IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 5, May 2016

Implementation of IBE with Outsourced Revocation technique in Cloud Computing

Sangappa Kuragod[1], Parikshit Nayak[2], Manjunath Kotari[3]

M.Tech Student, Dept. of CSE, Alva's Institute of Engg. & Technology, Mijar, Moodbidri, Karnataka, India[1]

Assistant Professor, Dept. of CSE, Alva's Institute of Engg. &Tech, Mijar, Moodbidri, Karnataka, India[2]

Sr. Associate Professor, Dept. of CSE, Alva's Institute of Engg. &Tech, Mijar, Moodbidri, Karnataka, India[3]

Abstract*:* Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this project, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique: Furthermore, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model.

Keywords: Identity-based encryption (IBE), revocation, outsourcing, cloud computing.

I. INTRODUCTION

IDENTITY-BASED Encryption (IBE) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys. Therefore, sender using IBE does not need to look up public key and certificate, but directly encrypts message with receiver's identity. Accordingly, receiver obtaining the private key associated with the corresponding identity from Private Key Generator (PKG) is able to decrypt such cipher text. Though IBE allows an arbitrary string as the public key which is considered as appealing advantages over PKI, it demands an efficient revocation mechanism. Specifically, if the private keys of some users get compromised, we must provide a mean to revoke such users from system. In PKI setting, revocation mechanism is realized by appending validity periods to certificates or using involved combinations of techniques [1]–[3]. Nevertheless, the cumbersome management of certificates is precisely the burden that IBE strives to alleviate.

As far as we know, though revocation has been thoroughly studied in PKI, few revocation mechanisms are known in IBE setting. In Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period. But this mechanism would result in an overhead load at PKG. In another word, all the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys. It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows. In 2008, Boldyreva, Goyal and Kumar presented a revocable IBE scheme. Their scheme is built on the idea of fuzzy IBE primitive but utilizing a binary tree data structure to record users' identities at leaf nodes. Therefore, key-update efficiency at PKG is able to be significantly reduced from linear to the height of such binary tree (i.e. logarithmic in the number of users). Never the less, we point out that though the binary tree introduction is able to achieve a relative high performance, it will result in other problems: 1) PK Ghas to generate a key pair for all the nodes on the path from the identity leaf node to the root node, which results in complexity logarithmic in the number of users in system for issuing a single private key. 2) The size of private key grow sin logarithmic in the number of users in system, which makes it difficult in private key storage for users. 3) As the number of users in system grows, PK Ghasto maintains a binary tree with a large amount of nodes, which introduces another bottleneck for the global system. In tandem with the development of cloud computing, there has emerged the ability for users to buy on-demand computing from cloud-based services such as Amazon's EC2 and Microsoft's Windows Azure. Thus it desires a new working paradigm for introducing such cloud services into IBE revocation to fix the issue of efficiency and storage overhead described above. A naive approach would be to simply hand over the PKG's master key to the Cloud Service Providers (CSPs). The CSPs could then simply update all the private keys by using the traditional key update technique [4] and transmit the private keys back to

unrevoked users. However, the naive approach is based on an unrealistic assumption that the CSPs are fully trusted and is allowed to access the master key for IBE system.

On the contrary, in practice the public clouds are likely outside of the same trusted domain of users and are curious for users' individual privacy. For this reason, a challenge on how to design a secure revocable IBE scheme to reduce the overhead computation at PKG with an un trusted CSP is raised. In this paper, we introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourced revocable IBE for the first time to the best of our knowledge. We propose a scheme to offload all the key generation related operations during key-issuing and key update, leaving only a constant number of simple operations for PKG and eligible users to perform locally. In our scheme, as with the suggestion in [4], we realize revocation through updating the private keys of the unrevoked users. But unlike that work [4] which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component. At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decrypt ability, unrevoked users needs to periodically request on key update for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP).

II. RELATED WORK

Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys. Therefore, sender using IBE does not need to look up public key and certificate, but directly encrypts message with receiver's identity.

