I J C T A, 9(16), 2016, pp. 7757-7762

Identity Based Encryption with Outsourced Revocation in Key Generator

Vaannesh K.* and Nirmal Sam S.**

ABSTRACT

Identity-Based Encryption (IBE) which simplified the public key encrypted and certificate management at Public Key Infrastructure (PKI) is animportant alternative method for public key encryption. However one of the main efficiency drawback is that IBE is the partially overheadcomputation method where its proceed at Private Key Generator (PKG) during user revocation method determined Efficient revocation is being well studied in traditional PKI setting where the process is carried out by an traditional management of certificated is the burden that IBE strives to processing thereby this paper, aiming at tackling the critical issue of identity revocation method thereby we introduce outsourcing format 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 like key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constantnumber of simple operations for PKG and users to perform locally structured The goal is achieved by utilizing a novel collusion-resistant technique thereby we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the rendering Finallythereby providingextensive experimental results to demonstrates the efficiency of our proposed construction.

Keywords: identity-based signature; identity-based encryption; identity-based key issuing; instant messaging; bilinear pairings; combat vehicle research development & establishment(CVRDE).

1. INTRODUCTION

Identity cryptosystem is the interesting alternative to proposed public key type encrypted which is proposed to simplified key management in a certificated method based on Public Key Infrastructure (PKI) purpose by using human intelligible identity based as public keys. Thereby sender using IBE does not need to look for public key and certificated but directly encrypts on messages with receiver's server identity.

Accordingly to receiver is obtaining formation of the private key associated corresponding identity from Private Key Generator (PKG) is able to decrypt such ciphertext format analysis. Though IBE allows an arbitrary formation string as the public key which is considered as an appealing advantages over PKI format as it demands an efficient revocation mechanism Specifically so if the private keys of some users get compromised we must provide a mean to revoke such users from system indication. In PKI setting revocation mechanism is realized by appending validity periods tocertificated by using involved combinations of techniques performed.

The revocation has been thoroughly studied in PKI where few revocation mechanisms are known in IBE settings. Thereby it is suggested that users renewal their private key periodic and these senders use the receivers identity key to concatenated with current time periodically . But this mechanism would result in an overhead load at PKG format.

* M.Tech (final year) Department of computer Science and Engineering, *Email: vaannesh@gmail.com*

** Assistant Professor, *Email: snirmalsam@gmail.com*

Thereby all the users regardless performing of whether their keys have been revoked or not have to contact with PKG periodically to proved their identities capacity and update new private keys encrypted format as It requires that PKG is online and the secure channel must be maintained for transactions.

PKG has to generate a keypair for all the nodes on the path from the identity based leaf node to the root node, which results in complexity logarithmic in the number of users in systematic type for issuing a single private key encryption entry.

The size of users in system which makes it difficult in private key storage type forusers format.

We introduce an outsourcing computation for revocation into IBE revocation by formalized the security definition of outsourced formation. The key generation for related operations during key issues is performed by simple operations for PKG by performing the revocation.

2. SYSTEM SPECIFICATIONS

The system model of an outsourced formation to revocable is generated by users. The deliver basic for computing the capabilities for services throughout the network in PKG computation.

When revocation is sended for private keys from PKG through predefined users where service providers is designed to to PKG.

Based on the system model proposed the KeyGen Encrypt and Decrypt is proposed to formation of algorithms in time component architecture.

3. SECURITY ISSUES AND PURPOSE

An identity based system where encryption is systemically relocated to adaptive process chosen-ciphertext attack.

There by the polynomial time is encrypted during process of recovery An IBE with revocation scheme is secured in polynomial time for adversary in revocation.

