MANTECH Publications

Recent Trends in Computer Science and Software Technology
Volume 4, Issue 3, September-December 2019

Privacy Preserving Authentication Protocol in Shared Authority based on Cloud Computing

Mali Puja[1], Nimbalkar Dhanashri[2], Khot Pranali[3], Chivate Shrishti[4], S. G. Bavachkar[5]

Students[1, 2, 3, 4], Assistant Professor[5]

Department of Computer Science and Engineering

Sanjay Bhokare Group of Institute Engineering Miraj, Maharashtra, India

Corresponding Author's Email: *bavachkarsg@sbgimiraj.org[5]*

Abstract

Cloud computing is emerging as a prevalent data interactive paradigm to realize user's data remotely stored in an online cloud server. Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. But security and privacy issues are becoming key concerns in data sharing among the multiple users in cloud storage. In order to avoid all these things, a system is proposed in which a shared authority based privacy-preserving authentication protocol (SAPA) to solve privacy and security issue for cloud storage.

Keywords: *Cloud Storage, Data de-duplicating, Data Privacy, Authentication*

INTRODUCTION

Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The existing security solutions mainly focus on the authentication to realize that a users privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server

Page 87-94 © MANTECH PUBLICATIONS 2019. All Rights Reserved

to request other users for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions.

Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing. It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be share in a pay-per-use manner.

Despite the tremendous benefits, security is the primary obstacle that prevents the wide adoption of this promising computing model, especially for customers when their confidential data are consumed and produced during the computation to combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing so as to provide end to- end data confidentiality assurance in the cloud and beyond.

However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying cipher text-policy, making the computation over encrypted data a very hard problem.

The proposed scheme not only achieves scalability due to its hierarchical structure. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semi honest model.

RELATED WORK

There are already well-known existing security solutions mainly focus on the authentication to realize that a user's privative data cannot be unauthorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the users privacy.

The existing systems define shared authority based privacy-preserving authentication protocol, which allows security and privacy in the cloud storage. In this, shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations.

Attribute based access control is adopted to realize that the user can only access its

Page 87-94 © MANTECH PUBLICATIONS 2019. All Rights Reserved

own data fields; proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users.

PROPOSED WORK

Users' identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. it seems natural that users are willing to keep their identities secret while they still get their private keys. [1]

Therefore, we propose a system that allows a privacy preserving with Anonymous Attribute-Based Encryption scheme. This will address data privacy and the user identity privacy. This will achieve the full anonymity by preventing the identity leakage.

The proposed scheme will be able to protect user's privacy against each single authority with whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes. Hence, the proposed scheme will be tolerant against authority compromise, and compromising of up to (N −2) authorities does not bring the whole system down.

We will provide detailed analysis on security and performance to show feasibility of the scheme. Shoulder surfing is direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing will be provided within the system with attribute based encryption. In the proposed scheme, de-duplication will be added where the server will store only a single copy of each file, regardless of how many users asked to store that file, depending upon the disk space of cloud servers.

Below Fig.1 shows the system architecture where the model of secure scheme is given. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information.

The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

A Data Owner is the entity who wishes to outsource encrypted data file to the Cloud Servers. The Cloud Server, who is assumed to have adequate storage capacity, does nothing but store them.

