# Mutual Authentication in Cloud Computing - A Review

Harpreet Kaur[1]Usvir Kaur[2]
*(Student)[1] (Assistant professor)[2]*
*Department of Computer Science*
*Sri Guru Granth Sahib World University Fatehgarh sahib, Punjab, India*

***Abstract-*** *Cloud computing nowadays has been involved in everyone's life. This emerging technology allows users to share its resources globally. Cloud computing is aimed at providing IT as a service to the cloud users on-demand basis with greater flexibility, availability, reliability and scalability with utility computing model. Among all researching areas of cloud computing, mutual authentication is one of the popular areas for researchers whose main task is to attain a secure mutual authenticated environment by using various approaches. This paper discussed various types of mutual authentication techniques.*

**Keywords*:*** *Cloud computing, Mutual Authentication, Encryption, Steganography*

## INTRODUCTION

**1.1 Cloud Computing:[6]**Cloud computing, also known as 'on-demand computing', is anemerging technology in IT world. It is basically termed as online usage of resources. Resources can be shared among different CSP and cloud clients.

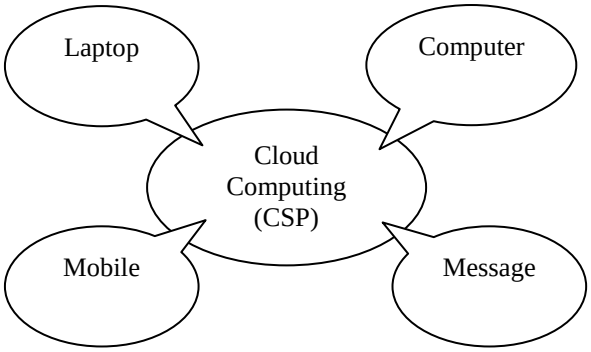


Figure1: Cloud computing

The term cloud is refered to as a set of hardware,Software, network, storage which are combined together and can be delivered as a servicein cloud computing. Cloud computing is still unclear to many security problems and user authentication, security of data stored in servers are challenging issues in cloud based environment.

Cloud computing is a model for convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services).

**1.2 Types of Clouds inCloud Computing [6]:**

***1.2.1 Public Cloud***: In this model, the cloud infrastructure is available to general public. It is usually operated by a large organization, government and a combination of both. Customers access resources and pay for the operating resources. The cloud services are taken from large resource pools that are shared by all end users. The location remains, separate from the customer and he has no physical control over the infrastructure.

The benefits of this type of cloud are its scalability and low capital costbut is also most vulnerable to various attacks**.**

***1.2.2 Private Cloud***: Cloud infrastructure is used by one organization. The cloud is externally hosted. It provides a limited access to its resources to consumers that belong to the same organization that owns the cloud. It offers high degree of data security, making it a popular option for organizations uncomfortable with storing information on someone else's infrastructure. The security and control level is highest while using a private network.

***1.1.3Hybrid Cloud*:** It is a combination of two or more cloud infrastructures i.e. private, public or community depending on their purpose. For example, public cloud can be used to interact with customers, while private cloud is use to secure the data of the customers. It includes standardized technologies that enable the cloud portability. The mission critical applications are placed on private cloud and remaining applications that are not mission critical stored in public cloud.

***1.1.4 Community Cloud:***This type of cloud infrastructure is shared by several organizations of a specific community. It is operated and managed by organizations, third party or combination of them. It is costlier than public cloud because cost is distributed over fewer customers but it provides high level of security.

**1.3 MUTUAL AUTHENTICATION:**

Mutual authentication is that security feature in which both the entities of communication link authenticate each other by providing or proving his/her own identity to one another. Hence before any communication channel sets up, client has to prove his originality by showing or proving his identity. Similarly, server has to prove his honesty by providing his identity to client process. This tool is

being widely used by companies or customers as it helps in minimizing the effect of online fraud. To create a secure connection between client and server, mutual authentication is a successful tool. Using mutual authentication, both the entities i.e. client and server can assure themselves that they are doing business with an honest or legitimate entity**[6]**.

A well- prepared or well-designed solution of mutual authentication helps in preventing data from various online attacks or frauds like Trojan Horse, man-in-middle attack, data confidentiality and many more.

## 1.4 CLOUD COMPUTING APPLICATION & MECHANISMS

Cloud computing is web based development and utilization of Internet based computing and storage. Cloud computing consists of three layers: the system layer, platform and application layer.

