Privacy Preserving in Cloud Computing by using Attribute Based Encryption

Dr. A Nirmal Kumar
Associate Professor
Christian College of Engineering and Technology
Oddanchatram, Dindigul

Jerin Mathew
Student
Christian College of Engineering and Technology
Oddanchatram, Dindigul

Lipin Varghese
Student
Christian College of Engineering and Technology
Oddanchatram, Dindigul

Prince Danial Philipose
Student
Christian College of Engineering and Technology
Oddanchatram, Dindigul

Abstract

Cloud computing provides the facility to access shared resources and common support which contributes services on-demand over the network to perform operations that meet changing business needs. A cloud storage system, consisting of a collection of storage servers, provides long-term storage services over the internet. Storing the data in a third party cloud system keeps serious concern over data confidentiality, without considering the local infrastructure limitations, the cloud services allow the user to enjoy the cloud applications. As the different users are working in the collaborative relationship, the data sharing becomes significant to achieve productive benefit during the data accessing. 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 productive benefits.

Keywords: Cloud computing, authentication protocol, privacy preservation, shared authority, universal composability

I. INTRODUCTION

Cloud computing is an emerging technology. It’s a promising information technology architecture for the enterprises and individuals. It launches an attractive data storage and interactive paradigm with obvious advantages, including on-demand self-services, secure network access, and location independent resource pooling. The cloud environment exists as a large open distributed system. Hence data preservation and user privacy is an important concern without considering the local infrastructure limitations. The cloud services allow the user to enjoy the on-demand cloud applications. Subsequently, data security and user 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 only its own data fields in on-demand mode. Along with the diversity of the application requirements, the users may want to access and share other users authorized data fields to achieve maximum productive benefits.

Research in cloud computing is receiving a great support and attention from each educational and industrial world. In cloud computing, users will source their compute and stores to servers (also called clouds) exploitation web. This helps users from the issue of maintaining their resources on-site. Clouds provides many varieties of services, such as infrastructures and platforms assist developers write applications (e.g., Amazon’s S3, Windows Azure). Since services are outsourced to a foreign server, security and privacy are the main concern in cloud. In one side, the user ought to evidence itself before initiating any dealings, and on the opposite side, it should be ensured that the cloud will not tamper with the information that's outsourced with the third party. User privacy is additionally required so the cloud or different users don't make use of the identity of the user.

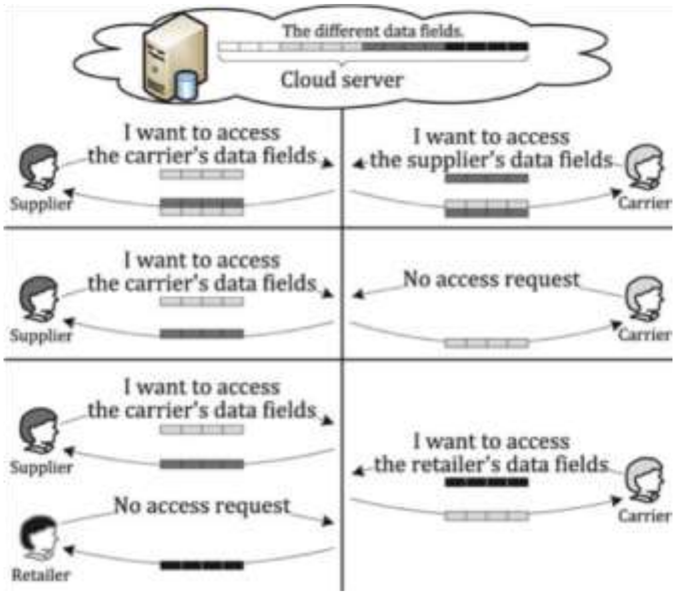
The different data fields.
Cloud server
I want to access the carrier's data fields
I want to access the supplier's data fields
Supplier
Carrier
I want to access the carrier's data fields
No access request
Supplier
Carrier
I want to access the carrier's data fields
Supplier
I want to access the retailer's data fields
Carrier
No access request
Retailer

Fig. 1: Three possible cases during sharing and accessing the data in cloud.

