International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Identity-based Encryption Scheme for Cloud Data Sharing

A. M. Rangaraj, P. Poojitha, M. Sravani
Department of Computer Science And Engineering, Sri Venkateswara College of Engineering & Technology(Autonomous), R.V.S Nagar, Chittoor, India

ABSTRACT

In this paper, aiming at confronting the essential issue of identity revocation, we tend to introduce outsourcing computation into IBE for the first time and propose a revokable IBE theme within the server-aided setting. Our theme offloads most of the key generation connected operations throughout key-issuing and key-update processes to a Key Update Cloud Service supplier, going solely a relentless range of simple operations for PKG and users to perform domestically. This goal is achieved by utilizing a unique collusion-resistant technique: we tend to employ a hybrid personal key for every user, within which an and gate is involved to attach and sure the identity element and therefore the time component. what is more, we propose another construction that is provable secure below the recently formulized Refereed Delegation of Computation model.

Keywords: Identity-based encryption, Revocation, Outsourcing, Cloud computing.

I. INTRODUCTION

Identity-Based encoding (IBE) is a motivating different to public key encoding, that is planned to modify key management in a very certificate-based Public Key Infrastructure (PKI) by victimization human-intelligible identities (e.g., distinctive name, email address, IP address, etc) as public keys. Therefore, sender victimization IBE doesn't ought to find public key and certificate, but directly encrypts message with receiver's identity. consequently, receiver getting the non-public key related to the corresponding identity from non-public Key Generator (PKG) is ready to rewrite such ciphertext. Though IBE permits a discretional string because the public key that is considered as associate degree appealing benefits over PKI, it demands an efficient revocation mechanism. Specifically, if the non-public keys of some users get compromised, we tend to should offer a mean to revoke such users from system. In PKI setting, revocation mechanism is complete by appending validity periods to certificates or victimization involved mixtures of techniques. Notwithstanding, the cumbersome management of certificates is exactly the burden that IBE strives to alleviate. As so much as we all know, tho' revocation has been totally studied in PKI, few revocation mechanisms ar noted in IBE.

setting. Boneh and Franklin steered that users renew their private keys sporadically and senders use the receivers' identities concatenated with current fundamental measure. however this mechanism would result in a overhead load at PKG. In another word, all the users regardless of whether or not their keys are revoked or not, have to contact with PKG sporadically to prove their identities and update new non-public keys. It needs that PKG is on-line and also the secure channel should be maintained for all transactions, which will become a bottleneck for IBE system because the range of users grows. In 2008, Boldyreva, Goyal and Kumar given a rescindable IBE scheme. Their theme is constructed on the concept of fuzzy IBE primitive however utilizing a binary tree system to record users' identities at leaf nodes. Therefore, key-update potency at PKG is ready to be

considerably reduced from linear to the height of such binary tree (i.e. index within the range of users). Nevertheless, we tend to suggests that tho' the binary tree introduction is able to attain a relative high performance, it'll lead to alternativeproblems: 1) PKG needs to generate a key try for all the nodes on the path from the identity leaf node to the basis node, which ends up in quality index within the range of users in system for issuing one non-public key. 2) the dimensions of personal key grows in index within the range of users in system, that makes it tough in camera key storage for users. 3) because the range of users in system grows, PKG needs to maintain a binary tree with a large quantity of nodes, that introduces another bottleneck for the global system. In wheel with the event of cloud computing, there has emerged the flexibility for users to shop for on-demand computing from cloud-based services like Amazon's EC2 and Microsoft's Windows Azure. so it wishes a replacement operating paradigm for introducing such cloud services into IBE revocation to repair the issue of potency and storage overhead delineate higher than. A naive approach would be to easily hand the PKG's passe-partout to the Cloud Service suppliers (CSPs). The CSPs might then merely update all the non-public keys by victimization the standard key update technique and transmit the non-public keys back to unrevoked users. However, the naive approach is predicated on associate degree false assumption that the CSPs ar totally sure and is allowed to access the passe-partout for IBE system. On the contrary, in observe the public clouds ar possible outside of an equivalent sure domain of users and ar curious for users' individual privacy. For this reason, a challenge on the way to style a secure rescindable IBE theme to reduce the overhead computation at PKG with associate degree untrusted CSP is raised.