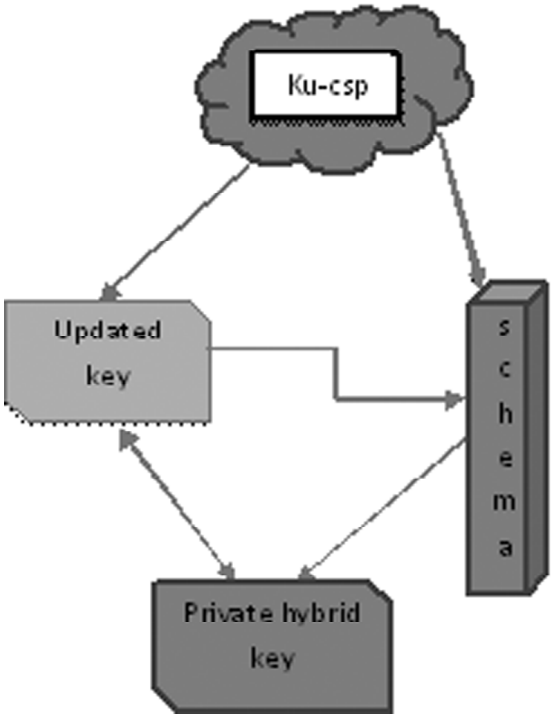

Figure 1: System Model Specifiacation

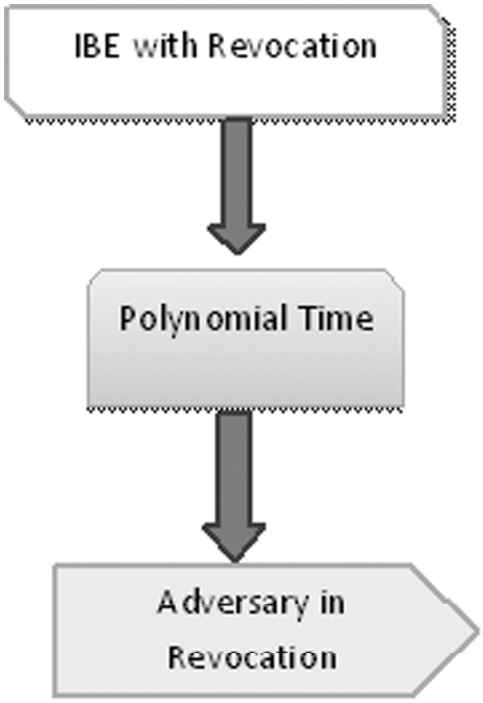

Figure 2: Security Issues in Revocation

4. PROBLEM DEFINATIONS

The critical formation of identity based type on revocation for computing a source of schemes into revocable one for operating system.

Itachieves efficiency for computation processing where key is generated.

The User specifies an update for PKG during key update on specifications.

5. OUTCOME FOR REVOCATION PROCESS

In order to maintain revocation we need an key update to hybrid cloud.

We utilize an hybrid key for predefined user in which time component isgenerated by PKG for key generation. In encrypting an key the user's identity is for specifications of an time period embedded in private key.

The private key is identical to component of time where user is predicted to capabilities of time Encrypted by it time component is updated for all users for revocation purpose for preferred users for identifying an key.

5.1. Multi-encryption in Client

The information and data are shared by the user in the cloud computing where keys are generated by it.

The information is varied by each processwhere the data is encrypted by an each sources.

The access control is based on PKG during Encryption algorithm where server is based on client features.

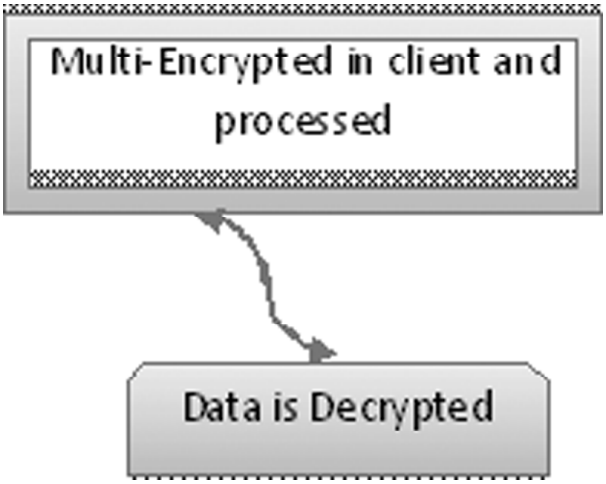

Figure 3: Multi Encryption in Client

6. SECURITY ISSUES

The KU-CSP is generated in the proposed manner of system specifications where the protocol is determined by revocation in which keys aregenerated by it.

Type-I specification: The user with identity key is obtained from time period constantly in the cipher text where keys are generated.

With the users the keys are unrevoked to allow then in private component where it can generate it.

Type-II specification: The outsourced formation of an keying is structured in revocation where keys are generated by schemes in hybrid type without interference of cloud

7. SECURITY ANALYSIS

The adversary model which captures server with private key is modified by outsourcekeys where key is generated by it. The outsourcing keys is analysed as the challenger for accomdation of keys. The analysis of keys is modified and generated by source of security purposes.

8. PERFORMANCE ANALYSIS

We aim to evaluate the efficiency of our outsourced revocable scheme by comparing the total time taken during each stage with the original IBE which does not consider revocation.

It is not surprising to see that our scheme takes more time because we consider the revocability issue.