Accordingly, receiver obtaining the private key associated with the corresponding identity from Private Key Generator (PKG) is able to decrypt such cipher text. Though IBE allows an arbitrary string as the public key which is considered as an appealing advantages over PKI, it demands an efficient revocation mechanism. Specifically, if the private keys of some users get compromised, we must provide a mean to revoke such users from system. In PKI setting, revocation mechanism is realized by appending validity periods to certificates or using involved combinations of techniques. Nevertheless, the cumbersome management of certificates is precisely the burden that IBE strives to alleviate

Firstly implemented by Boneh and Franklin, IBE has been researched intensively in cryptographic community. On the aspect of construction, these first schemes were proven secure in random oracle. Some subsequent systems achieved provable secure in standard model under selective-ID security or adaptive-ID security. Recently, there have been multiple lattice-based constructions for IBE systems. Nevertheless, concerning on revocable IBE, there is little work presented. As mentioned before, Boneh and Franklin's suggestion [4] is more a viable solution but impractical. Hanaoka et al. proposed a way for users to periodically renew their private keys without interacting with PKG. However, the assumption required in their work is that each user needs to possess a tamper-resistant hardware device. Another solution is mediator-aided revocation: In this setting there is a special semi-trusted third party called a mediator who helps users to decrypt each cipher text. If an identity is revoked then the mediator is instructed to stop helping the user. Obviously, it is impractical since all users are unable to decrypt on their own and they need to communicate with mediator for each decryption.

Recently, Lin et al. proposed a space efficient revocable IBE mechanism from non-monotonic Attribute-Based Encryption (ABE), but their construction requires times bilinear pairing operations for a single decryption where the number of revoked users is. As far as we know, the revocable IBE scheme presented by Boldyreva et al. remains the most effective solution right now. Libert and Vergnaud improved Boldyreva's construction to achieve adaptive-ID security. Their work focused on security enhanced, but inherits the similar disadvantage as Boldyreva's original construction. As we mentioned before, they are short in storage for both private key at user and binary tree structure at PKG.

Another work related to us originates from Yu et al. The authors utilized proxy re-encryption to propose a revocable ABE scheme. The trusted authority only needs to update master key according to attribute revocation status in each time period and issue proxy re-encryption key to proxy servers. The proxy servers will then re-encrypt cipher text using the re-encryption key to make sure all the unrevoked users can perform successful decryption. We specify that a third party service provider is introduced in both Yu et al. and this work. Differently, Yu et al. utilized the third party (work as a proxy) to realize revocation through re-encrypting cipher text which is only adapt to the special application that the cipher text is stored at the third party. However, in our construction the revocation is realized through updating private keys for unrevoked users at cloud service provider which has no limits on the location of cipher text.

The problem that how to securely outsource different kinds of expensive computations has drawn considerable attention from theoretical computer science community for a long time.Chaum and Pedersen [8] firstly introduced the notion of wallets with observers, a piece of secure hardware installed on the client's computer to perform some expensive computations. Atallah et al. presented a framework for secure outsourcing of scientific

computations such as matrix multiplication and quadrature. Nevertheless, the solution used the disguise technique and thus leaded to leakage of private information. Hohenberger and Lysyanskaya proposed the first outsource-secure algorithm for modular exponentiations based on pre-computation and server-aided computation. Atallah and Li investigated the problem of computing the edit distance between two sequences and presented an efficient protocol to securely outsource sequence comparison with two servers. Furthermore, Benjamin and Atallah addressed the problem of secure outsourcing for widely applicable linear algebraic computations. Nevertheless, the proposed protocol required the expensive operations of homomorphism encryption. Atallah and Frikken further studied this problem and gave improved protocols based on the so-called weak secret hiding assumption. Chen et al. made an efficiency improvement on the work and proposed a new scheme for outsourcing single/simultaneous modular exponentiations.

III. METHODOLOGY

The proposed Identity Based Encryption and outsourced revocation uses the alorithm is called RSA algorithm for encryption and decryption of the massages and also uses the two more algorithm Extended Euclidean Algorithm and MD5 Algorithm for the plain text to cipher text oprations. using collusion resistant algorithm we are going to outsourced the computation of user revocation to another system then every thing will be done automatically like, find out the expire date of public key and issue the new public key to the user all those thing will be done automatically in proposed system.

IV. EXISTING SYSTEM

As far as we know, though revocation has been thoroughly studied in PKI, few revocation mechanisms are known in IBE setting. Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period. But this mechanism would result in an overhead load at PKG.

In another word, all the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys. It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows. In 2008, Boldyreva, Goyal and Kumar presented a revocable IBE scheme. Their scheme is built on the idea of fuzzy IBE primitive but utilizing a binary tree data structure to record users' identities at leaf nodes. Therefore, key-update efficiency at PKG is able to be significantly reduced from linear to the height of such binary tree (i.e. logarithmic in the number of users).

Nevertheless, we point out that though the binary tree introduction is able to achieve a relative high performance, it will result in other problems:

PKG has to generate a key pair for all the nodes on the path from the identity leaf node to the root node, which results in complexity logarithmic in the number of users in system for issuing a single private key.

The size of private key grows in logarithmic in the number of users in system, which makes it difficult in private key storage for users.

As the number of users in system grows, PKG has to maintain a binary tree with a large amount of nodes, which introduces another bottleneck for the global system.

