Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST

Secured Public Integrity Auditing with Key-Exposure Resistance and Shared Dynamic Cloud

Basavaraj Neelagund
Don Bosco Institute of Technology, Bangalore, India
bneelagund@gmail.com

***Abstract*—Cloud storage auditing is one of the important services to verify the integrity of the data present in public cloud. Modern auditing protocols are all based on the conjecture that the client's secret key for auditing is absolutely secure. This benefit in sparing efforts on heavy data maintenance and management. Nevertheless, since the outsourced cloud storage is not fully honourable, it raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing. To provide an efficient public integrity auditing scheme for data on public cloud. We design a concrete scheme based on scheme definition. Our scheme supports the public checking and efficient user revocation and also some polite properties, such as assertively, effectiveness, countability and traceability of secure group user revocation. Finally, the security and experimental analysis shows that, compared with its relevant schemes our scheme is also secure and efficient.**

***Index Terms*— Public integrity auditing, dynamic data, victor commitment, group signature, cloud computing.**

I. INTRODUCTION

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering this collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage. There are numerous ABE schemes that have been proposed. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked, however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant. In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness. Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult. As one example, Lavab it was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to shut down its email service. Since it is difficult to fight against outside coercion, we aimed to build an encryption scheme that could help

Grenze ID: 02.ICCTEST.2017.1.18

cloud storage providers avoid this predicament. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a user's stored ciphertext. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called **deniable encryption**. Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have system wide secrets and must be able to decrypt all encrypted data. In this work, we describe a deniable ABE scheme for cloud storage services. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. Our scheme is based on Waters ciphertext policy-attribute based encryption (CP-ABE). We enhance the Waters scheme from prime order bilinear groups to composite order bilinear groups. By the subgroup decision problem assumption, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

II. LITERATURE SURVEY

A. *Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems*

Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. Ciphertext-policy attribute-based encryption is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data. However, the problem of applying the attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. In this paper, we propose an access control mechanism using cihertext-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. We demonstrate how to apply the proposed mechanism to securely manage the outsourced data. The analysis results indicate that the proposed scheme is efficient and secure in the data outsourcing systems.

B. Role-Based Access Controls

While Mandatory Access Controls (MAC) is appropriate for multilevel secure military applications, Discretionary Access Controls (DAC) is often perceived as meeting the security processing needs of industry and civilian government. This paper argues that reliance on DAC as the principal method of access control is unfounded and inappropriate for many commercial and civilian government organizations. The paper describes a type of non- discretionary access control - role-based access control (RBAC) - that is more central to the secure processing needs of non-military systems then DAC.

C. Secure Provenances: The Essential of Bread and Butter of Data Forensics in Cloud Computing

Secure provenance that records ownership and process history of data objects is vital to the success of data forensics in cloud computing, yet it is still a challenging issue today. In this paper, to tackle this unexplored area in cloud computing, we proposed a new secure provenance scheme based on the bilinear pairing techniques. As the essential bread and butter of data forensics and post investigation in cloud computing, the proposed scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access, and provenance tracking on disputed documents. With the provable security techniques, we formally demonstrate the proposed scheme is secure in the standard model.

D. Trust Cloud: A Framework for Accountability and Trust in Cloud Computing

The key barrier to widespread uptake of cloud computing is the lack of trust in clouds by potential customers. While preventive controls for security and privacy measures are actively being researched, there is still little

focus on detective controls related to cloud accountability and audit ability. The complexity resulting from the sheer amount of virtualization and data distribution carried out in current clouds has also
Revealed an urgent need for research in cloud accountability, as has the shift in focus of customer concerns from server health and utilization to the integrity and safety of end-users' data. This paper discusses key challenges in achieving a trusted cloud through the use of detective controls, and presents the Trust Cloud framework, which addresses accountability in cloud computing via technical and policy-based approaches.

III. IMPLEMENTATION

A. Data Owner

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

B. Cloud Server

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. It is responsible for authorizing all end users.

C. Key Distribution centre

KDC **who** is trusted to store verification parameters and offer public query services for these parameters such as generating secret key based on the file and send to the corresponding end users. It is responsible for capturing the attackers.

D. Data Consumer/End User

In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Data owner and the Data users are controlled by the data owner only. Users may try to access data files either within their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. He is sending request to KDC to generate secret key and KDC will generate the keys and send to corresponding end user.

