INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

Hide me and Authenticate Implementation of Multi party Key Authentication and SAPA Protocol for Secured Data Transaction in Cloud

R. Archana #1, S. Prasanna *1

Mailam Engineering College, Mailam #1, *1

archanaravanan@gmail.com

Abstract - In the Cloud computing is an evolving data communicative design to determine the user data remotely stored in an online cloud server. Security solutions mainly focus on the authentication cannot be illegally accessed, but neglect a subtle privacy issue. In the proposed mechanism, there will be three Entities Users, Cloud Server & Trusted Third Party (TPA). Data Users are both Data Owners & Data Users. Every User will be registering with the Cloud Server. Cloud will be generating Pair wise Keys, Primary & Secondary Keys for both Cloud Server & Data User. Users 1 wants to Access the data of Users 2 then Keys are Shared Keys are generated and accordingly the Data is authorized for Usage. In our modified process, an Access key is generated while Registration with Cloud. After that only Shared Keys are generated. Finally a Mutual Access key is generated by the data owner to the data user and sent via Email. Data User will have to hide that Mutual Key in an Image called Steganography and sent to the Data Owner. Data is accessed by only after Verifying Mutual Key using Destaganography.

Keywords – Cloud, Trusted Third Party, Shared keys, Mutual key

1 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, 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 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

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

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

2 Related Work

In the existing mechanism, security solutions mainly focus on the authentication cannot be illegally accessed, but neglect a subtle privacy issue. Here it provides some drawbacks are, Less Security, Data hacking, missing privacy

2.1 Proposed Mechanism

In the proposed mechanism, there will be three Entities Users, Cloud Server & Trusted Third Party (TPA). Data Users are both Data

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

Owners & Data Users. Every User will be registering with the Cloud Server. Cloud will be generating Pair wise Keys, Primary & Secondary Keys for both Cloud Server & Data User. Users 1 wants to Access the data of Users 2 then Keys are Shared Keys are generated and accordingly the Data is authorized for Usage. In our modified mechanism, an Access key is generated while Registration with Cloud. After that only Shared Keys are generated. Finally a Mutual Access key is generated by the data owner to the data user and sent via Email. Data User will have to hide that Mutual Key in an Image called Steganography and sent to the Data Owner. Data is accessed by only after Verifying Mutual Key using Destaganography. Here it provides some benefits are High security, Data integrity, easily find the attacker.

3 System Design

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. 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. 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, flat forms, 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. 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. Towards the trust model, there

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

are no full trust relationships between a cloud server S and a user U x S is semi-honest and curious. Being semi-honest means that S can be regarded as an entity that appropriately follows the protocol procedure. Being curious means that S may attempt to obtain U's private information (e.g., data content, and user preferences). It means that S is under the supervision of its cloud provider or operator, but may be interested in viewing users' privacy. In the passive or honest-but curious model, S cannot tamper with the users' data to maintain the system normal operation with undetected monitoring x.

4 Literature review

1. **P. Mell and T. Grance, Draft NIST Working Definition of Cloud Computing," Nat'**

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

2. **Moreno-Vozmediano, R., Key Challenges in Cloud Computing: Enabling the Future Internet of Services**

Cloud computing will play a major role in the future Internet of Services, enabling on-demand provisioning of applications, platforms, and computing infrastructures. However, the cloud community must address several technology challenges to turn this vision into reality. Specific issues relate to deploying future infrastructure-as-a-service clouds and include efficiently managing such clouds to deliver scalable and elastic service platforms on demand, developing cloud aggregation architectures and technologies that let cloud providers collaborate and interoperate, and improving cloud infrastructures' security, reliability, and energy efficiency.

3. **Kai Hwang, Trusted Cloud Computing with Secure Resources and Data Coloring**

Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized data center resources, uphold user privacy, and preserve data integrity. The authors suggest using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners. Data coloring and software watermarking techniques protect shared data objects and massively distributed software modules. These techniques safeguard multi-way authentications, enable single sign-on in the cloud, and tighten access control for sensitive data in both public and private clouds.

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

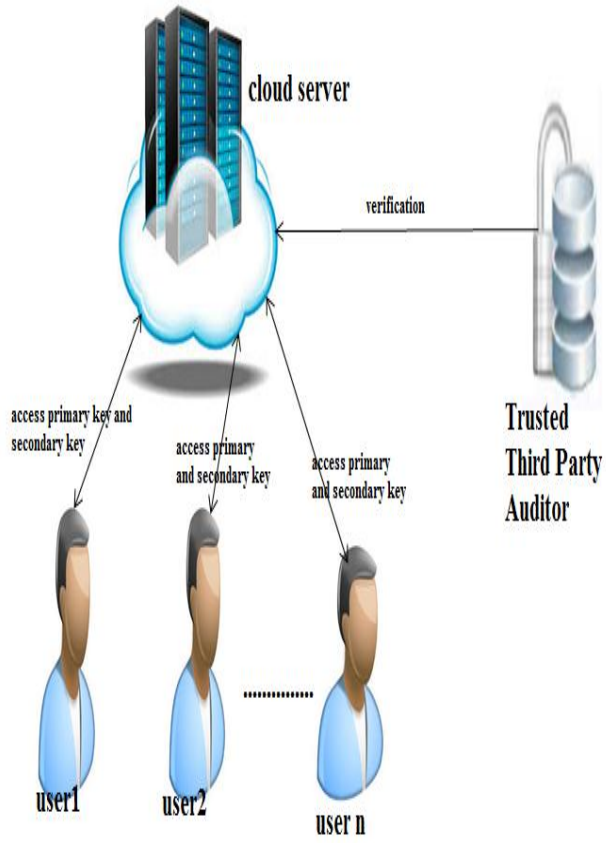
ISSN 2454-9924 Volume: 1 Issue: 1(2015)

4. **Jianyong Chen, On-Demand Security Architecture for Cloud Computing**

An architecture thatdifferentiates security ac cording to service-specific characteristics avoids an unnecessary drain on IT resources by protecting a variety of cloud computing services at just the right level.

5 Architecture Design

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. Towards the trust model, there are no full trust relationships between a cloud server S and a user Ux. S is semi-honest and curious. Being semi-honest means that S can be regarded as an entity that appropriately follows the protocol procedure.



6 Conclusion

From this hide me and Authenticate Implementation of Multi party Key Authentication and SAPA Protocol for Secured Data Transaction in Cloud have been implemented, 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

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

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. In future, we also demonstrate the efficient system performance.

7 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] 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] 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.

[4] 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.

[5] 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.

[6] H. Zhuo, S. Zhong, and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," IEEE Trans. Knowledge and Data Eng., vol. 23, no. 9, pp. 1432-1437, Sept. 2011.

[7] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, no. 7, pp. 73-78, 2012.

[8] 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.

[9] 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.

[10] 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.

[11] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," Nat'l Inst. of Standards and Technology, 2009.

[12] R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," Proc. 42nd IEEE Symp. Foundations of Computer Science (FOCS '01), pp. 136-145, Oct. 2001.

ISSN 2454-9924 Volume: 1 Issue: 1(2015)

[13] 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=&ar number=6203493, July/Aug.2013.

[14] 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.

[15] 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.js p? tp=&arnumber=6463404, Feb. 2014.

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

[17] 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=&ar number=6374615, June 2013.

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

[19] Y. Xiao, C. Lin, Y. Jiang, X. Chu, and F. Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing," Proc. IEEE GLOBECOM '10, Dec.2010.

[20] 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.