutely secret and secure between two parties.

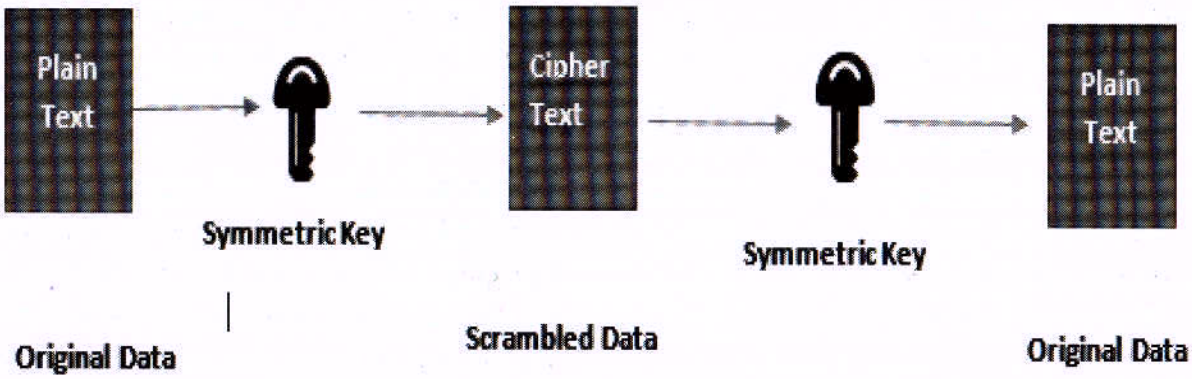


**Fig. 2 Symmetric Key Encryption**

**b) Asymmetric Encryption :**

A pair of keys is used to encrypt and decrypt the message. The pair of keys is termed as public and private keys. Private keys are kept secret by the owner, and the public key is visible to everyone. Here is how it works:

Suppose 'A' and 'B' want to communicate using asymmetric encryption. So 'A' encrypts the message with 'B' public key so that only 'B' can decrypt the message with its private key. After decrypting the message, 'B' will encrypt the message with 'A' public key so that only 'A' can decrypt it using its own private key.

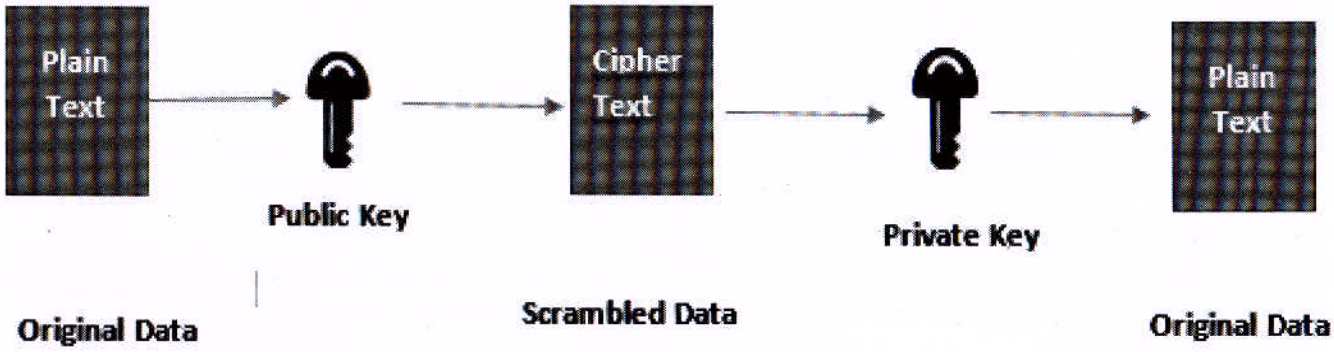


**Fig.3 Asymmetric encryption**

**3.2 PKI (Public Key Information) :**

The public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

Public Key Infrastructure is a type of asymmetric encryption. In this Public Key Infrastructure (PKI) three different formats of messages are encrypted message, signed message, signed and encrypted message with some entities.

- CA (Certification Authority)
- RA (Registration Authority)
- Subscribers
- IAM (Identify Access Management)

A Certificate Authority (CA) stores, issues and signs the digital certificate. A Registration Authority (RA) verifies the identity of entities requesting their digital certificate to be stored at the CA.

### 3.3 SSO (Single Sign On) :

Single Sign On is a session and user authentication service that permits a user to use one set of login credentials (e.g. name & password) to access multiple applications.

- No need to re-authenticate
- Improving productivity
- Minimize phishing

### 3.4 IAM (Identify and Access Management) :

One need an identity to access the data. It is necessary to provide access & identity is necessary for those only for us sending data. IAM system is used to store information of the user. It can also support digital signatures, digital certificate, biometric hardware, voice recognition etc. Data access governance and privacy management is a progressively essential aspect of identify and access management. It grants control over who can access user data and how it can be used and shared, including the application of user agreement.

### 3.5 Steganography :

Steganography is a technique of hiding secret data within an ordinary, non-secret, file or message in order to detection; the secret data is then extracted as its destination. The word steganography is derived from the Greek words steganos and the Greek root graph. One can use it to transport sensitive data from one point to another point with unknown data transfer. Steganography means hiding one piece of data within another unknown message. The message gets known on its detection [6-7].

#### a) Text steganography:

Text steganography can be applied in a format such as PDF, Digital Watermark and Information hiding. It is very difficult to realize the information hiding based on text. TextHide command hides the information in the way of text overwriting and words selection.

#### b) Audio Steganography:

Embedding the secret messages into digital sound's known as Audio Steganography. Audio Steganography method embed messages WAV, AU and mp3 sound files. HAS (Human Auditory System) are utilized in the process of Audio Steganography.

## 4. Conclusion:

Cloud Computing is a growing trend to provide a resource to store data over the network. But this stored data is not secured. In this paper we have discuss four different data security mechanisms for cloud storage. Security risk arises at two modes in cloud computing e.g. Data-At-Rest and Data-In-Transit. Data get more secured at both two modes of cloud storage by using mentioned strategies of security mechanism

## References:

[1] Ahmed A, Roert JW, and Madini A, Gary W, (2016) Data Security In Cloud Computing, Fifth International Conference on Future Generation Communication Technologies, April 2016, pp.56-59.

[2] Sharma S, Soni S. and Sengar S. (2012) Security In Cloud Computing, National Conference on Security Issues In Network Technology, August 11-12, 2012.

[3] Siani P, (2012) Privacy, Security & Trust in Cloud Computing, HP laboratories, 2012

[4] Seong H and Kazukuni K (2013) Towards Secure Cloud Storage, National Institute of Advance Industrial Science And Technology.

[5] Aized AS, Khan I, and Fazal A, (2014) A Review on Data Security in Cloud Computing, International Journal of Computer Application, 94(5): 12-20.

[6] Handa K, and Singh U, (2015) Data Security In Cloud Computing Using Encryption and Steganography, Journal of Computer Science & Information Technology, 4(5): 786-791.

[7] Yan Z, Deng RH, and Varadharajan V (2017) Cryptography and Data Security In Cloud Computing, Information Sciences, 387: 53-55