e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Privacy-Preserving Authentication through proxy re-encryption method in Cloud Computing

Dhivyabharathi.S[1], Mr.T.K.P.Rajagopal[2]
[1]*Computer Science and Engineering, Kathir College of Engineering,dhivya23bharathi@gmail.com*
[2]*Computer Science and Engineering, Kathir College of Engineering, tkprgrg@gmail.com*

Abstract- Cloud computing is emerging as a prevalent data interactive paradigm to realize user's data remotely stored in an online cloud server.. A cloud storage system, consisting of a collection of storage servers, provides long-term storage services over the Internet. Storing data in a third party's cloud system causes serious concern over data confidentiality. Constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. We propose a proxy re-encryption scheme that supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. Our method fully integrates encrypting, encoding, and forwarding. We analyze and suggest suitable parameters for the number of copies of a message dispatched to storage servers and the number of storage servers queried by a key server.

Keywords-Cloud Computing, authentication protocol, privacy preservation, shared authority, re-encryption, Cipher text policy, Data anonymity, Forward Security.

I. INTRODUCTION

CLOUD computing is a promising information technology architecture for both enterprises and individuals. It launches an attractive data storage and interactive paradigm with obvious advantages, including on-demand self-services, ubiquitous network access, and location independent resource pooling . Towards the cloud computing, a typical service architecture is anything as a service (XaaS), in which infrastructures, platform, software, and others are applied for ubiquitous interconnections. Recent studies have been worked to promote the cloud computing evolve towards the internet of services. Subsequently, security and privacy issues are becoming key concerns with the increasing popularity of cloud services. Conventional security approaches mainly focus on the strong authentication to realize that a user can remotely access its own data in on-demand mode. Along with the diversity of the application requirements, users may want to access and share each other's authorized data fields to achieve pro- ductive benefits, which brings new security and privacy challenges for the cloud storage.

In the cloud storage based supply chain management, there are various interest groups (e.g., supplier, carrier, and retailer) in the system. Each group owns its users which are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from diverse groups should access different data fields of the same file. There into, a supplier purposely may want to access a carrier's data fields, but it is not sure whether the carrier will allow its access request. If the carrier refuses its request, the supplier's access desire will be revealed along with nothing obtained towards the desired data fields. Actually, the supplier may not send the access request or withdraw the unaccepted request in advance if it firmly knows that its request will be refused by the carrier. It is unreasonable to thoroughly disclose the supplier's private information without any privacy considerations.

Case 1: The carrier also wants to access the supplier's data fields, and the cloud server should inform each other and transmit the shared access authority to the both users.

Case 2: The carrier has no interest on other users' data fields, therefore its authorized data fields should be properly protected, mean while the supplier's access request will also be concealed.
Case 3: The carrier may want to access the retailer's data fields, but it is not certain whether the retailer will accept its request or not. The retailer's authorized data fields should not be public if the retailer has no interests in the carrier's data fields, and the carrier's request is also privately hidden. Towards above three cases, security protection and privacy preservation are both considered without revealing sensitive access desire related information

In the cloud environments, a reasonable security protocol should achieve the following requirements.
Authentication: a legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.
Data anonymity: any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.
User privacy: any irrelevant entity cannot know or guess a user's ac-cess desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.
Forward security: any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages

In this paper, we address the aforementioned privacy issue to propose a proxy based privacy-preserving authentication protocol for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. The main contributions are as follows.

- 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.
- Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.
- 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.

II. SYSTEM MODEL

Fig.1 illustrates a system model for the cloud storage architecture, which includes three main network entities: users (U_x), a cloud server (S), and a trusted third party.

- *User:* an individual or group entity, which owns its data stored in the cloud for online data storage and computing. Different users may be affiliated with a common organization, and are assigned with independent authorities on the certain data field.

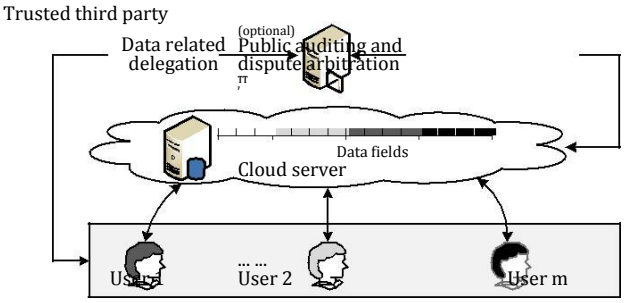

Fig. 1. The cloud storage system model

➢ *Cloud server:* an entity, which is managed by a particular cloud service provider or cloud application operator to provide data storage and computing services. The cloud server is regarded as an entity with unrestricted storage and computational resources.

➢ *Trusted third party:* an optional and neutral entity, which has advanced capabilities on behalf of the users, to perform data public auditing and dispute arbitration.