Page 87-94 © MANTECH PUBLICATIONS 2019. All Rights Reserved

A. System architecture

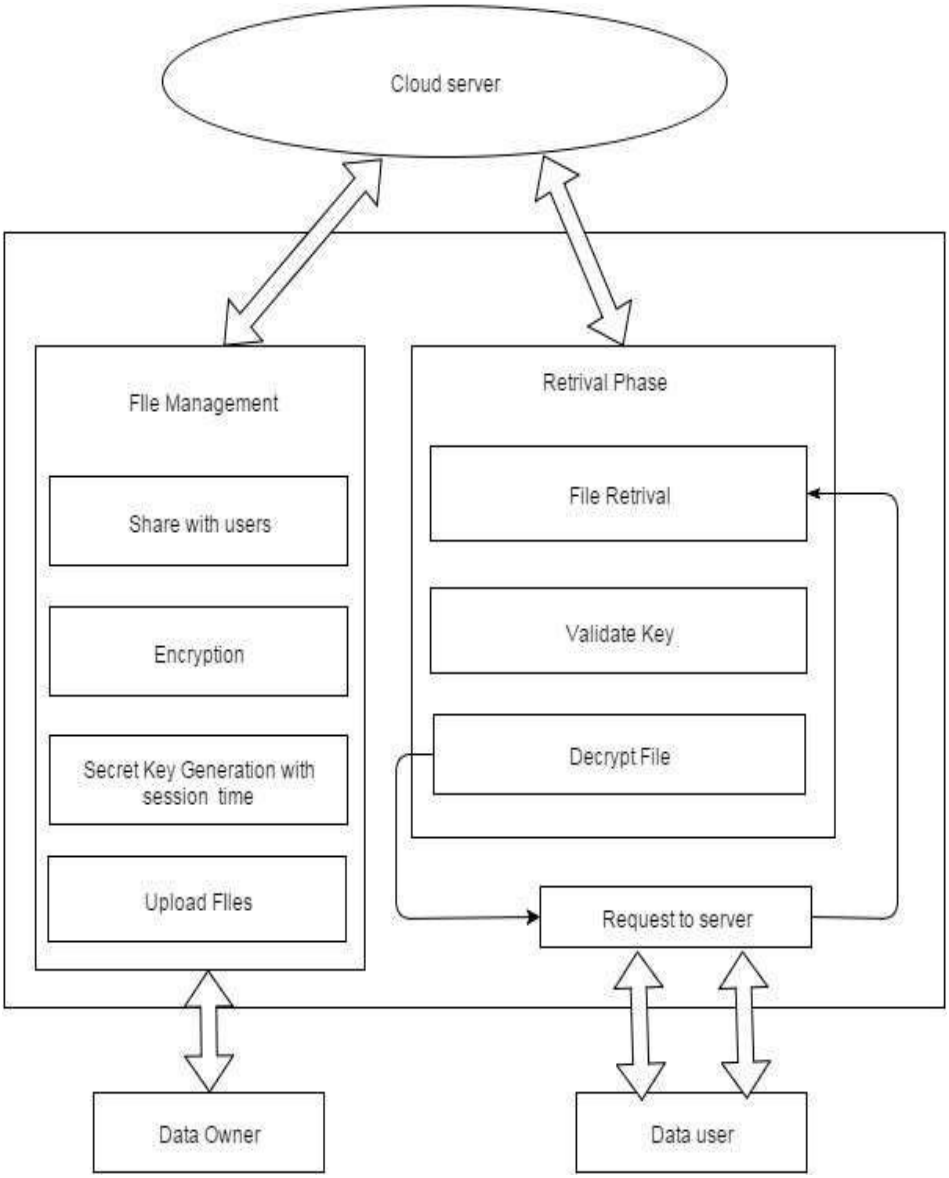


Figure1.System architecture

Data users request private keys from all of the authorities, and they do not know which attributes are controlled by which authorities. When the Data users request their private keys from the authorities, authorities jointly create corresponding private key and send it to them. All Data users are able to download any of the encrypted data files, but only those whose private keys satisfy the privilege tree can execute the operation. The server is delegated to execute an operation if and only if the user's credentials are verified through the privilege tree.

Page 87-94 © MANTECH PUBLICATIONS 2019. All Rights Reserved

MODULES

B. File Management

Encryption algorithm takes as input the public key PK, a message M, and set of privilege trees {Tp}pϵ{0,….,r-1},where r is determined by the encrypter. It will encrypt the message M and returns a ciphertext CT and verification set VR so that the user can execute specific operation on the ciphertext if and if only his attribute satisfy the corresponding privilege tree Tp privilege to read the file.

C. Shoulder Surfing

Shoulder surfing is direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing will be provided within the system with attribute based encryption.

D. Data De-duplication

In the proposed scheme, de-duplication will be added where the server will store only a single copy of each file, regardless of how many users asked to store that file, depending upon the disk space of cloud servers.

E. File Retrieval

In this module, Decryption will be used at file controlling (e.g. reading, modification, and deletion). It takes as input the public key PK, a ciphertext CT, and a private key SKu, which has a set of attributes Au and corresponds to its holder's GIDu. Au satisfies any tree in the set{Tp}pϵ{0,….,r1}, the algorithm returns a message M or a verification parameter.

EXPERIMENTAL SETUP

Operating System: Win7, Windows XP,
Platform : C Sharp.NET
Backend : MS-SQL 2008 SERVER R2

