International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 08 | August - 2022 Impact Factor: 7.185 ISSN: 2582-3930

IMPLEMENTING SECURE DATA SHARING USING IBE USING CLOUD BASED REVOCABLE STORAGE SYSTEMS

S. Sampoornamma [1] , O. Bhargavi [2] , P.Nikhila [3] , T. Harshitha [4] ,

[1] Assistant Professor, Department of CSE , Narayana Engineering College, Gudur, A.P,India, sampoorna551@gmail.com

[2] Student, Department of CSE , Narayana Engineering College, Gudur, India, oggubhargavi333@gmail.com

[3] Student, Department of CSE , Narayana Engineering College, Gudur, India, nikhilapakanati11@gmail.com

[4] Student, Department of CSE , Narayana Engineering College, Gudur, India, harshitheegala@gmail.com

Abstract – Now days cloud computing provides a more and more 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. 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.

Index Terms – Identity based Encryption, User Revocation, Access Control Policy, Cloud Computing.

I. INTRODUCTION

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].

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. 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. 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.

The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographical tool to achieve the above security goals. We also note that there exist other security issues that are equally important for a practical system of data sharing, such as the authenticity and availability of the shared data. But the research on these issues is beyond the scope of this paper.

II. BACKGROUND

A) Revocable identity-based encryption

The concept of identity-based encryption was introduced by Shamir [13], and conveniently instantiated by Boneh and Franklin [14]. IBE eliminates the need for providing a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there must be an approach to revoke users from the system when necessary, e.g., the authority of some user is expired or the secret key of some user is disclosed. In the traditional PKI setting, the problem of revocation has been well studied [15], [16], [17], [18], [19], and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE. Boneh and Franklin [14] first proposed a natural revocation way for IBE. They appended the current time period to the ciphertext, and non-revoked users periodically received private keys for each time period from the key authority.

Unfortunately, such a solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. To conquer this problem, Boldyreva, Goyal and Kumar [20] introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users. However, this scheme only achieves selective security. Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud [21] proposed an adaptively secure

RIBE scheme based on a variant ofWater's IBE scheme [22], Chen et al. [23] constructed a RIBE scheme from lattices. Recently, Seo and Emura [24] proposed an efficient RIBE scheme resistant to a realistic threat called decryption key exposure, whichmeans that the disclosure of decryption key for current time period has no effect on the security of decryption keys for other time periods. Inspired by the above work and [25], Liang et al. [26] introduced a cloud- based revocable identity-based proxy re- encryption that supports user revocation and ciphertext update.

To reduce the complexity of revocation, they utilized a broadcast encryption scheme [27] to encrypt the ciphertext of the update key, which is independent of users, such that only non-revoked users can decrypt the update key. However, this kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non-revoked users can share the update key with those revoked users. Furthermore, to update the ciphertext, the key authority in their scheme needs to maintain a table for each user to produce the re-encryption key for each time period, which significantly increases the key authority's workload.

B) Forward-secure cryptosystems

In 1997, Anderson introduced the notion of forward security in the setting of signature to limit the damage of key exposure. The core idea is dividing the whole lifetime of a private key into T discrete time periods, such that the compromise of the private key for current time period cannot enable an adversary to produce valid signatures for previous time periods. Subsequently, Bellare and Miner provided formal definitions of forward-secure signature and presented practical solutions. Since then, a large number of forward-secure signature schemes has been proposed.

In the context of encryption, Canetti, Halevi and Katz proposed the first forward-secure public-key encryption scheme. Specifically, they firstly constructed a binary tree encryption, and then transformed it into a forward-secure encryption with provable security in the random oracle model. Based on Canetti et al's approach, Yao et al. proposed a forward-secure hierarchical IBE by employing two hierarchical IBE schemes, and Nieto et al. Designed a forward-secure hierarchical predicate encryption. Particularly, by combining Boldyreva et al.'s [20] revocation technique and the aforementioned idea of forward security1, in CRYPTO 2012 Sahai, Seyalioglu and Waters proposed a generic construction of so-called revocable storage attribute-based encryption, which supports user revocation and ciphertext update simultaneously.

In other words, their construction provides both forward and backward secrecy. What must be pointed out is that the process of ciphertext update of this construction only needs public information. However, their construction cannot be resistant to decryption key exposure, since the decryption is a matching result of private key and update key.

III. PROPOSED METHOD

In this paper, we introduce a notion called revocable storage identity-based encryption (RS-IBE) for building a cost-effective data sharing

system that fulfills the three security goals. More precisely, the following achievements are captured in this paper:

- We provide formal definitions for RS-IBE and its corresponding security model;
- We present a concrete construction of RS- IBE. The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously;
- We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure;
- The proposed scheme is efficient in the following ways: The procedure of ciphertext update only needs public information. Note that no previous identity-based encryption schemes in the literature can provide this feature;

– The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by $O(\log(T)^2)$, where T is the total number of time periods.

A) KUNodes Algorithm

Our RS-IBE scheme uses the same binary tree structure introduced by Boldyreva, Goyal and Kumar to achieve efficient revocation. To describe the revocation mechanism, we first present several notations. Denote by ε the root node of the binary tree BT , and Path(η) the set of nodes on the path from ε to the leaf node η (including ε and η). For a non-leaf node θ, we let θl and θr stand for its left and right child, respectively. Given a time period t and revocations list RL, which is comprised of the tuples (ηi, ti) indicating that the node ηi was revoked at time period ti, the algorithm KUNodes(BT ,RL, t) outputs the smallest subset Y of nodes of BT such that Y contains an ancestor for each node that is not revoked before the time period t.

Algorithm 1 KUNodes$(\mathcal{BT}, RL, t)$

```
X,Y ← ∅
for all (η_i, t_i) ∈ RL do
  if t_i ≤ t then
    Add Path(η_i) to X
  end if
end for
for all θ ∈ X do
  if θ_l ∉ X then
    Add θ_l to Y
  end if
  if θ_r ∉ X then
    Add θ_r to Y
  end if
end for
if Y = ∅ then
  Add the root node ε to Y
end if
return Y
```

IV. SYSTEM IMPLEMENTATION

Data Provider

In this module, we develop the Data Provider module. The data provider module is developed such that the new users will Signup initially and then Login for authentication. The data provider module provides the option of uploading the file to the Cloud Server. The process of File Uploading to the cloud Server is undergone with Identity-based encryption format. Data Provider will check the progress status of the file upload by him/her. Data Provider provided with the features of Revocation and Ciphertext update the file. Once

after completion of the process, the Data Provider logouts the session.

User:

- User will Register and login on the user' page
- User will search file after send the request to auditor for the file access
- After getting decrypt key from the auditor he/she can access to the file.
- After download to the file.
- User logout the session.

Cloud Server:

- Cloud server offers the Data Storage as a Service and store the users upload file in the public cloud.

Key Authority:

Auditor Will Login on the Auditor's page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt. After the complete process, the Auditor logout the session.

V. CONCLUSION

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, a concrete construction of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the standard model.

REFERENCES

[1] 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.

[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 cloudcomputing: 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, "Privacypreserving 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] 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.

[9] 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, pp. 2904–2912.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.