E. Attacker (Unauthorized User)

Attacker adds the malicious data to a block in cloud server. Then the Unauthorized user will considered as a attacker.

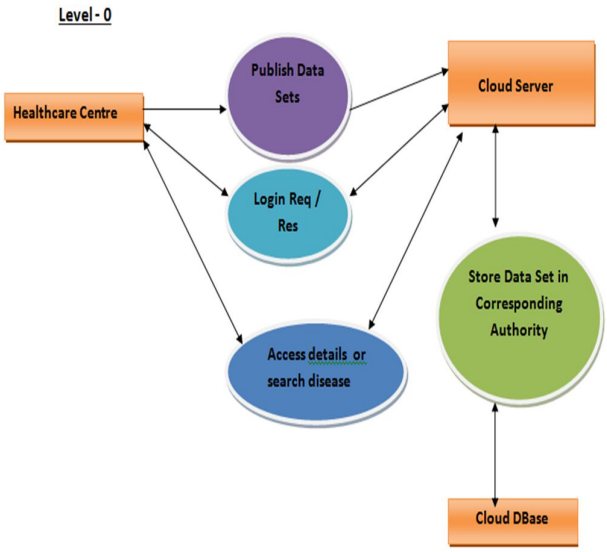

Figure 1. Data Flow Diagram

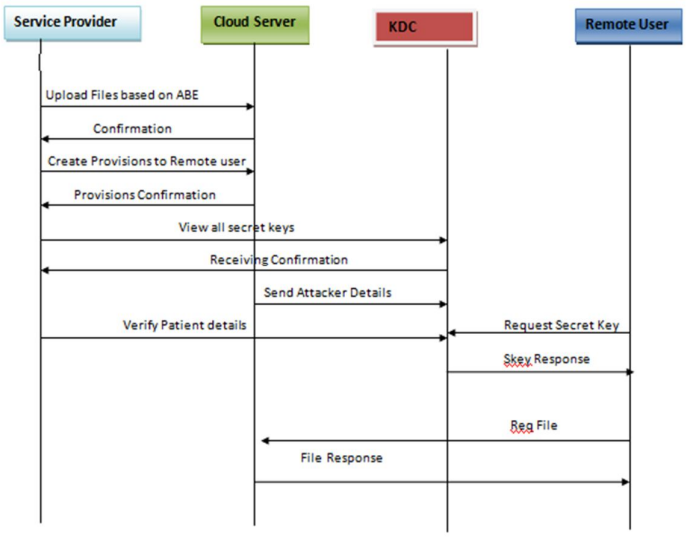

Figure 2. Sequence Diagram

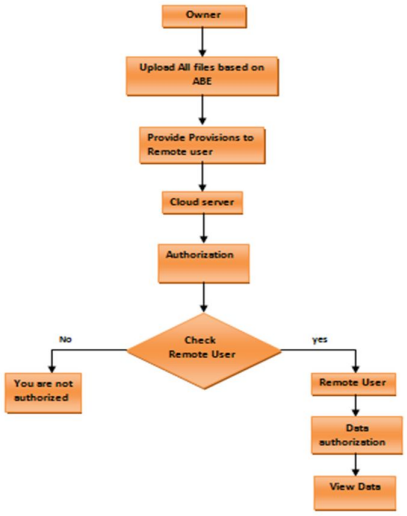

Figure 3. Flow Diagram

IV. Conclusion and Future Enhancement

In this work, we proposed a deniable CP-ABE scheme to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud user privacy.

References

[1] Sahai and B. Waters, "Fuzzy identity-based encryption," in *Eurocrypt*, 2005, pp. 457–473.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM Conference on Computer and Communications Security*, 2006, pp. 89–98.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, 2007, pp. 321–334.
[4] Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography*, 2011, pp. 53–70.
[5] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Crypto*, 2012, pp. 199–217.
[6] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public Key Cryptography*, 2013, pp. 162–179.
[7] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption- based key management for secure and scalable mobile applications in clouds." *IEEE T. Cloud Computing*, pp. 172–186, 2013.
[8] (2014) Edward snowden. [Online]. Available: http://en. wikipedia.org/wiki/Edward Snowden.
[9] (2014) Lavabit. [Online]. Available: http://en.wikipedia. Org/wiki/Lavabit.