RESULT AND DISCUSSION



Figure: 2 User Login

Page 87-94 © MANTECH PUBLICATIONS 2019. All Rights Reserved



Figure 3.Upload new File

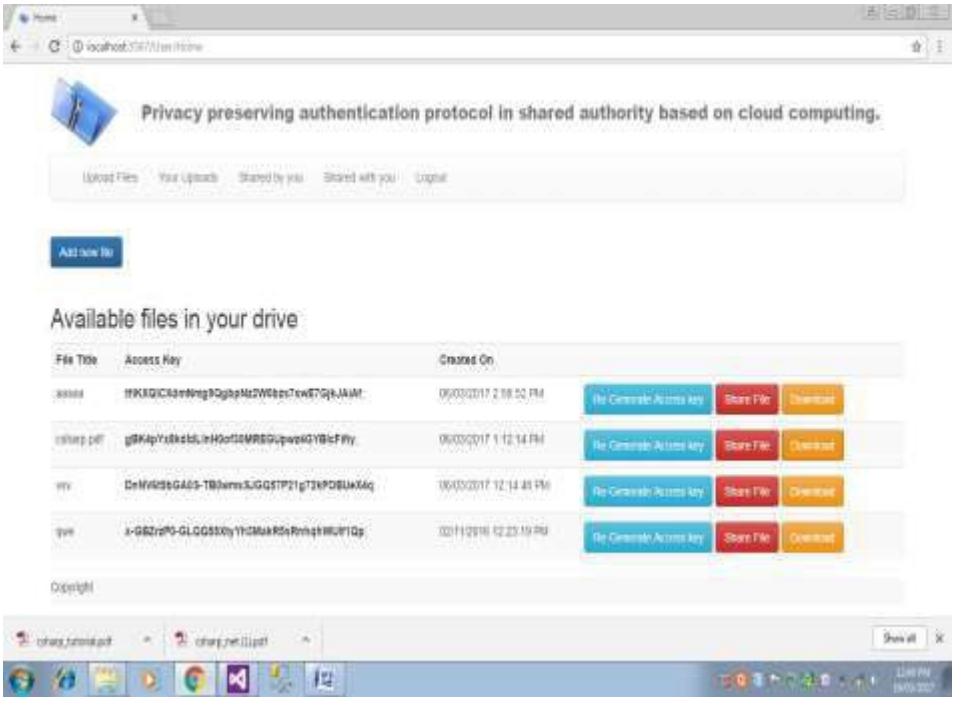


Figure 4. Available files in drive

Page 87-94 © MANTECH PUBLICATIONS 2019. All Rights Reserved

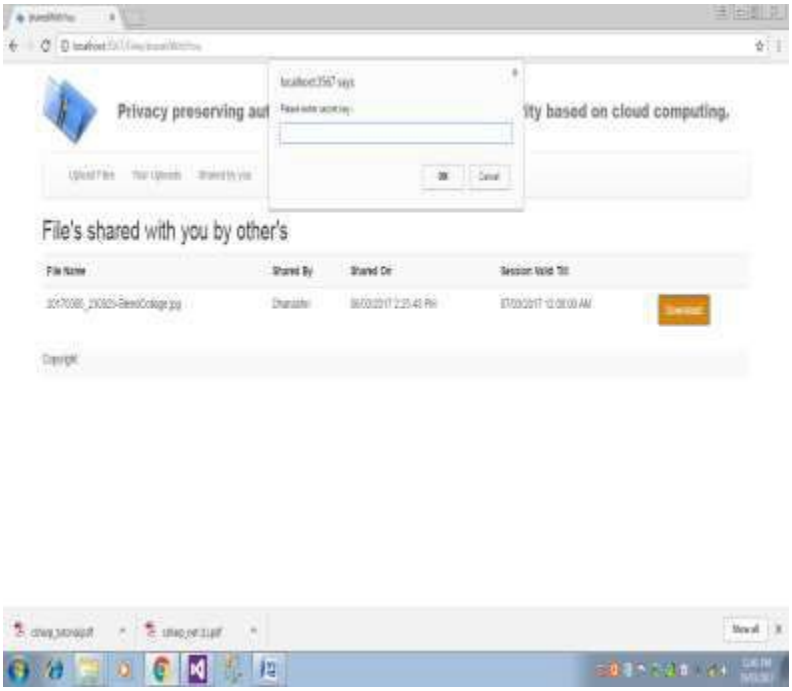


Figure 5.File Shared with you by other user.

CONCLUSION

In this work, we have identified a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users access desires. The session identifiers to prevent the session correlation realize forward security. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

REFERENCES

I. Jingwei Li, Jin Li, DongqingXie and Zhang Cai "Secure Auditing and Deduplicating Data in Cloud", IEEE Transactions on Computers

II. R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services", IEEEInternet Computing, [online] ieeexplore 2012.

III. P. Mell and T. Grance, Draft NIST Working De_nition of Cloud Computing, National Institute of Standards and Technology, USA, 2009.

Page 87-94 © MANTECH PUBLICATIONS 2019. All Rights Reserved

IV. A. Mishra, R. Jain, and A. Durresi, Cloud Computing: Networking and Communication Challenges, IEEE Communications Magazine, vol. 50, no.9, pp, 24-25, 2012.

V. K. Hwang and D. Li, Trusted Cloud Computing with Secure Resources and Data Coloring, IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, 2010.

VI. J. Chen, Y. Wang, and X. Wang, On-Demand Security Architecture for Cloud Computing, Computer, vol. 45, no. 7, pp. 73-78, 2012.

VII. Y. Zhu, H. Hu, G. Ahn, and M. Yu, Cooperative Provable Data Possession for Integrity Veri_cation in Multi-cloud Storage, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.

Page 87-94 © MANTECH PUBLICATIONS 2019. All Rights Reserved