The cloud keeps the user in control of the information it outsources, and likewise, the cloud provides a self-control over the services it provides. It also verifies the validity of the user who stores the information on it. Except for the technical solutions to confirm security and privacy, there's conjointly a necessity for enforcement. Efficient auditing is additionally a very important concern in clouds. In the cloud storage based supply chain management, there are variety of interest groups (e.g., supplier, carrier, and retailer) in the system. Each group owns its users those who are permitted to access the authorized data fields, and different users own relatively independent access authorities. It means that any two users from different groups can access different data fields of the same file. Steve jobs, a supplier 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 rejects 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 rejected by the carrier. It is not possible to access the supplier's private information without any privacy considerations. Fig. 1 illustrates three revised cases to address above described privacy issue.

1) Case 1: The carrier wants to access the supplier's data fields, and the cloud server should inform each other about the access and transmit the shared access authority to the both users, that is both the supplier and carrier is interested to share their data fields.
2) Case 2: The carrier has no interest on other users' data fields, therefore its authorized data fields should be properly protected, so the supplier's access request will also be rejected. Here the carrier is not interested to share the data fields, so SAPA considers it as an unauthorized access and the access will not be permitted.
3) Case 3: The carrier wants to access the retailer's data fields, but it is not sure that 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.

In the above three cases, security, protection and privacy preservation are considered without revealing sensitive access desire related information.

In the cloud environments, a reasonable security protocol must achieve the following requirements

A. 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 unauthorized data fields cannot be accessed by a legal user.

B. Data Anonymity

any unauthorized entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages through an open channel.

C. User Privacy

any unauthorized entity cannot know or guess a user's access desire, which shoes 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**.**

D. *Forward Security*

any adversary cannot correlate two communication sessions to compute the prior interrogations according to the currently captured messages.

In this paper we propose the protocol Shared Authority Based Privacy-Preserving Authentication Protocol(SAPA) to provide security in cloud storage.

1) Identify the privacy challenges in cloud computing, and address a 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.
2) Propose an authentication protocol to enhance the users access-request based privacy.
3) Apply attribute based encryption(ABE) to realize that the user can access its own data fields.

II. Related works

Dunning and Kresman introduced an anonymous ID assignment based data sharing algorithm (AIDA) for multiparty based cloud and distributed computing systems. In the AIDA, an integer data sharing algorithm is designed for securing the data mining operation, and adopts a variable and unbounded number of iterations for anonymous assignment. Specifically, Newton's identities and Sturm's theorem are used for the data mining. A distributed solution of certain polynomials over finite fields to enhance the algorithm scalability, and Markov chain representations are used to specify statistics on the required number of iterations.

Liu et al proposed a multi-owner data sharing secure scheme (Mona) for multiple groups in the cloud applications. The Mona aims to realize that a user can securely share its data with other users through the untrusted cloud server, and can efficiently support dynamic group interactions and communications. In this scheme, a new granted user can directly decrypt data files without the previous contact with data owners, and user revocation is achieved by a revocation list without updating the secret keys of the remaining users. Access control is applied to ensure that any user in a group can illegally utilize the cloud resources, and the data owners' real identities can only be revealed by the group manager for dispute arbitration. This indicates the storage overhead and encryption computation costs are independent with the number of the users.

Grzonkowski and Corcoran introduced a zero knowledge proof (ZKP) based authentication scheme for cloud services. Based on the social home networks, a user oriented approach is applied to enable the sharing of personalized content and sophisticated network-based services through the TCP/IP infrastructures, in which a trusted third party is introduced for decentralized interactions.

Nabeel et al introduced broadcast group key management (BGKM) to make the symmetric key cryptosystem more efficient in public clouds, and the BGKM realizes that a user doesn't needs a public key cryptography, and can dynamically access the symmetric keys during decryption.

Also, attribute based encryption mechanism is introduced 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. The BGKM has an obvious advantage during adding/revoking users and updating access control policies.

In the above mentioned works, various security issues are addressed. But, a user's subtle access request related privacy problem caused by data accessing and data sharing has not been studied yet in the literature. Here, we identified a new privacy challenge, and proposes a protocol not only considering the authentication to realize the valid data accessing, but also focuses authorization to provide the privacy-preserving access authority sharing.

The attribute based encryption and proxy re-encryption mechanisms are jointly applied for authentication and authorization.

