International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 2 Issue 3, March 2016 pp. 28 - 33
Scientific Journal Impact Factor : 3.468
http://www.ijcter.com

PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

N.CHITRA[1], S.P. SANTHOSHKUMAR[2], V. BABY VENNILA[3], V. ANURADHA[4]

[1]*UG Scholar, Dept of CSE, Shree Sathyam College of Engineering and Technology,Sankari, India.*
[2]*Assistant Professor, Dept of CSE, Shree Sathyam College of Engineering and Technology,Sankari, India.*
[3]*Associate Professor, Dept of CSE, Shree Sathyam College of Engineering and Technology,Sankari, India.*
[4]*HOD, Dept of CSE, Shree Sathyam College of Engineering and Technology,Sankari, India.*

Abstract—In this system we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity. This Project Mainly Focus To Realize The Authentication For The Data Access on a Demand Mode. New Security And The Privacy Concerns Can Be Performed. AIDA Algorithm Is Used For The Multiparty Oriented Cloud Services. SAPA Protocol for Address the Privacy Issue.

Keywords—AIDA, SAPA**,** metadata, auditing, Cloud server, data sharing

I. INTRODUCTION

Cloud Computing is a Promising Information Technology Architecture for both Enterprises and Individuals. In Cloud Computing, A Typical Service Architecture Is Anything As A Service (Xaas), in Which Infrastructures, Platform, Software, And Others Are Applied For Ubiquitous Interconnections. IDA Algorithm Is Used For The Distributed Computing System. SAPA Protocol To Address The Privacy Issue For The Cloud Storage. An example is introduced to identify the main motivation. Recent studies have been worked to promote the cloud computing evolve towards the internet of services [3], [4].

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 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. Fig. 1 illustrates three revised cases to address above imperceptible privacy issue.

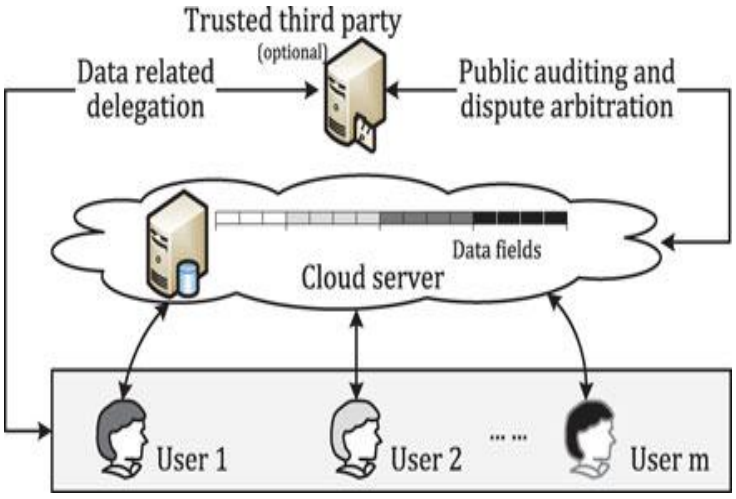

Figure 1:Data accessing and data sharing in cloud applications

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 and 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 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.

The main contributions are as follows.

1. 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.
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.

Many mechanisms have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing. In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. A public verifier could be a data user (e.g. researcher) who would like to utilize the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services.

II. LITERATURE SURVEY

Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing Using the methodology is AIDA. Advantage of this system is Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information. In this paper survey we found the disadvantage is Local infrastructure limitations [Hong Liu,, Qingxu Xiong et al, 2015].

Cloud Computing Networking and Communication Challenges. Here, methodology using in Authority. Advantage of this survey we found less User privacy Small forward security and the disadvantage of Existing security solutions only focus on the authentication [A. Mishra, R. Jain, and A. Durresi et al 2012].

Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds. Here Public Key Infrastructure (PKI methodlogy is used in this survey.In exixting system concept is Local infrastructure limitations. Disadvantage of this paper we found Oruta can preserve data privacy from public verifiers. [A. Barsoum and A. Hasan, et al 2013].

Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds.Methodology used SAPA Protocol.Existing security solutions only focus on the authentication is the advantage in this survey and disadvantage of this survey we found The identity of the signer on each block in shared data is kept private from the public verifier [S. Ruj, M. Stojmenovic, and A. Nayak, et al 2014].

III. SYSTEM MODEL

3.1 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 certain data fields.

3.2 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.

3.3 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, flatforms, 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. One of the users may want to access other associated users' data fields to achieve bi-directional data sharing, but it cares about 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 declines or ignores its challenge. In the paper, we pay more attention on the process of data access control and access authority sharing other than the specific file oriented cloud data management.

