ISSN (e): 2250 – 3005 || Volume, 09 || Issue, 1 || January – 2019 ||
International Journal of Computational Engineering Research (IJCER)

Securing Multi User Authentication in Cloud Computing Using Secret Sharing

Sonali Patil
Associate Professor,Department of Computer Engineering,Pimpri Chinchwad College of Engineering, Pune, India.

Date of Submission: 28-01-2019 Date of acceptance: 11-02-2019

ABSTRACT
Cloud computing is a very much essential in various individual as well as business oriented applications. Cloud computing provides very cost-effective, scalable and flexible solution to the required applications. It provides large range of services. For sharing and availability of resources cloud computing is a great revolution. To access services on the cloud the user need to be authenticated. So, the authentication is one of the important problems in Cloud computing environment. In many applications multiple users are involved to get the things done. This type of applications needs authentication of all these users. This is called as group authentication or multi user authentication.
The multi user authentication is specially designed for group-oriented applications. Multi user authentication emphasis on communication between the members of a group and then authenticates the members. Security and privacy are major challenges in group authentication in cloud computing. Researchers have proposed various schemes for group authentication in the literature. This paper analyses the multi user authentication techniques in cloud computing. The techniques are compared on various parameters. The study shows that secret sharing based group authentication techniques are more effective compare to other techniques.
KEYWORDS: *Authentication, Group Authentication, Cloud Computing, Secret Sharing*

I. INTRODUCTION

Authentication is the process of determining the truth related to the identity of a person, a software program or ensuring that the product is found to be what its labeling claims to be. There is always a great difference between the process of authentication and authorization. The authentication always tends to the process of verifying that "You are tend to be who you say you are" Where as authorization is the process to providing verification for "You are permitted to do for what you want to do", For example a person having a proper Aadhar card gives the proof indicating the identity of that particular person, The client's who authentication request is permitted, only then he/she is authorized to acquire facilities for an Indian citizen, The process of authentication can be done in different ways depending upon the requirements. The first type of authentication techniques is acceptance of proof of identity given by a credible user who has the proper evidence relating to that identity.
The second type of authentication technique is the process of comparison among the attributes of the object itself to what is known about the origin of the objects. In group authentication, a group represents three or more individuals involved in sharing secret messages with each other. In this, communication is always done between the members of the group and authentication is provided to these members. The main purpose of group communication is to express, share and exchange information and ideas, in order to arrive at a decision regarding important matters and here communication is done to share secret messages, The communication among the members within a group is only through encrypted secret messages, Each user within a group has to register to become a member of that group, There is a group manager who performs the responsibility to reject or approve user to become member of the group. Once the user becomes the member of the group, he/she can communicate with other members within the group.

Cloud computing, also on-demand computing, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand.

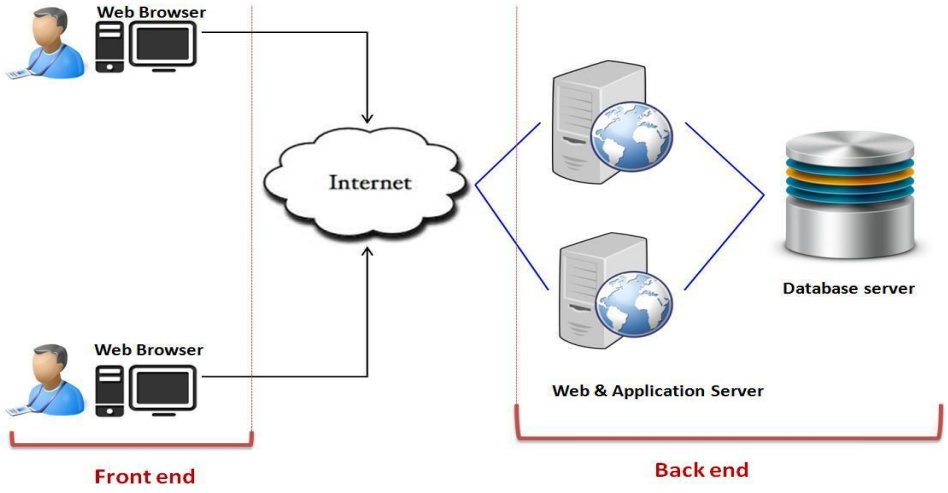

Fig.1. Cloud Architecture for multi user Authentication

Secret sharing [1] is the technique of distribution of secrets among the participants or group members within a group, Each of the participants holds only a share of the secret and individual shares are of no use in order to reconstruct the original secret. The original secret can be reconstructed only when a definite number of shares are combined together and individual shares does not indicate the original secret.

