International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Privacy-Preserving in Cloud Computing Using Single Sign-On

S.Kiruthika[1], P.sathiya priya[2]

[1]S.Kiruthika, PG Scholar, Dept. of computer science,
SINCET, Nagapattinam, Tamil Nadu, India.
[2]P.Sathiya priya, Assistant Professor, Dept. of computer science
SINCET, Nagapattinam, Tamil Nadu, India.

Abstract *- Cloud computing is emerging as a prevalent data interactive paradigm to realize multiple users data remotely stored in an online cloud server. The solutions mainly focus on the authentication to realize that a user's privative data cannot be un authorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. This shared authority based directory services authentication protocol (SAPA) to address above privacy issue for cloud storage. Shared access authority is achieved by LDAP authentication for create many directory services. Attribute based access control is adopted to realize that the user can only access its own data fields. AE Attribute encryption is applied by the cloud server to store and retrieve data, and to provide data sharing among the multiple users. universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol realizing privacy-preserving data access authority sharing is attractive for multi-user collaborative cloud applications. Single sign-on concept used to signin same time in multiple directory.*

Key Words**: SAPA, Universal Composability, privacy preserving, Attribute encryption, single sign on.**

1.INTRODUCTION

cloud storage architecture will have a collection of storage servers with higher end configuration which will provides long-term storage services over the Internet and also for the cloud storage system. Here storing and retrieving the data in a third party's cloud system and public auditing scheme causes serious problems and conflict over data confidentiality during the data transactions. Whenever third party big data storage will involve with the cloud server this conflict will occur naturally. Even thou there are various methods are available to overcome this problem like cryptography, key encryption and etc. But general encryption schemes protect data confidentiality during the transaction, but along with this process the main drawback will, it limits the functionality of the storage system. These methods will cause failure. In order to constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. We proposes a secured threshold proxy re-encryption server and integrates it with a decentralized erasure code such that a secure distributed storage system is formulated for processing the data. In this method multiple users can interact with the storage system. The main technical contribution is that the proxy re-encryption scheme supports encoding operations along with a key over encrypted messages, as well as forwarding operations over encoded and encrypted messages. The content in the database will be in the decrypted format. So that even intruder cant able to access the big data even they access the database. The encrypted data will become unused even the data obtained by the intruder. This makes the system so stronger. The storage and robustness are more flexible with the users. So that user will authorize the sender request to generate the key. Using the authorized one time key sender can access the encrypted file in decrypted format at once. The key will become invalid after one use. This is method is implemented for secured data forwarding. During data forwarding a proxy server will be created virtually to access the encrypted data from the sender side. The original data from the cloud server will be transmitted to the proxy virtually. After the transaction the proxy server will be deleted along with the data. So that data will be safe always in the cloud storage servers.

2. LITERATURE SURVEY

AijunGe, et al., [1] exposed a decentralized attribute based encryption system, any party can act as an authority by creating a public key and issuing private keys to different users that reflect their attributes without any collaborative computation in the setup phase of multi authority ABE schemes, thus is considered more preferable. A challenging open problem to construct a decentralized privacy-preserving multi authority ABE scheme in the standard model.

Gurav.Y.B, et al., [2] Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption described Personal health record (PHR) is an emerging patient-centric model of health information

exchange, which is often outsourced to be stored at a third party, such as cloud providers. issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine grained, cryptographically enforced data access control.

Hongwei Li, et al., [3] Identity-based authentication for cloud computing cloud computing is a recently developed new technology for complex systems with massive-scale services sharing among numerous users. Therefore, authentication of both users and services is a significant issue for the trusted and security of the cloud computing. SSL Authentication Protocol(SAP),once applied in cloud computing, will become so complicated that users will undergo a heavily loaded point both in computation and communication. This paper, based on the identity based hierarchical model for cloud computing (IBHMCC) and its corresponding encryption and signature schemes.

Melissa Chase, et al., [4] Improving privacy and security in multi-authority attribute-based encryption It gave a multi-authority ABE scheme using the concepts of a trusted central authority(CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially un trusted authorities.

Ming Li et al., [5] defines Personal Health Record(PHR) has emerged as a patient-centric model of health information exchange, which features storing PHRs electronically in one centralized place, such as a third-party cloud service provider. Although this greatly facilitates the management and sharing of patients personal health information(PHI),there have been serious privacy concerns about whether these service providers can be fully trusted in handling patients sensitive personal health information. However, key functionalities of a PHR service such as keyword searches by multiple users become especially challenging with PHRs stored in encrypted form. The problem of Authorized Private Searches(APS) over encrypted PHRs in cloud computing, where multiple PHR owners encrypt their health records along with a keyword index to allow searches by multiple users in the public domain.

S. Sandareswaran et al., [6] proposed highly decentralized answerability framework to keep track of the actual usage of the user's data in the cloud. The Cloud Information Accountability framework proposed in this work conducts automated logging and distributed auditing of relevant access performed by any entity, carried out at any point of time at any cloud service provider. It has two major elements: logger and log harmonizer. The proposed methodology will also take concern of the JAR file by converting the JAR into obfuscated code which will adds an additional layer of security to the infrastructure. Apart from that we are going to increase the security of user's data by provable data possessions for integrity verification. Handling can be outsourced by the direct Cloud Service Provider(CSP) to other entities in the cloud and theses entities can also delegate the task to other and so on.