Figure 2.The cloud storage system model.

In the system model, assume that point-to-point communication 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.

To solve the above privacy issue on shared data, we propose Oruta, a novel privacy preserving public auditing mechanism.

More specifically, we utilize ring signatures to construct homomorphism authenticators in Oruta, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier.

In addition, we further extend our mechanism to support batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks.

Oruta can preserve data privacy from public verifiers. The identity of the signer on each block in shared data is kept private from the public verifier. With ring signatures, a verifier is convinced that a signature is computed using one of group members' private keys, but the verifier is not able to determine which one.

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, user may want to access and share each others authorized data fields to acheive productive benefits which brings new security and privacy challenges for the cloud storage. Anonymous ID assignment based data sharing algorithm (AIDA) for multiparty oriented cloud and distributed computing systems. Protocol is attractive for multi-user collaborative cloud applications. A shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage.

In summary, the SAPA adopts integrative approaches to address secure authority sharing in cloud applications.

Authentication.

The ciphertext-policy attribute based access control and bilinear pairings are introduced for identification between Uu and S, and only the legal user can derive the ciphertexts. Additionally, Uu checks the re-computed ciphertexts according to the proxy re-encryption, which realizes flexible data sharing instead of publishing the interactive users' secret keys.

Data anonymity.

The pseudonym PIDUu are hidden by the hash function so that other entities cannot derives 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.

User privacy.

The access request pointer (e.g., RUx Uu) is wrapped along with HðsidSukPIDUu Þ for privately informing S about Uu's access desires. Only if both users are interested in each other's data fields, S will establish the re-encryption key kUu to realize authority sharing between Ua and Ub. Otherwise, S will temporarily reserve the desired access requests for a certain period of time, and cannot accurately determine which user is actively interested in the other user's data fields.

Forward security.

The dual session identifiers {sidSu , sidUu } and pseudorandom numbers are introduced as session variational operators to ensure the communications 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 correlate with the prior interrogations.

IV. THE PROPOSED PROTOCOL DESCRIPTIONS

The interactions among {Ua, Ub, S}, in which both Ua and Ub have interests on each other's authorized data fields for data sharing. Note that the presented interactions may not be synchronously launched, and a certain time interval is allowable.

4.1 {Ua, Ub}'s Access Challenges and S's Responses

{Ua, Ub} respectively generate the session identifiers {sidUa , sidUb }, extract the identity tokens {TUa , TUb }, and transmits {sidUakTUa , sidUbkTUa} to S as an access query to initiate a new session. Accordingly, we take the interactions of Ua and S as an example to introduce the following authentication phase.

4.2 {Ua, Ub}'s Data Access Control

Ua first extracts it data attribute access list AUa ¼ ½aij_ (aij 2 f0; 1g, aij _ pij) to re-structure an access list LUa ¼ ½lij_n_m for lij ¼ pij _ aij. Ua also defines a polynomial FUa ðx;LUa Þ according to LUa and TUa :

Ua derives Ub's temp authorized data fields _DUb :

$$\dot{D}_{U_b} = E^{-1}_{k_{\Sigma_a}}\left(M'_{U_b 2} e\left(M'_{U_b 1}, h\right)^{-k_{\Sigma_a}/k_S}\right) \quad (1)$$

V. 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 privacy preservation in cloud applications. We propose a shared authority based privacy-preserving authentication protocol(SAPA) to address above privacy issues for cloud storage.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," Nat'l Inst. of Standards and Technology, 2009.
[2] 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.
[3] R. Moreno-Vozmediano, R.S. Montero, and I.M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services,"IEEEInternet Computing,vol.17,no. 4,pp. 18-25,http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6203493, July/Aug.2013.
[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, Sept./Oct. 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 Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.
[7] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, Oct.-Dec. 2012.
[8] 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.
[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 Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859-25, May 2011.
[10] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[11] L.A. Dunning and R. Kresman, "Privacy Preserving Data Sharing with Anonymous ID Assignment," IEEE Trans. Information Forensics and Security, vol. 8, no. 2, pp. 402-413, Feb. 2013.
[12] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, http:// ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, June 2013.
[13] S. Grzonkowski and P.M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Trans. Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, Aug. 2011.
[14] 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, http://ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6298891, Nov. 2013.
[15] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.
[16] S. Sundareswaran, A.C. Squicciarini, and D. Lin, "Ensur ing Distributed Accountability for Data Sharing in the Cloud," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, July/Aug. 2012.