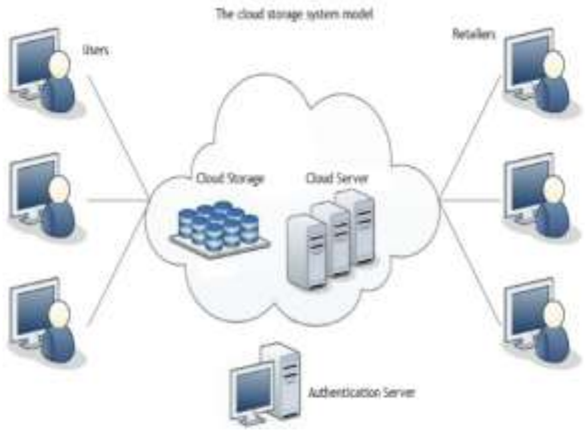

Fig. 2: The cloud storage system model.

A. *User*

A user is an individual or group entity, which owns its data stored in the cloud for online data storage and computing. Different users may be associated with a common organization, and are assigned with independent authorities on certain data fields.

B. *Cloud Server*

It is an entity which is managed by a particular cloud service provider or cloud application operator to provide relevant data storage and computing services. The cloud server is considered as an entity with unrestricted storage and computational resources.

C. *Trusted Third Party*

An optional and neutral entity, which has advanced capabilities to access users for performing data auditing and dispute arbitration. In the cloud storage, a user remotely stores its data through online infrastructures, platforms, or by using a software for cloud services, which are operated in the distributed, parallel, and cooperative modes. During cloud data accessing, the user interacts with the cloud server without external interferences, and is assigned with the full and independent authority on its own data fields. It is a guarantee that the users' outsourced data cannot be illegally accessed by other users, and is of critical importance to ensure the private information during the users' data access challenges. In some cases, there are multiple users in a system (e.g., supply chain management), and the users are having different identity attributes from different interest groups. One of the users may want to access other associated users' data fields to achieve dynamic data sharing, but it considers two aspects: whether the aimed user would like to share its data fields, and how to avoid exposing its access request if the aimed user rejects or ignores its challenge. In this paper, we mainly focus on the process of data access control and access authority sharing other than the specific file oriented cloud data management.

III. THE SHARED AUTHORITY BASED PRIVACY PRESERVING AUTHENTICATION PROTOCOL

A. *Authentication*

The cipher text policy attribute based access control and dynamic pairings are introduced for identification between the User and Server, and only the authorized user can derive the cipher-texts. Additionally, user checks the decrypted ciphertexts based on the proxy re-encryption, which realizes flexible data sharing instead.

B. *Data Anonymity*

The pseudonym are hidden by the hash function so that other entities cannot access the real values by inverse operations. Meanwhile,U~u 's temp authorized fields DU~u are encrypted by kSu for anonymous data transmission. Hence, an adversary cannot recognize the data, even if the adversary intercepts the transmitted data, it will not decode the full-fledged cryptographic algorithms.

C. *User Privacy*

The access request pointer (e.g., RUxUu) is wrapped along with privately informing Server about Uu's access desires. Only if both users are having a mutual interest in each other's data fields, Server will establish the re-encryption key kUu to realize authority sharing between Ua(user A) and Ub(USER B). Otherwise, Server will temporarily reserve the desired access requests for a particular period of time, and exactly cannot determine which user is actively interested in the other user's data fields.

D. *Forward Security*

The dual session identifiers {sidSu ,sidUu } and pseudorandom numbers are introduced as session variational operators to ensure that the communication is dynamic. An adversary regards the prior session as random even if {S, Uu} get corrupted, or the adversary obtains the PRNG algorithm. The current security compromises cannot be correlated with the prior interrogations.

The cloud storage system mainly consists of a server(S) and a user (Ux). Ua and Ub are two users and they are having independent access authorities on their own data fields. This means that the user must have a permission to access particular data fields in the server(s), which means only authorized accesses are allowed. This means that if the user wants to be an authorized user he must be a member of the cloud. SAPA is having the following three conditions.

1) A user can access its own data fields.
2) A user cannot modify other user's data fields.
3) Proxy re-encryption is applied by cloud server to provide data sharing among the multiple users.

SAPA provides security for the users during storing, retrieving and sharing the data. Since SAPA prevents unauthorized access and unauthorized modifications it keeps the user secure. The existing systems mainly focuses on authentication, user security and forward security, it does not provide user privacy. SAPA was introduced to fulfill this disadvantages. SAPA provides user privacy along with the other three.

