ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Mutual Authority Using Privacy Preserving and Authentication Protocol in Cloud Computing

Ali Abdulbaqi Abdulazeez
Master of Science (Information System),
Nizam College (Autonomous),O.U,
Basheer Bagh, Hyderabad.

Abstract:

Cloud computing is continuously developing as a standard for sharing the data over the remote storage in an online cloud server. Cloud services offers great amenities for the users to enjoy the on-demand cloud applications without any obligations related to data. During the data retrieving, different users may be in a cooperative relationshipp, and hence data distribution becomes important. Though the user's data is not accessed by unwanted sources, the other's data is exposed to risk by request for sharing The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this paper, we propose mutual authority using privacy preserving and authentication protocol or in other word a shared authority using privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage.

In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security); 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, universal compos ability (UC) model is established to prove that the mutual authority using privacy preserving and authentication protocol 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.

Index Terms:

Cloud computing, authentication protocol, privacy preservation, shared authority.

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 [1]. 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 [2], [3]. 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, which brings new security and privacy challenges for the cloud storage. An example is introduced to identify the main motivation. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

Three revised cases to address above imperceptible privacy issue.

• 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, meanwhile 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 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.

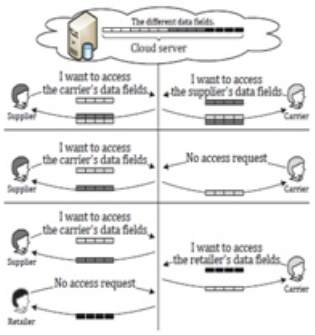

Fig:- Three possible cases in cloud computing

1) 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.

2) Data anonymity:

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

3) User privacy:

any irrelevant entity cannot know or guess a user's access 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.

4) Forward security:

any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages. Researchers have been worked to strengthen security protection and privacy preservation in cloud applications, and there are various cryptographic algorithms to address potential security and privacy problems, including security architectures [4], [5], data possession protocols[6], [7], data public auditing protocols [8]–[10], secure data storage and data sharing protocols [11]–[16], access control mechanisms [17]–[19], privacy preserving protocols[20]–[23], and key management [24]–[27]. However most previous researches focus on the authentication to realize that only a legal user can access its authorized data, which ignores the case that different users may want to access and share each other's authorized data fields to achieve productive benefits. When a user challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this work, we aim to address a user's sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation. In this paper, we 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.

The main contributions are as follows:

1) Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a userchallenging 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 a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.

3) 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. The remainder of the paper is organized as follows. Section 2 introduces related works. Section 3 introduces the system model, and Section 4 presents the proposed authentication protocol.

LITERATURE SURVEY:

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy in company strength. Once these things are satisfied, then next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites

"Privacy Preserving Data Sharing with Anonymous ID Assignment,":

We proposed an anonymous ID assignment based data sharing algorithm (AIDA) for multiparty 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, Newton's identities and Sturm's theorem are used for the data mining, a distributed solution of certain polynomials over finite fields enhances the algorithm scalability, and Markov chain representations are used to determine statistics on the required number of iterations.

"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud":

We consider a multi-owner data sharing secure scheme (Mona) for dynamic groups in the cloud applications. The Mona aims to realize that a user can securely share its data with other users via the untrusted cloud server, and can efficiently support dynamic group interactions. In the scheme, a new granted user can directly decrypt data files without pre-contacting 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 anonymously utilize the cloud resources, and the data owners' real identities can only be revealed by the group manager for dispute arbitration. It indicates the storage overhead and encryption computation costar independent with the amount of the users.

"Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking,":

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

"Privacy Preserving Policy Based Content Sharing in Public Clouds":

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We 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.

Problem Statement:

The 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 expose the user's privacy no matter whether or not it can obtain the data access permissions. Existing data reduplication systems, the cloud is occupied as a different to allow data owner/ users to securely perform duplicate check with differential privileges. The data owners only outsource their data storage by utilizing cloud.

Disadvantages:

During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions.

Problem Solution:

In this project, we propose a mutual or shared authority using privacy-preserving and authentication protocol (SAPA) to address a privacy issue for cloud storage. It indicates that the proposed protocol realizing privacy-preserving data access authority sharing is attractive for multi-user collaborative cloud applications.

In reduplication method prevent the unauthorized use of data accessing and create duplicate data on cloud the encryption technique to encrypt the data before stored on cloud server. In using advanced deduplication system supporting authorized duplicate check. In this new deduplication system, a hybrid cloud architecture is introduced to solve the problem.

Advantages:

1) Shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security);

2) Attribute based access control is adopted to realize that the user can only access its own data fields

3) Proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users.

