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

Identity-Based Encryption of Data Under Cloud System

S.Mamatha[1], K.Sunitha[2]

[12]RIIMS College, Tirupati, Andhra Pradesh, India

ABSTRACT

Identity-Based coding that simplifies the public key and certificate management at Public Key Infrastructure (PKI) is a vital different to public key coding. However, one of the most potency drawbacks of IBE is that the overhead computation at non-public Key Generator (PKG) throughout user revocation. Efficient revocation has been well studied in ancient PKI setting, but the cumbersome management of certificates is exactly the burden that IBE strives to alleviate. In this paper, aiming at coping with the important issue of identity revocation, we tend to introduce outsourcing computation into IBE for the first time and propose a revocable 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, deed solely a relentless variety 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 non-public key for every user, within which an AND circuit is involved to attach and sure the identity part and the time component. what is more, we tend to propose another construction that is provable secure beneath the recently formulized Refereed Delegation of Computation model. Finally, we offer in depth experimental results to demonstrate the potency of our planned construction.

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

I. INTRODUCTION

Identity-Based coding (IBE) is a motivating different to public key coding, that is planned to alter key management during a certificate-based Public Key Infrastructure (PKI) identities (e.g., distinctive name, email address, IP address, etc) as public keys. Therefore, sender victimization IBE doesn't have to be compelled to research 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 in a position to decipher such cipher text. Though IBE permits an impulsive string because the public key that is considered as an 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 accomplished by appending validity periods to certificates or victimization involved mixtures of techniques. However, the cumbersome management of certificates is exactly the burden that IBE strives to alleviate. As so much as we all know, the revocation has been totally studied in PKI, few revocation mechanisms are famous in IBE setting. 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 brand new operating paradigm for introducing such cloud services into IBE revocation to mend the issue of potency and storage overhead represented higher than. A naïve approach would be to easily deliver the PKG's key to the Cloud Service suppliers (CSPs). The CSPs may then merely update all the non-public keys by victimization the normal key update technique and transmit the non-public keys back to unrevoked users. However, the naive approach relies on an chimerical assumption that the CSPs are

absolutely trusty and is allowed to access the key for IBE system. On the contrary, in observe the public clouds are probably outside of constant trusty domain of users and are curious for users' individual privacy. For this reason, a challenge on the way to style a secure revocable IBE theme to reduce the overhead computation at PKG with an untrusted CSP is raised. In existing system the mobile cloud atmosphere is employed for storing and assessing information and so it's required to own an economical cloud network that's a framework for communication and information authentication. For authentication it's important to design a security framework for mobile cloud environment that ensures higher authentication of information in the mobile devices and within the storage devices. However identity revocation could be a major issue In this paper, we tend to introduce outsourcing computation into IBE revocation, and formalize the safety 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, going away solely a constant variety of easy operations for PKG and eligible users to perform regionally. In our theme we tend to understand revocation through change the non-public keys of the unrevoked users. However not like that job that trivially concatenates period of time with identity for key generation/update and needs to re-issue the entire non-public key for unrevoked users, we propose a completely unique collusion-resistant key issue technique: we tend to employ a hybrid non-public key for every user, during which a gate is concerned to attach and certain 2 sub-components, namely the identity part and also the time part. At first, user is in a position 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 keep up decryptability, unrevoked users has to sporadically request on key-update for time part to a fresh introduced entity named Key Update.

II. SCHEME

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 $\in \{0, 1\}*$. It returns a private key *SK*ID 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,SK_{ID}) : The decryption algorithm is run by receiver, which takes as input the ciphertext *CT* and his/her private key *SK*ID . It returns a message *M* or an error. An IBE scheme must satisfy the definition of consistency. Specifically, when the private key *SK*ID generated by algorithm KeyGen when it is given ID as the input, then Decrypt(*CT,SK*ID) = *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, concentrating on the basic issue of personality repudiation, we bring outsourcing calculation into IBE and propose a revocable plan in which the denial task are appointed to CSP. With the guide of KU-CSP, the proposed conspire is full-included: It accomplishes consistent productivity for both calculation at PKG and private key size at client; User needs not to contact with PKG amid key-refresh, at the end of the day, PKG is permitted to be disconnected in the wake of sending the renouncement rundown to KU-CSP; No protected channel or client confirmation is required amid key-refresh amongst client and KU-CSP.

Moreover, we consider acknowledging revocable IBE under a more grounded enemy show. We exhibit a

propelled development also, demonstrate it is secure under RDoC show, in which no less than one of the KU-CSPs is thought to be straightforward. Subsequently, regardless of whether a renounced client and both of the KU-CSPs connive, it can't enable such client re-to acquire his/her decrypt ability. At long last, we give broad test results to illustrate the effectiveness of our proposed development.

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.