II. LITERATURE REVIEW

Nikhitha K Nair, Navin K S. [2] proposed that group authentication emphasis on communication between the members of a group and then authenticates the members. The main purpose of group communication is to share and exchange ideas and messages with different members of the group. The messages are sent to each other in encrypted form to enhance security. The group manager has the responsibility of overall control over the group. A group key is there for each group which generates the session keys which are used by the group members to share the secret messages.

In the paper [3], Lein Harn and Jian Ren proposed that Public-key digital certificate has been widely used in public-key infrastructure (PKI) to provide user public key authentication. However, the public-key digital certicate itself cannot be used as a security factor to authenticate user. In this paper, we propose the concept of generalized digital certificate (GDC) that can be used to provide user authentication and key agreement. A GDC contains users public information, such as the information of users digital drivers license, the information of a digital birth certificate, etc., and a digital signature of the public information signed by a trusted certificate authority (CA). However, the GDC does not contain any user's public key. Since the user does not have any private and public key pair, key management in using GDC is much simpler than using public-key digital certificate. The digital signature of the GDC is used as a secret token of each user that will never be revealed to any verifier. Instead, the owner proves to the verifier that he has the knowledge of the signature by responding to the verifier challenge. Based on this concept, we propose both discrete logarithm (DL)-based and integer factoring (IF)-based protocols that can achieve user authentication and secret key establishment.

In the paper [4], Mrudula Sarvabhatla,M.Giri Chandra, Sekhar Vorugunti proposed that Cloud computing is a collection of virtually massive distributed large scale computers to handle enormous enterprise computing, hardware, storage needs. An exponential advancement of communication and information technologies results in substantial traffic for accessing of cloud resources wired and mobile, through various communication devices like desktop, laptop, abs, etc. via Internet. Significance of enterprise data and increased access rates from low-resource terminal devices demands for reliable and low cost authentication techniques. Lots of researchers have proposed authentication schemes based on password, biometric, steganography etc. with varied efficiencies.

Nimmy K., M. Sethumadhavan [5] proposed that Proper authentication is an essential technology for cloud-computing environments in which connections to external environments are common and risks are high. Here, a new scheme is proposed for mutual authentication where the user and cloud server can authenticate one another. The protocol is designed in such a way that it uses steganography as an additional encryption scheme. The

scheme achieves authentication using secret sharing. Secret sharing allows a part of the secret to be kept in both sides which when combined becomes the complete secret. The secret contains information about both parties involved. Further, out of band authentication has been used which provides additional security. The proposed protocol provides mutual authentication and session key establishment between the users and the cloud server. Also, the users have been given the exibility to change the password. Further-more, strong security features makes the protocol well suited for the cloud environment

In the paper [6], Ching-Nung Yang,Jia-Bin Lai proposed that Cloud computing is an Internet-based computing. Computing services, such as data, storage, software, computing, and application, are delivered to local devices through Internet. The major security issue of cloud computing is that the cloud provider must ensure that their infrastructure is secure, and that prevent illegal data accesses from outsiders, other clients, or even the unauthorized cloud employees. In this paper, authors used Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing, which they called the secure cloud computing (SCC). [6] proposed two types of SCC. One requires a trusted third party (TTP), and the other does not need a TTP. Also, they proposed multi-server SCC (MSCC) to fit an environment as a future scope, where each multi-server system contains multiple servers to collaborate for serving applications. Due to the strong security and operation efficiency, the proposed SCC and MSCC are extremely suitable for use in cloud computing..

