IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-12, May 2019 E-ISSN: 2347-2693

Cloud Data Security Authentication and Data Sharing Using Revocable-Storage Identity-Based Encryption

Nikita Daudkar[1*], Pranjal Dhore[2], Nisha Balani[3]

[1,2,3]M.Tech, Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, India

Corresponding Author: nikitadaudkar1@gmail.com

Available online at: www.ijcseonline.org

Abstract— Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries. Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. 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. 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. he 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-effective data-sharing system. Finally, we provide 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.

Keywords— Revocable Storage Identity-Based Encryption,Cloud data security, Authentication.

I. INTRODUCTION

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.

CLOUD computing is a paradigm that provides massive computation capacity and huge memory space at a low cost [1]. It 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. Among numerous services provided by cloud computing, cloud storage service, such as Apple's iCloud [2], Microsoft's Azure [3] and Amazon's S3 [4], can offer a more flexible and easy way to share data over the Internet, which provides various benefits for our society [5], [6]. However, it also suffers from several security threats, which are the primary concerns of cloud users [7].
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.

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.

3] 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.

A natural solution to conquer the aforementioned problem is to use cryptographically enforced access control such as identity-based encryption (IBE). Furthermore, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals:

• **Data confidentiality**: Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious,
should also be deterred from knowing plaintext of the shared data.

• **Backward secrecy**: Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented
from accessing the plaintext of the *subsequently* shared data that are still encrypted under his/her identity.

• **Forward secrecy**: Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be
previously accessed by him/her.

II. RELATED WORK

To give satisfactory output of our research we studied following researches.
In This paper we studied the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20 definitions have been studied allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches.

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

In this paper we studied 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.

III. METHODOLOGY

a. **GUI**

- **i.** In this module we will design GUI for cloud data sharing and authentication.
- **ii.** We will develop data sharing GUI's on cloud

b. **Microsoft Windows Azure**

i. It is Microsoft cloud operating system where we will share data

ii. We will us SQL Azure for database management system

iii. We will use Azure security for user management

c. **Authentication Cryptography**

i. User's Profile Data will be stored in encrypted format to improve data security. Only authenticated and properly decrypted user can share and receive data.

ii. We will maintain key to share and receive data.

d. **RS-IBE RESISTANT TO DECRYPTION KEY EXPOSURE**

i. We first will present a concrete construction of RSIBE resistant to decryption key exposure, and then discuss its security and performance.

e. **Security Analysis**

i. If there exists a PPT adversary A breaking the INDRID- CPA security of the proposed RS-IBE scheme, then there exists an algorithm C solving the decisional ℓ-BDHE problem such that

$$\mathrm{Adv}_{C}^{\ell\text{-dBDHE}}(\lambda) \geq \frac{1}{32Tq^{2}(n+1)} \cdot \mathrm{Adv}_{\text{RS-IBE},A}^{\text{IND-RID-CPA}}(\lambda, T, N)$$

Where q is the maximum numberof secret key queries anddecryption key queries, and T = 2ℓ is the total number of timeperiods. Proof. Given a PPT adversary Abreaking the IND-RIDCPAsecurity of the proposed RS-IBE scheme, we willconstruct an algorithm C to solve the decisional ℓ-BDHEproblem. More precisely, given a random instance of ℓ-BDHE problem in the form of a tuple (G1,G2, e, p, **f**,D)where **f** = (g, gs, f1, ..fℓ, fℓ+2, ..., f2ℓ) and fi = gai∈G1 for≤ i≤ 2ℓ, the algorithm C can decide if D = e(fℓ+1, gs) by simulating the experiment according to the following steps.

IV. RESULTS AND DISCUSSION

Expected output will be such that

- There will be GUI that will contain user authentication in cryptography.
- After user authentication they will share confidential data in encrypted mode.
- User receiving data must be authenticated and need some keys to receive and decrypt data.

V. CONCLUSION AND FUTURE SCOPE

Cloud computing brings great convenience for people. Particularly,it perfectly matches the increased need of sharingdata over the Internet. In this paper, to build a cost-effectiveand secure data sharing system in cloud computing, weproposed a notion called RS-IBE, which supports identityrevocation and ciphertext update simultaneously such that arevoked user is prevented from accessing previously shareddata, 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 comparisonresults demonstrate that our scheme has advantagesin terms of efficiency and functionality, and thus is morefeasible for practical applications.

In Future we will develop a mobile based security algorithm where users will encrypt their confidential data and will share data without any hesitation with confidentiality proof sharing algorithm. Future App must be fast using jSon patterns even though with huge security models applied.

REFERENCES

[1] Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.

[2] iCloud. (2014) Apple storage service. [Online]. Available:https://www.icloud.com/

[3] Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/

[4] Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving
public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[7] G. Anthes, "Security in the cloud," *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.

[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] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction," in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 216–234.

[10] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50–55, 2008.

[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