In the cloud storage, a user remotely stores its data via online infrastructures, platforms, or software for cloud services, which are operated in the distributed, parallel, and cooperative modes. During cloud data accessing, the user autonomously interacts with the cloud server without external interferences, and is assigned with the full and independent authority on its own data fields. It is necessary to guarantee that the users' outsourced data cannot be unauthorized accessed by other users, and is of critical importance to ensure the private information during the users' data access challenges.

In some scenarios, there are multiple users in a system (e.g., supply chain management), and the users could have different affiliation attributes from different interest groups. In the system model, assume that point-to-point com-munication channels between users and a cloud server are reliable with the protection of secure shell protocol (SSH). The related authentication handshakes are not highlighted in the following protocol presentation.

III. OBJECTIVE

➢ The main objective of this project is to develop a cloud architecture using privacy preservation protocol
➢ Shared authority based data forwarding can be done through proxy server. Using Proxy re encryption method.
➢ To create a cloud storage server for long term storage over the internet
➢ The Storage server will act as a data base server.
➢ Uploaded data stored in the cloud server through proxy re encryption method.
➢ To generate proxy re encryption key for one time data access
➢ A proxy server will be created virtually for one time data access. To create fully integrates encrypting, encoding, and forwarding

IV. GOAL

To create a Shared authority based data forwarding using cloud environment through proxy re encryption method. With virtual proxy server for secured data forwarding from cloud server.

V. CLOUD FORMATION

The public cloud environment is the IaaS/PaaS Infrastructure or Platform as a Service that we rent from Linux (IaaS) or Microsoft (PaaS). Both are enabled for web hosting. Then, your SaaS stack will run under your Internet environment most likely in a virtualized one on your own equipment which would make it private. In this project we specialize in private cloud technology. Here we execute in a cloud environment. If strict security requirements go public or hybrid and if not, try the public or community cloud environment. So that here we are implementing a web services for the output purpose as well as the environment will be shown in actual while hosting the application. So finally SaaS can be fully utilized in cloud environment as IaaS/PaaS. Thus we formed cloud environment.

VI. RELATED WORK

Dunning *et al.* [11] proposed an anonymous ID assign-ment based data sharing algorithm (AIDA) for multiparity oriented cloud and distributed computing systems. In the AIDA, an integer data sharing algorithm is designed on top of secure sum data mining operation, and adopts a variable and unbounded number of iterations for anonymous assignment. Specifically,

Nabeel *et al.* [10] proposed a broadcast group key management (BGKM) to improve the weakness of symmetric key cryptosystem in public clouds, and the BGKM realizes that a user need not utilize public key cryptography, and can dynamically derive the symmetric keys during decryption. Accordingly, attribute based access control mechanism is designed to achieve that a user can decrypt the contents if and only if its identity attributes satisfy the content provider's policies. The fine-grained algorithm applies access control vector (ACV) for assigning secrets to users based on the identity attributes, and allowing the users to derive actual symmetric keys based on their secrets and other public information.

Sundareswaran *et al.* [9] established a decentralized information accountability framework to track the user-s' actual data usage in the cloud, and proposed an object-centered approach to enable enclosing the logging mechanism with the users' data and policies. The Java ARchives (JAR) programmable capability is leveraged to create a dynamic and mobile object, and to ensure that the users' data access will launch authentication. Addi-tionally, distributed auditing mechanisms are also pro-vided to strengthen user's data control, and experiments demonstrate the approach efficiency and effectiveness.

Wang *et al.* [8] proposed a distributed storage integrity auditing mechanism, which introduces the homomorphic token and distributed erasure-coded data to enhance secure and dependable storage services in cloud computing. The scheme allows users to audit the cloud storage with lightweight communication overloads and computation cost, and the auditing result ensures strong cloud storage correctness and fast data error localization. Towards the dynamic cloud data, the scheme supports dynamic outsourced data operations. It indicates that the scheme is resilient against Byzantine failure, malicious data modification attack, and server colluding attacks.

VII. 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. 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 We integrate a newly proposed proxy re-encryption scheme and erasure codes over exponents. The proxy re-encryption scheme supports encoding, forwarding, and partial decryption operations in a distributed way.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2009.
[2] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Net-working and Communication Challenges," *IEEE Communications Magazine*, vol. 50, no. 9, pp, 24-25, 2012.
[3] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services," *IEEE Internet Computing*, [online] ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, 2012.
[4] 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.
[5] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architec-ture for Cloud Computing," *Computer*, vol. 45, no. 7, pp. 73-78, 2012.
[6] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no, 12, pp. 2231-2244, 2012.

[7] H. Wang, "Proxy Provable Data Possession in Public Cloud-s," *IEEE Transactions on Services Computing*, [online] ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.
[8] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE Transactions on Services Computing*, vol. 5, no. 2, pp. 220-232, 2012.
[9] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, [online] ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.
[10] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Pol-icy Based Content Sharing in Public Clouds," *IEEE Trans-actions on Knowledge and Data Engineering*, [online] ieeex-plore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, 2012.
[11] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," *IEEE Transactions on Informa-tion Forensics and Security*, vol. 8, no. 2, pp. 402-413, 2013.