In the paper [7], Takahashi, Shiro Kobayashi, Hyunho Kang, Keiichi Iwamur proposed that Secret sharing schemes can be used in cloud computing to allow many participants to distribute multiple data. However, the application of (k, n) secret sharing to cloud systems causes a large increase in storage capacity, making it unsuitable for systems with many secrets to distribute. Authors proposed a computationally secure ramp secret sharing. The proposed scheme is secure and space efficient as created shares are of small size.

These all papers are using different techniques to secure group authentication. Most of the researchers have proposed secret sharing based multi user authentication to make the system more secure.

The next section compares the above discussed papers in next section.

III. COMPARATIVE ANALYSIS

The papers discussed in section II are compared on various parameters. The below table I, describes these methods on various parameters that are used in the group communication. The most of the approaches used the public cloud for data storage. Each concept basically states the group communication in a secured way by allowing the proxy signature technique in some methods. The table also states the basic principal used for a group communication. The comparison is done on various parameters like technique used, security, time complexity, replay attacks, session key agreement, user anonymity, impersonating attack, key exchange.

Table 1. Comparative Analysis of Multi User Authentication in Cloud Computing

Parameters	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**	**[7]**
Technique Used	RSA,Key Generation	Stenography	Shamir's Authentication	cryptography	Secret Sharing	RSA, key management
Key Exchange	Key Exchange take place	No Key Exchange needed	Key Exchange needed hence increase speed	Key Exchange take place	Key Exchange needed hence increase speed	Key Exchange take place
Secure	Moderate Security	High security and easily revocable	High security and easily revocable	Moderate Security	High security and easily revocable	Moderate Security
Time Complexity	O(log n)	O(n)	O(n)	O(log n)	O(n)	O(log n)
Replay Attack	no	no	Yes	no	yes	yes
Session key Agreement	yes	no	NA	yes	NA	yes
Impersonating Attack	no	yes	Yes	no	yes	no
User Anonymity	no	no	Yes	no	yes	no
Identity management	yes	yes	Yes	yes	yes	yes

IV. CONCLUSION

Group authentication can authenticate multiple users at once. This paper analyses group authentication techniques for cloud based applications. The comparison is done on various parameters like technique used, security, time complexity, replay attacks, session key agreement, user anonymity, impersonating attack, key exchange. The comparative study shows that the technique based on secret sharing is more secure and useful for group authentication. The multifarious secret sharing [8] opens a new research direction for the group authentication in cloud environment.

REFERENCES

[1]. Sonali Patil et. al., "Secret Sharing Schemes for Secure Biometric Authentication", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013
[2]. Nikhitha K. Nair and K. S. Navin, An efficient group authentication mechanism supporting key confidentiality, key freshness and key authentication in cloud computing, IEEE Transactions on Computers, 2015.
[3]. Mrudula Sarvabhatla, M. Giri, Chandra Sekhar Vorugunti, A Secure Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography IEEE Transactions on Computers, 2014
[4]. Lein Ham, "Group Authentication", IEEE Transactions on Computers, vol.62, no. 9, 2013
[5]. Xuejiao Liu1, Yingjie Xia1, Shasha Jiang1, Fubiao Xia2, Yanbo Wang3, Hierarchical Attribute-based Access Control with Authentication for Outsourced Data in Cloud Computing IEEE Transactions on Computers, 2013
[6]. Ching-Nung Yang, Jia-Bin Lai, Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing IEEE Transactions on Computers, 2013
[7]. L. Harn and J. Ren, "Generalized Digital Certi_cate for User Authentication and Key Establishment for Secure Communications", IEEE Trans. Wireless Comm., vol. 10, no. 7, pp. 2372-2379, 2011
[8]. Sonali Patil, Prashant Deshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications (0975 – 8887) , Volume 46– No.19, May 2012

Sonali Patil" Securing Multi User Authentication in Cloud Computing Using Secret Sharing" International Journal of Computational Engineering Research (IJCER), vol. 09, no. 1, 2019, pp 13-15