***1.4.1 Software as a Service (SaaS):***It represents the top layer of cloud computing. SaaS is one of the first implementation of cloud service. Using this application, clients can rent applications present on cloud according to their requirement instead of paying for an application.It allows the user to access services of cloud by running simple software like a browser. It is also referred as "on demand software" in which software and data are centrally hosted in the cloud. Google App, Window Azure, Oracle On demand are also the good examples of SaaS. [10]

***1.4.2 Platform as a Service (PaaS):***This is the middle layer of cloud computing. This service of cloud computing provides the clients a developed platform to design their necessary applications.PaaS offers an environment where developer can create and develop applications without worrying about memory and processors usage. The user is responsible for installing and managing the applications that it is deploying. Google App Engine, force.com, AppJet are some of the examples of PaaS. PaaS offers high level of abstraction. [10]

***1.4.3 Infrastructure as a Service (IaaS):***IaaS model represents the bottom layer i.e. system layer of cloud computing which include resources such as storage, memory, infrastructure of servers and network devices. It provides operating system and virtualization technology to its clients for managing resources. The client has to pay only when he uses this service. An example of IaaS model is Amazon's Elastic Compute cloud. EC2 provides web interface that allows customers to access virtual machines. It offers scalability under user's control with the user paying for resources by the hour. [10]

***1.4.4. File Storage****:* Cloud can offer you the possibility of storing your files and accessing, storing and retrieving them from any web-enabled interface. The web services interfaces are usually simple. At any time and place you have high availability, speed, scalability and security for your environment. In this scenario, organizations are only paying for the amount of storage they are actually consuming, and do so without the worries of overseeing the daily maintenance of the storage infrastructure. There is also the possibility to store the data either on or off premises depending on the regulatory compliance requirements. Data is stored in virtualized pools of storage hosted by a third party based on the customer specification requirements.[6]

***1.4.5. Backup****:* Backing up data has always been a complex and time-consuming operation. This included maintaining a set of tapes or drives, manually collecting them and dispatching them to a backup facility with all the inherent problems that might happen in between the originating and the backup site. This way of ensuring a backup is performed is not immune to problems such as running out of backup media, and there is also time to load the backup devices for a restore operation.[6]

***1.4.6. Disaster Recovery****:* This is yet another benefit derived from using cloud based on the cost effectiveness of a disaster recovery (DR) solution that provides for a faster recovery from a mesh of different physical locations at a much lower cost that the traditional DR site with fixed assets, rigid procedures and a much higher cost.[6]

## 1.5 THREATS IN CLOUD COMPUTING

There are various threats found in cloud computing that makes clients not to store data¸ use resources on cloud server. These threats are as follows.

- ***Man in the Middle Attack:***In this type, the communication between sender and receiver is relayed by a third person called attacker in the middle. The attacker can read out all the messages and can inject new one in the conversation.


Fig. 2: Example of Man in middle attack

The above figure shows the process of eavesdropping or relying by the attacker. A is the actual sender of the communication process where B is the actual receiver of the process. C acts as a man in the middle i.e. attacker who can harm the conversation. [6]

- ***Brute Force Attack:***This attack is widely used to break any code and to steal data or any sensitive information. One with powerful computing capability can make it successful as it require hundreds or thousands of possible passwords to send to the target user's account and keep sending

possible passwords until it get the correct one to access.[10]

- ***Timing Attack:***Using this attack, attacker leaks out the information from the system using measurement of time taken by the system to respond some queries. Any algorithm that has data dependent timing-variation can be used or targeted to apply timing attacks.[6]
- ***Replay Attack:***It is the type of attack in which attacker fraudulently repeats or delayed the actual data information. Session tokens, one time passwords, time stamping and many more are the solutions surveyed to prevent replay attack. [6]
- ***Masquerade Attack:***The type of attack in which attacker uses fake identity is called as masquerade attack. An unprotected authorization process can become vulnerable to masquerade attack. It can be accomplished using stolen passwords or logons.[6]
- ***Denial of Service Attack*:** Denial of service attack disrupt the network resource or host to make users unable to access or use computer services by flooding the network with useless traffic or bogus requests so that the services needed by legitimate users can be blocked.[10]

## 2. EXIXTING AUTHENTICATION PROTOCOLS

***2.1 Secret Sharing and Steganography:***Secret sharing and steganography is one of the finest protocols used for Mutual Authentication in cloud computing.

**Nimmy K., M.Sethumadhavan. et al [2]** proposed this scheme which is designed in such a way that it uses secret sharing for achieving authentication and uses steganography as an additional encryption scheme. In secret sharing, both client and server contain a part of secret on their sides which after combining becomes the complete secret. The secret contains information about both parties involved..To achieve mutual authentication, steganography and secret sharing is used with the assumption that cloud service providers and users are honest during the registration phase. It also involves human interaction i.e. out of band authentication which makes protocol more stronger by providing additional security. This protocol resists against different popular attacks such as man in the middle attack, replay attack and denial of service attack.

**M.Sarvabhatla, M.Giri, C.S.Voruguni. et al [3]** proposed a scheme which uses Steganography and Secret sharing same as **[2]** but claimed that their scheme is suitable for resisting more attacks such as Stolen Smart Card Attack, Password Guessing Attack, Insider attack and achieves strong mutual authentication. Their proposed scheme has taken off the resources consuming encryption decryption operations, stegano from client side to reduce heavy weight cryptographic operations on resource on client side. So, less computation requirement from client side makes this scheme more adoptable to use with resources constrained devices like tabs, mobiles etc.