In this paper, we tend to introduce outsourcing computation into IBE revocation, and formalize the protection definition of outsourced revocable IBE for the primary time to the simplest of our information. We propose a theme to dump all the key generation connected operations throughout key-issuing and key-update, departure solely a constant range of easy operations for PKG and eligible users to perform domestically. In our theme, like the suggestion in, we tend to understand revocation through change the non-public keys of the unrevoked users. however not like that job that trivially concatenates fundamental measure with identity for key generation/update and needs to re-issue the full non-public key for unrevoked users, we propose a unique collusion-resistant key issue technique: we tend to employ a hybrid non-public key for every user, within which associate degree gate is concerned to attach and sure 2 sub-components, namely the identity part and also the time part. At first, user is ready to obtain the identity part and a default time part (i.e., for current time period) from PKG as his/her non-public key in key-issuing. Afterwards, so as to take care of decryptability, unrevoked users must sporadically request on key-update for time part to a recently introduced entity named Key Update Cloud Service supplier (KU-CSP).

II. ALGORITHM

Identity-based Encryption An IBE scheme which typically involves two entities, PKG and users (including sender and receiver) is consisted of the following four algorithms.

Setup(λ) : The setup algorithm takes as input a security parameter λ and outputs the public key PK and the master key MK. Note that the master key is kept secret at PKG.

KeyGen(MK,ID): The private key generation algorithm is run by PKG, which takes as input the master key MK and user's identity ID ∈ {0, 1}∗. It returns a private key SKID corresponding to the identity ID.

Encrypt(M,ID) : The encryption algorithm is run by sender, which takes as input the receiver's identity ID and a message M to be encrypted. It outputs the ciphertext CT.

Decrypt(CT,SKID): The decryption algorithm is run by receiver, which takes as input the ciphertext CT and his/her private key SKID . It returns a message M or an error ⊥. An IBE scheme must satisfy the definition of consistency. Specifically, when the private key SKID generated by algorithm KeyGen when it is given ID as the input, then Decrypt(CT,SKID) = M where CT = Encrypt(M,ID). The motivation of IBE is to simplify certificate management. For example, when Alice sends an email to Bob at bob@company.com, she simply encrypts her message using Bob's email address "bob@company.com", but does not need to obtain Bob's public key certificate. When Bob receives the encrypted email he authenticate himself at PKG to obtain his private key, and read his email with such a private key.

III. 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. Furthermore, we consider to realize revocable IBE under a stronger adversary model. We present an advanced construction and show it is secure under RDoC model, in which at least one of the KU-CSPs is assumed to be honest. Therefore, even if a revoked user and either of the KU-CSPs collude, it is unable to help such user re-obtain his/her decryptability.

IV. REFERENCES

[1]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology – CRYPTO'98. Springer, 1998.

[2]. V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 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 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375–388.

[4]. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology – CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213–229.

[5]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS '08. New York, NY, USA: ACM, 2008, pp. 417–426.

[6]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 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, Report 2011/518, 2011.

[8]. U. Feige and J. Kilian, "Making games short (extended abstract)," in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC '97. New York, NY, USA: ACM, 1997, pp. 506–516.

[9]. S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proceedings of the Second

international conference on Theory of Cryptography, ser. TCC'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 264–282.

[10]. R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, ser. Lecture Notes in Computer Science, A. Smith, Ed. Springer Berlin / Heidelberg, 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 17th European Symposium on Research in Computer Security (ESORICS), 2012.

[12]. M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebra computations," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 48–59.

[13]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology – CRYPTO, ser. Lecture Notes in Computer Science, G. Blakley and D. Chaum, Eds. Springer Berlin / Heidelberg, 1985, vol. 196, pp. 47–53.

[14]. C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, ser. Lecture Notes in Computer Science, B. Honary, Ed. Springer Berlin / Heidelberg, 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 2003, ser. Lecture Notes in Computer Science, E. Biham, Ed. Springer Berlin / Heidelberg, 2003, vol. 2656, pp. 646–646.

Author's Profile:

A.M. Rangaraj working as an Assoc. professor in Sri Venkateswara College of Engineering & Technology, Chittoor, A.P.

P.Poojitha received the PG degree from Sri Venkateswara College of Engineering & Technology, Chittoor, A.P.

M.Sravani received the PG degree from Sri Venkateswara College of Engineering & Technology, Chittoor, A.P.