This is because we embed a time component into each user's private key to allow periodically update for revocation resulting that some additional computations are needed in our scheme to initialize this component.

To sum up, our revocable scheme achieves both identity based encryption/decryption and revocability.

9. KEY ISSUE STAGE PROCESS

The maximum number of users in the system and show the responding time for a single key generation request.

This is because a binary tree is utilized to manage all the users, each leaf node of which is assigned to a single user in system.

During key-issuing, PKG has to perform computation on all the nodes in the path from the corresponding leaf node to root node.

The maximum number of users in system initially to facilitate building the binary tree wherethe maximum number is fixed it is difficult to add users exceeding this bound. Ours does not have such a drawback, and flexibly supports dynamic management of users.

10. OUTSOURCE COMPUTATION PROCESS

The KU-CSP provides computing service in the Infrastructure as a service which provides the raw materials of cloud computing, such as processing, storage and other forms of lower level network and hardware resources in a virtual

Differing from traditional hosting services with which physical servers or parts thereof are rented on a monthly or yearly basis, the cloud infrastructure is rented as virtual machines on a per-use basis and can scale in and out dynamically

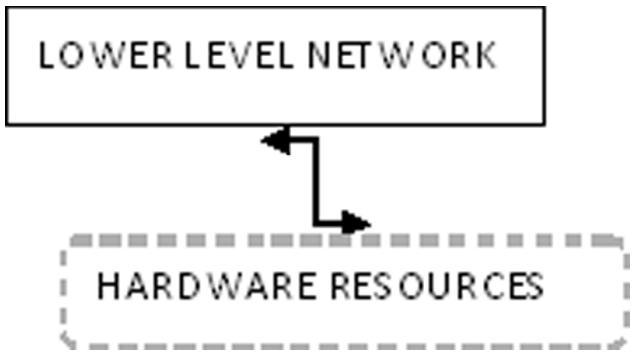

Figure 4: Outsource Configuration

11. CONCLUSION

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.

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 keyupdate.

Finally it provides an extensive experimental results to demonstrate the efficiency of our proposed construction.

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. 15th ACM Conf. 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/2011/518.

[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in Proc. 29th Annu. ACM Symp. Theory Comput. (STOC'97), 1997, pp. 506–516.

[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography (TCC'05), 2005, pp. 264–282.

[10] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, A. Smith, Ed. Berlin, Germany: Springer, 2012, vol. 7412, pp. 37–61.

[11] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Security (ESORICS), 2012, pp. 541–556.

[12] 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.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology (CRYPTO), G. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, vol. 196, pp. 47–53.

[14] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, B. Honary, Ed. Berlin/ Heidelberg: Springer, 2001, vol. 2260, pp. 360–363.

[15] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in Advances in Cryptology (EUROCRYPT'03), E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656, pp. 646–646.

[16] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'04), C. Cachin and J. Camenisch, Eds. Berlin, Germany: Springer, 2004, vol. 3027, pp. 223–238.

[17] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in Advances in Cryptology (CRYPTO'04), M. Franklin, Ed. Berlin, Germany: Springer, 2004, vol. 3152, pp. 197–206.

[18] B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127.

[19] C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.

[20] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proc. 40th Annu. ACM Symp. Theory Comput. (STOC'08), 2008, pp. 197–206.

[21] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (h)ibe in the standard model," in Advances in Cryptology (EUROCRYPT'10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.

[22] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in Advances in Cryptology (EUROCRYPT'10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 523–552.

[23] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-insulated encryption and its application," in Advances in Cryptology (ASIACRYPT'05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495–514.

[24] D. Boneh, X. Ding, G. Tsudik, and C. Wong, "A method for fast revocation of public key certificates and security capabilities," in Proc. 10th USENIX Security Symp., 2001, pp. 297–308.

[25] B. Libert and J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in Proc. 22nd Annu. Symp. Principles Distrib. Comput., 2003, pp. 163–171.

[26] H. Lin, Z. Cao, Y. Fang, M. Zhou, and H. Zhu, "How to design space efficient revocable IBE from non-monotonic ABE," in Proc. 6th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'11), 2011, pp. 381–385.

[27] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identitybased encryption," in Topics in Cryptology (CT-RSA'09), M. Fischlin, Ed. Berlin, Germany: Springer, 2009, vol. 5473, pp. 1–15.

[28] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'10), 2010, pp. 261–270.

[29] 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.

[30] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," in Trends in Software Engineering, M. V. Zelkowitz, Ed. New York, NY, USA: Elsevier, 2002, vol. 54, pp. 215–272.