SHARED AUTHORITY BASED PRIVACY-PRESERVING AUTHENTICATION PROTOCOL IN CLOUD COMPUTING

S.Poongodi[#1], P.Murugan[*2], Dr.P.Kuppusamy[*3]

[#1]*Research Scholar, Dept. of Computer Science, Gnanamani college of technology,Namakkal, India*
[*2]*Assistant Professor (CSE), Gnanamani college of technology,Namakkal, India*
[*3]*Ph.D.,Head of the Department(CSE), Gnanamani college of technology,Namakkal, India*

Abstract--**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.**

Keywords: Cloud computing, server, text-policy attribute based access control

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

Securing Infrastructure as a Service

The IaaS model lets users lease compute, storage, network, and other resources in a virtualized environment. The user doesn't manage or control the underlying cloud infrastructure but has control over the OS, storage, deployed applications, and possibly certain networking components. Amazon's Elastic Compute Cloud (EC2) is a good example of IaaS. At the cloud infrastructure level, CSPs can enforce network security with intrusion-detection systems (IDSs), firewalls, antivirus programs, distributed denial-of-service (DDoS) defenses, and so on.

Securing Platform as a Service

Cloud platforms are built on top of IaaS with system integration and virtualization middleware support. Such platforms let users deploy user-built software applications onto the cloud infrastructure using provider-supported programming languages and software tools

(such as Java, Python, or .NET). The user doesn't manage the underlying cloud infrastructure. Popular PaaS platforms include the Google App Engine (GAE) or Microsoft Windows Azure. This level requires securing the provisioned VMs, enforcing security compliance, managing potential risk, and establishing trust among all cloud users and providers.

Securing Software as a Service

SaaS employs browser-initiated application software to serve thousands of cloud customers, who make no upfront investment in servers or software licensing. From the provider's perspective, costs are rather low compared with conventional application hosting. SaaS — as heavily pushed by Google, Microsoft, Salesforce.com, and so on — requires that data be protected from loss, distortion, or theft. Transactional security and copyright compliance are designed to protect all intellectual property rights at this level. Data encryption and coloring offer options for upholding data integrity and user privacy.

II. LITERATURE SURVEY

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.

III. EXISTING SYSTEM

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.

Disadvantages of existing system:

- Loss of data's.
- Does not provide any privacy for private data's.
- Authentication time takes too long.

IV. PROPOSED SYSTEM

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.

- 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.

Advantages Of Proposed System:

- 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.
- 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.

V. ARCHITECTURE

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.

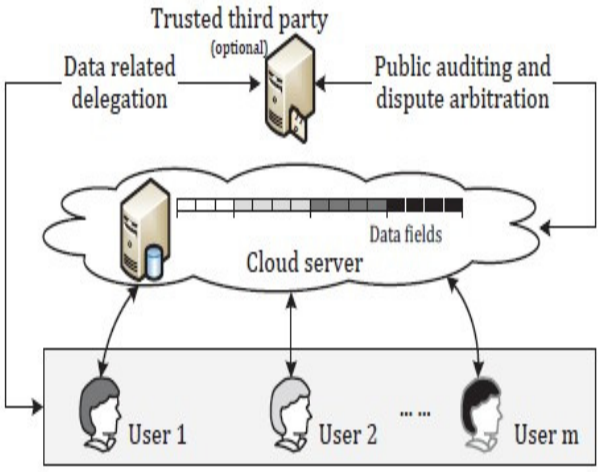

Fig 1: System Architecture

VI. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Implementation is the process of converting a new system design into operation. It is the phase that focuses on user training, site preparation and file conversion for installing a candidate system. The important factor that should be considered here is that the conversion should not disrupt the functioning of the organization.

VII. CONCLUSION AND FUTURE WORK

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.

REFERENCES

[1] K. Hwang, G. Fox, and J. Dongarra, Distributed Systems and Cloud Computing: Clusters, Grids/P2P, and Internet Clouds, Morgan Kaufmann, to appear, 2010.

[2] K. Hwang, S. Kulkarni, and Y. Hu, –Cloud Security with Virtualized Defense and Reputation-Based Trust Management, IEEE Int'l Conf. Dependable, Autonomic, and Secure Computing (DASC 09), IEEE CS Press, 2009.

[3] J. Nick, –Journey to the Private Cloud: Security and Compliance, tech. presentation, EMC, Tsinghua Univ., 25 May 2010.

[4] S. Song et al., –Trusted P2P Transactions with Fuzzy Reputation Aggregation, IEEE Internet Computing, vol. 9, no. 6, 2005, pp. 24–34.

[5] –Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance, Apr. 2009; www. cloudsecurityalliance.org/guidance/csaguide.v2.1.

[6] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009.

[7] J. Rittinghouse and J. Ransome, Cloud Computing: Implementation, Management and Security, CRC Publisher, 2010.

[8] X. Lou and K. Hwang, –Collusive Piracy Prevention in P2P Content Delivery Networks, IEEE Trans. Computers, July 2009, pp. 970–983.

[9] C. Clark et al., –Live Migration of Virtual Machines, Proc. Symp. Networked Systems Design and Implementation, 2005, pp. 273–286.

[10] L. Xiong and L. Liu, –Peer Trust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities, IEEE Trans. Knowledge and Data Eng., July 2004, pp. 843–857.

[11] R. Zhou, and K. Hwang, –Power Trust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing, IEEE Trans. Parallel and Distributed Systems, Apr. 2007, pp. 460–473.

[12] C. Collberg and C. Thomborson, –Watermarking, Tamper-Proofing, and Obfuscation-Tools for Software Protection, IEEE Trans. Software Eng., vol. 28, 2002, pp. 735–746.

[13] D. Li, C. Liu, and W. Gan, –A New Cognitive Model: Cloud Model, Int'l J. Intelligent Systems, Mar. 2009, pp. 357–375.

[14] D. Li and Y. Du, Artificial Intelligence with Uncertainty, Chapman & Hall, 2008.