“Review On Revocable-Storage Identity-Based Encryption on Cloud Data Security Authentication And Data Sharing”

Monika Ingole , Prof. Nisha Balani , Prof. Amrita Kungwani

Department of CSE , Jhulelal Institute of Technology
Email Id:-monikaingole04@gmail.com,nisha.balani@jit.org.in,a.kungwani@jit.org.in

Abstract

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries[2]. Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics, intelligence and more—over the Internet (“the cloud”) to offer faster innovation, flexible resources and economies of scale. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static. That is, when some user’s authorization is expired, there should be a mechanism that can remove him/her from the system[11]. Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. [11]

Keywords*—Cloud computing, data sharing, revocation, Identity-based encryption, ciphertext update, decryption key exposure.*

1. Introduction

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics, intelligence and more—over the Internet (“the cloud”) to offer faster innovation, flexible resources and economies of scale[2][3]. You typically pay only for cloud services you use, helping lower your operating costs, run your infrastructure more efficiently and scale as your business needs change.Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the societyand individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the dataoften contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data.Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control isnot static. That is, when some user’s authorization is expired, there should be a mechanism that can remove him/her from the system.[8]

Consequently, the revoked user cannot access both the previously and subsequently shared data. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effectivedata-sharing system. Finally, Implementation results of the proposed scheme to demonstrate its practicability. Further we will use cryptography in authentication process so as to authenticated person only could share data.

3. Literature Review

Identity-Based Encryption [1](IBE) offers an interesting alternative to PKI-enabled encryption as it eliminates the need for digital certificates. While revocation has been thoroughly studied in PKIs, few revocation mechanisms are known in the IBE setting. Until quite recently, the most convenient one was to augment identities with period numbers at encryption. All non-revoked receivers were thus forced to obtain a new decryption key at discrete time intervals, which places a significant burden on the authority. A more efficient method was suggested by Boldyreva, Goyal and Kumar at CCS'08. In their revocable IBE scheme, key updates have logarithmic (instead of linear in the original method) complexity for the trusted authority. Unfortunately, security could only be proved in the selective-ID setting where adversaries have to declare which identity will be their prey at the very beginning of the attack game.

[2]Introduction of the notion of certificate-based encryption. In this model, a certificate — or, more generally, a signature — acts not only as a certificate but also as a decryption key. To decrypt a message, a keyholder needs both its secret key and an up-to-date certificate from its CA (or a signature from an authorizer). Certificate-based encryption combines the best aspects of identity-based encryption (implicit certification) and public key encryption (no escrow). We demonstrate how certificate-based encryption can be used to construct an efficient PKI requiring less infrastructure than previous proposals, including Micali's Novomodo, Naor-Nissim and Aiello-Lodha-Ostrovsky.

[3] It is introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. The scheme assumes the existence of trusted key generation centers, whose sole purpose is to give each user a personalized smart card when he first joins the network. The information embedded in this card enables the user to sign and encrypt the messages he sends and to decrypt and verify the messages he receives in a totally independent way, regardless of the identity of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue to function in a completely decentralized way for an indefinite period.

[4] In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this paper, we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. It further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor.[5] **Microsoft Azure** (formerly **Windows Azure** is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. It provides software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) and supports many different programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems. Azure was announced in October 2008, started with codename "Project Red Dog", and released on February 1, 2010, as "Windows Azure" before being renamed "Microsoft Azure" on March 25, 2014.

4. Existing System Drawbacks

Cloud enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. However, it also suffers from several security threats, which are the primary concerns of cloud users.

1] Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information.[5]

2] Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data[11]

5. Conclusion

Cloud computing brings great convenience for people. Particularly,it perfectly matches the increased need of sharingdata over the Internet. A cost-effective and secure data sharing system in cloud computing called RS-IBE, which supports identity revocation and updates cipher text simultaneously such that user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, aconcrete construction of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the standardmodel, under the decisional ℓ-DBHE assumption. The comparison results demonstrate that our scheme has advantagesin terms of efficiency and functionality, and thus is morefeasible for practical applications.

References

1. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.
2. Azure.(2014) Azure service. Available: http://www.windowsazure.com
3. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013
4. iCloud.(2014) Apple storage service. Available: https://www.icloud.com
5. B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013*Proceedings IEEE*. IEEE, 2013
6. Boneh and M. Franklin, "Identity-based encryption from the eil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.
7. S.Micali, "Efficient certificate revocation," Tech. Rep., 1996.
8. D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Advances in Cryptology–CRYPTO 2001*. Springer, 2001, pp. 41–62.
9. C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology–EUROCRYPT 2003*.Springer, 2003, pp. 272–293.
10. B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity based encryption," in Topics in Cryptology–CT-RSA 2009. Springer, 2009, pp. 1–15
11. Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption Jianghong Wei, Wenfen Liu, Xuexian Hu