***2.2 Smart Cards and Passwords*: G.Yang, Duncan.S.Wong, Huaxiong Wong, Xiaotie Deng[4] et.al** proposed the scheme of smart cards and passwords. This is also called smart card based password authentication scheme. It is implemented in the sense that client must have a smart card and he must know a password to gain access to server. This scheme is better suitable for resisting offline guessing attack. It also provide server authentication. It addition, they have added a generic construction framework to the scheme which allows them to use a protocol which is password based and is efficient enough to implement on smart cards.

***2.3 ECC (Elliptive Curve Cryptography)*:Tien-Ho Chen, Hsiu-lien Yeh, Wei-kuan Shih[5] et.al** proposed an elliptive curve crypto system dynamic based scheme for mutual authentication in cloud computing for remote devices. This scheme is more secured to authenticate remote servers and users for cloud computing. It consisted of three phases initialization phase, user registration phase and mutual authentication with key agreementphase. This scheme provides security against impersonation attack, insider attack, outside attack and mutual authentication.

***2.4Cryptography and Steganography:* V.K.Zadiraka and A.M.Kudina[1] et.al** has considered some new statements of problems insteganography and cryptography.Cloud based information communication system(CICS) are implemented for the distributed computing system.

The LSB steganography is one such technique in which least significant bit of the image is replaced with data bit. To make the data more secure, we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same provides higher security also.

Steganography is an art of hiding information in other information. In this technique, some of the messages are hidden in multimedia datum. Main purpose of steganography technique is to prevent the existence of the secret message from being detected by third party. So that the third party does not know where is the secret so that any malicious user will not be able to attack the secret.

***2.5 Digital Signatures along RSA Algorithm:* Uma Somani et al. [7]** surveyed the prevalent problem associated with cloud computing i.e. cloud security and appropriate implementation of cloud over the

network. This paper uses the concept of digital signatures along with RSA algorithm, to encrypt data while transferring over the network. This technique solves the dual problem of authentication and security. The encryption process is done by using RSA algorithm, and authentication process is done by using digital signatures. This paper compares RSA and AES algorithm in terms of key size and concluded that asymmetric encryption algorithm provides high security with the increased key size.

***2.6 Zero Knowledge Proof Protocol:*** **Mahmood Khalil Ibrahim et al. [8]** proposes a zero knowledge proof protocol by modifying diifie hellmann key exchange algorithm. Two versions of the proposed protocol are presented which solves the problem of man in middle attack in D-H key exchange algorithm. The version 1 is still vulnerable against man in middle attack. To protect the proposed algorithm from this attack, version 2 provides mutual authentication to prove that the server is honest. Analysis of the protocol shows that it satisfies the ZKP properties and resist against various attacks like discrete logarithmic attacks and man in the middle attacks.

## 3. CONCLUSION

Cloud computing is an advanced technology gaining acceptance day by day by providing services which are beneficial for users. But somewhere, the fear of losing data, fear of leakage of data or fear of any kind of fraud makes the client think twice before using this technology. This paper provides a review of mutual authentication for cloud computing in which a number of security features are provided. It provides solution to prevent popular attacks such as replay attack, man in middle attack and denial of service attack and many more.

## REFERENCES


[1] V.K.Zadirakaa and A.M.Kudina "Cloud Computing in Cryptography and Steganography" *Cybernetics and Systems Analysis, Springer*, pp. 584-588, 2013.

[2] Nimmy K., M.Sethumadhavan "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography", ICADIWT (*Applications of digital information and web Technologies*), IEEEfifth international conference pp.101-106, 2014.

[3] Mrudula Sarvabhatla, M.Giri, Chandra Sekhar Vorugunti "A Secure Mutual Authentication protocol for Cloud Computing using Secret Sharing and steganography", *Cloud Computing in Emerging markets*(CCEM) , IEEE, pp.1-8, 2014.

[4] G Yang, DS Wong, H Wang, X Deng" Two-factor mutual authentication based on smart cards and passwords", *journal of Computer and System Sciences* , vol.74(7), pp.1160-1172, 2008

[5] Tien-Ho Chen, Hsiu-lien Yeh, Wei-kuan Shih "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing" IEEE *conf. on Multimedia and Ubiquitous Engineering*, 2011.

[6] www.google.com

[7] U.Somani, K.Lakhani; M.Mundra "implementing digital signature with RSA encryption algorithm to enhance the Data Security of Cloud in Cloud Computing" PDGC *(parallel distributed and grid computing)*, pp. 211-216, 2010.

[8] M.K.Ibrahem "Modification of Diffie-Hellman key exchange algorithm for Zero knowledge proof", *future Communication Networks* (ICFCN), pp.147-152, 2012.

[9] F.F.Maghaddam, S.G.Moghaddam, S.Rouzbeh "A Scalable and Efficient user Authentication Scheme for Cloud Computing Environments", IEEE, 2014.

[10] Te-Shun Chou "Security threats on cloud computing vulnerabilities", IJCSIT (*International journal of computer science and information technology)*, vol5, pp.78-88, June 2013.