3. SYSTEM ANALYSIS

3.1 Existing System

Anonymous request matching method that provide security access in cloud using shared based authentication In address the aforementioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.

3.1.1 Drawback Of Existing System

Previous System does not have the option of granting/revoking data access SAPA does not provide any privacy for private data then Authentication time takes too long.

3.2 Proposed System Analysis

Apply cipher text policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re encryption to provide temp authorized data sharing among multiple users. Single sign on process applied to multi domain access in cloud storage.

4. MODULES

1.Owner module

2.Cloud Server Module

3.Attribute Based Access Policy Module

4.Data Consumer Module

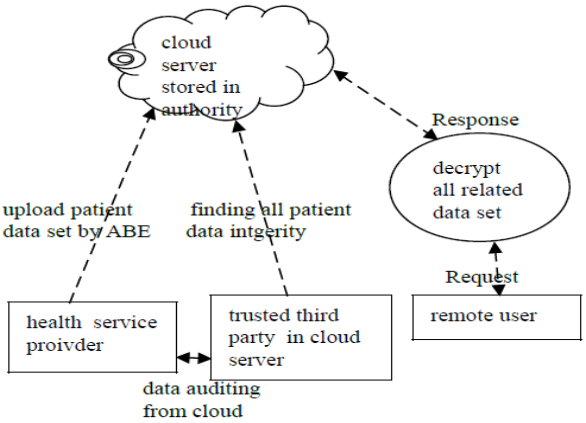

Fig -1: Architecture

4.1 Owner Module

The data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file. The main goal of our framework is to provide secure patient-centric BR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner and they make accesses to BRs based on access rights assigned by the owner.

4.2 Cloud Server Module

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. consider the server to be semi-trusted . That means the server will try to find out as much secret information in the stored BR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits.

4.3 Attribute Based Access Policy Module

The owners upload ABE-encrypted BR files to the server. Each owner's BR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the BR files, excluding the server. In our framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition, two ABE systems are involved. We term the users having read and write access as data readers and contributors, respectively.

Cipher text-Policy Attribute-base Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage. In almost all existing CP-ABE schemes, it is assumed that there is only one authority in the system responsible for issuing attributes to the users. However, in many applications, there are multiple authorities co-exist in a system and each authority is able to issue attributes independently.

4.4 Data Consumer Module

Module user status is revoked to earlier state, when t is disabled by human error or misused by others. User revocation is processed in two stages. In first step, disabled/ noted user will get message about its authentication fail on allowed trines. User has to verify their identity to prove the uniqueness. Once the identity is confirmed new access code or secret key will be send by data owner from the server.

5. TECHNIQUES

5.1 Light Weight Directory Access Protocol

LDAP is mostly used by medium to large organizations. If you belong to one that has an LDAP server. LDAP not limited to contact information or even information about people. LDAP is appropriate for any kind of directory for kind of directory like information. LDAP server exist at three levels there a big public server, large organizational servers at universities and corporations and smaller LDAP work groups.

5.2 Single Sign on

Single sign-on is something of a holy grail for large organizations. Everyone seems to want it, many people claim to have it for sale, but no one seems to agree as to exactly. To many single sign on means that each user in the enterprise has only one user id and associated password. To others, single sign-on means that wherever a user logs in, he is presented with an interface and application set that is specifically tailored to him and which follows him throughout the enterprise. Another interpretation, favored by that single sign-on is the goal of presenting the end user with only one authentication challenge during a single work session.

6 CONCLUSION

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 user's access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

7 FUTURE WORK

Apply cipher text policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re encryption to provide temp authorized data sharing among multiple users. Single sign on process applied to multi domain access in cloud storage.

REFERENCES

[1] AijunGe,Jiang Zhang (2012)"Proposed security analysisof a privacy preserving decentralized key policy abescheme "IEEETrans .ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=642538

[2] Gurav.Y.B,ManjiriDeshmukh,(2013) "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption" IEEE trans , jan vol. 24, no. 1, j

[3] Hongwei Li1, Yuanshun Dai1,2, Ling Tian1, "Identity-based authentication for cloud computing "in *Proc*. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun.2010, pp. 253–262

[4] Melissa Chase Microsoft Research1 Microsoft Way Redmond, WA 98052, USA m sa c@microsoft.com "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption "

[5] Ming Li,Shucheng Yu (2013)" Authorized private keyword search over encrypted phrin cloud computing"IEEETrans,vol. 22, no. 5, pp. 847-859.

[6] S Sankareswari, S.Hemanth (2014)"Attribute based encryption with privacy preserving using asymmetric key in cloud computing""IEEE Int. conf Computer Vol.5(5), 6792-6795

[7] S. Sundareswaran, A. C. Squicciarini, and D. Lin, (2012)"Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Trans.vol. 9, no.4, pp.556-568,

[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li,(2011) "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans,vol. 22, no.5, pp. 847-859, 2011

[9] Wang.C, Q. Wang, K." Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[10] Y. Zheng(2013) "Privacy preserving phr system usingabe" iEE INFOCOM' *13*,Turin, Italy, Apr. , pp. 2625–263.