IV. PROPOSED WORK

Fig. 2 illustrates a system model for the cloud storage architecture. The owner uploads the file in the server and it was in encrypted format. If any user wants the owner file, then user send the request to the server for download. Then the server checks the file attributes and policy. If the requested file attribute and stored file's attributes are matched, it will allow accessing the file. Otherwise, doesn't allow accessing the file.

A. *Admin Login*

The admin is an administrator who administrates the system. The admin login page is mainly to provide the security of the unauthorized access. Without the admins acknowledgement no, one can access the system. Here the admin is used to maintain the users and doctors' details. It also forwards the user details in the cloud.

B. *User Login*

Users are having authentication and security to access the data which are present in the cloud. Before accessing or searching the details user should have the account in that otherwise they should register first. After entering into the cloud, he or/she can access the required file by entering the field. This field is being stored by the admin while uploading the file in the cloud.

C. *Access Control*

Access control is a method to ensure that only authorized user access the data and the system. Very large distributed open systems are developing very rapidly. These systems are like virtual organizations with various autonomous domains. The relationship between users and resources is dynamic and are more ad-hoc in cloud and inter cloud systems. In these systems, users and resource providers does not belong to the same security domain. Users are normally identified by their identity attributes or characteristics and not by predefined identities.

D. *Encryption and Decryption*

Encryption is the process of transforming information so it is insignificant to anyone but the predetermined recipient. Decryption is the process of reconstruct encrypted information so that it is valid again.

E. *File Upload and Download*

In this module admin uploads the file (along with Meta data) into database, with the help of the existing metadata and its contents, the end user can download the file. The downloaded file is in encrypted form, only registered and authorized user can decrypt the file

The user can download the required file from the cloud database. This system also suggests recommends parameters for the number of copies of a message dispatched to the storage servers and the number of storage servers queried by a key server. The parameters mentioned above allow more flexible adjustment between the number of storage servers and robustness. Each individual doctor is given a clear and secured platform for viewing the record details and prescription information.

V. CONCLUSION

In this paper, to achieve maximum privacy and a well secured data sharing and access we identified a new privacy challenge during the data access. Data confidentiality and data integrity is achieved by authentication. During the transmission of data, the wrapped values are exchanged hence data anonymity is achieved. Anonymous access requests enhance the user privacy that privately inform the cloud server about the user access desires. To prevent the session correlation, the session identifiers provides the forward security. This shows that the proposed scheme can be applied for enhancing privacy in cloud applications.

REFERENCES

[1] A. Barsoum and A. Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 12, pp. 2375-2385, http://ieeexplore.ieee.org/stamp/stamp.jsp? tp=&arnumber=6392165, Dec. 2013.
[2] H.Y. Lin and W.G. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 995-1003, June 2012
[3] K.W.Park,J.Han,J.W.Chung,andK.H.Park,"THEMIS:AMutually Verifiable Billing System for the Cloud Computing Environment," IEEETrans.ServicesComputing,vol.6,no.3,pp.300-313,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6133267,JulySept.2013.
[4] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717-1726, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, Sept. 2013.
[5] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Trans. Knowledge and Data Eng., vol. 25, no. 11, pp. 2602-2614..
[6] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," Nat'l Inst. of Standards and Technology, 2009.A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," IEEE Comm. Magazine, vol. 50, no. 9, pp. 24-25, Sept. 2012.
[7] R. Sanchez, F. Almenares, P. Arias, D. Dıaz-Sanchez, and A. Marın, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing," IEEE Trans. Consumer Electronics, vol. 58, no. 1, pp. 95-103, Feb. 2012 =6392165, Dec. 2013.

[8] R. Sanchez, F. Almenares, P. Arias, D. Dıaz-Sanchez, and A. Marın, “Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing,” IEEE Trans. Consumer Electronics, vol. 58, no. 1, pp. 95-103, Feb. 2012.

[9] S. Ruj, M. Stojmenovic, and A. Nayak, “Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds,” IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp. 384-394, http://ieeexplore.ieee.org/stamp/stamp.jsp tp=&arnumber=6463404, Feb. 2014.

[10] X. Liu, Y. Zhang, B. Wang, and J. Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,” IEEE Trans. Paralleland Distributed Systems, vol. 24, no. 6, pp. 1182-1191, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, June 2013.