4) Data deduplication is one of the techniques which used to solve the repetition of data.

5) The deduplication techniques are generally used in the cloud server for reducing the space of the server.

IMPLEMENTATION:

The basic approach implemented on Amazon S3 which is a popular cloud based storage service. The content management consists of two tasks. First, the Owner encrypts the data item sets based on the access control policies and uploads the encrypted sets along with some meta-data.Then, authorized users download the encrypted data items sets and meta-data from the Cloud , and decrypt the data item sets using the secrets they have. Now we illustrate the interactions of the Owner with Amazon S3 as the Cloud . In our implementation, we have used the REST API to communicate with Amazon S3. Figure 2 shows the overall involvement of the Owner in the user and content management process when uploading the data item sets to Amazon S3. While the fine-grained access control is enforced by encrypting using the keys generated through the ABGKM scheme, it is important to limit the access to even the encrypted data item sets in order to minimize the bandwidth utilization.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We associate a hash-based message authentication code (HMAC) with each encrypted data item sets such that only the users having valid identity attributes can produce matching HMACs.Initially the Owner creates a bucket , which is a logical container in S3, to store encrypted data item sets as objects . Subsequently, the Owner executes the following steps:1. The Owner generates the symmetric keys using the AB-GKM's KeyGen algorithm and instantiates an encryption client. Note that the Owner generates a unique symmetric key for each policy configuration .

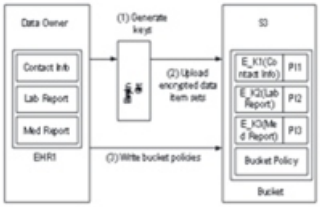

Fig:-Implementation details

Owner:

owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database. In this module, any of the above mentioned person have to login, they should login by giving their emailid and password .

User :

if a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database. If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

Access Control:

Owner can permit access or deny access for accessing the data. So users can able to access his/her account by the corresponding data owner. If owner does not allow, user can't able to get the data.

Encryption & Decryption:

Here we are using this AES_encrypt &AES_decrypt for encryption and decryption. The file we have uploaded which has to be in encrypted form and decrypt it.

File Upload:

In this module Owner uploads the file(along with meta data) into database, with the help of this metadata and its contents, the end user has to download the file. The uploaded file was in encrypted form, only registered user can decrypt it.

File Download:

The Authorized users can download the file from cloud database.

Cloud Service Provider Registration:

In this module , if a cloud service provider(maintainer of cloud) wants to do some cloud offer , they should register first.

Cloud Service Provider Login:

After Cloud provider gets logged in, He/ She can see Cloud provider can view the files uploaded by their clients. Also upload this file into separate Cloud Database.

TTP (Trusted Third Party) Login :

In this module TTP has monitors the data owners file by verifying the data owner's file and stored the file in a database .Also TTP checks the CSP(CLOUD SERVICE PROVIDER),and find out whether theCSP is authorized one or not.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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: Networking and Communication Challenges," IEEECommunications 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] ,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 Architecture 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 Multicloud Storage," IEEETransactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012.

[7] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, 2012 .

[8] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, 2012

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[10] C. Wang, K. Ren, W. Lou, J, Lou,"Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no.4, pp. 19-24, 2010.

[11] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[12] 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, 2012.

[13] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking,"IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, 2011.

[14] M. Nabeel, N. Shang and E. Bertino, "Privacy Preserving Policy Based Content Sharing in Public Clouds," IEEE Transactions on Knowledge and Data Engineering,2011

[15] 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.

[16] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.

[17] Y. Tang, P. C. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 903-916, 2012.

[18] Y. Zhu, H. Hu, G. Ahn, D. Huang, and S. Wang, "Towards Temporal Access Control in Cloud Computing," in Proceedings of the 31stAnnual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012), pp. 2576-2580, March 25-30, 2012.

[19] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds,"IEEE Transactions on Parallel and Distributed Systems, [online] 2013.

[20] R. S´anchez, F. Almenares, P. Arias, D. D´ıaz-S´anchez, and A.Mar´ın, "Enhancing Privacy and Dynamic Federation in IdM forConsumer Cloud Computing," vol. 58, no. 1, pp. 95-103, 2012.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[21] H. Zhuo, S. Zhong, and N. Yu, "A Privacy-Preserving RemoteData Integrity Checking Protocol with Data Dynamics and PublicVerifiability," IEEE Transactions on Knowledge and Data Engineering,vol.23,no. 9, pp.1432-1437, 2011.

AUTHORS BIOGRAPHY:

Ali Abdulbaqi Abdulazeez, pursuing his Master of Science in Information System, from Nizam College (Autonomous),O.U,Basheer Bagh, Hyderabad,India.