In tandem with the development of cloud computing, there has emerged the ability for users to buy on-demand computing from cloud-based services such as Amazon's EC2 and Microsoft's Windows Azure. Thus it desires a new working paradigm for introducing such cloud services into IBE revocation to fix the issue of efficiency and storage overhead described above. A naive approach would be to simply hand over the PKG's master key to the Cloud Service Providers (CSPs). The CSPs could then simply update all the private keys by using the traditional key update technique and transmit the private keys back to unrevoked users.

However, the naive approach is based on an unrealistic assumption that the CSPs are fully trusted and is allowed to access the master key for IBE system. On the contrary, in practice the public clouds are likely outside of the same trusted domain of users and are curious for users' individual privacy. For this reason, a challenge on how to design a secure revocable IBE scheme to reduce the overhead computation at PKG with an un trusted CSP is raised.

Major Drawbacks of the Existing System

- Boneh and Franklin's mechanism would result in an overhead load at PKG (Private Key Generator)
- All the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys.
- It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows.
- IBE revocation has the issue of efficiency and storage overhead.

V. PROPOSED SYSTEM

- In this project, we introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourced revocable IBE for the first time to the best of our knowledge. We propose a scheme to offload all the key generation related operations during key-issuing and key update, leaving only a constant number of simple operations for PKG and eligible users to perform locally.

- In our scheme, as with the suggestion in, we realize revocation through updating the private keys of the

unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component.

• At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decrypt ability, unrevoked users needs to periodically request on key update for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP). Compared with the previous work, our scheme does not have to re-issue the whole private keys, but just need to update a lightweight component of it at a specialized entity KU-CSP. We also specify that 1) with the aid of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP. 2) No secure channel or user authentication is required during key-update between user and KU-CSP.

• Furthermore, we consider realizing revocable IBE with a semi-honest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Supporting Diagram for reference

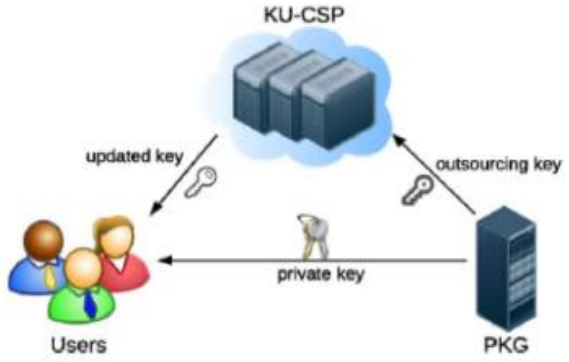

Fig1. System model for IBE with outsourced revocation.

Major Advantages of the Proposed System

- We tackle the critical issue of identity revocation
- We introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting.
- Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally
- We also consider realizing revocable IBE with a semi-honest KU-CSP

VI. PROBLEM STATEMENT

Attribute based Encryption has the following three issues:

- Complexity of user secret key management for large scale cloud environments
- Complexity of revoking the user access rights
- Computational complexity involved in assigning user rights, encrypting access rights, encrypting and accessing data files

VII. CONCLUSION

In this paper, focusing on the critical issue of identity revocation, we introduce outsourcing computation into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the proposed scheme is full-featured: 1) It achieves constant efficiency for both computation at PKG and private key size at user; 2) User needs not to contact with PKG during key update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP; 3) No secure channel or user authentication is required during key-update between user and KU-CSP.

REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology (CRYPTO'98). New York, NY, USA: Springer, 1998, pp. 137–152.
[2] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, S. Dietrich and R. Dhamija, Eds. Berlin, Germany: Springer, 2007, vol. 4886, pp. 247–259.
[3] F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficient certificate validation and revocation," in Public Key Cryptography (PKC'04), F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany: Springer, 2004, vol. 2947, pp. 375–388.
[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology (CRYPTO '01), J. Kilian, Ed. Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.
[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15thACMConf. Comput.Commun.Security (CCS'08), 2008, pp. 417 426.
[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557–557.
[7] R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation," Cryptology ePrint Archive, Rep. 2011/ 518, 2011 [online]. Available: http://eprint.iacr.org/2011/51
[8] D. Chaum and T. P. Pedersen, "Wallet databases with observers," in Proc. 12th Annu. Int. Cryptology Conf. Adv. Cryptology (CRYPTO'92), 1993, pp. 89–105.
[9] M. J. Atallah and J. Li, "Secure outsourcing of sequence comparisons," Int. J. Inf. Security, vol. 4, pp. 277–287, 2005.
[10] M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebra computations," in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'10), 2010, pp. 48–59.