IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

Crossbreed-Identity based Encryption (C-IBE) with Outsourced Abolishment in Cloud Computing

Ashwini Sajjanrao Bhosale[1], S.T. Singh[1]

Department of Computer Engineering, P K Technical Campus, Kadachiwadi, Near Chakan, Shikrapur Road, Pune[1]

Abstract: IBE (Identity-Based Encryption) simplifies the public key and certificates management at public key infrastructure is an important alternative public key encryption. One of the main efficiency drawbacks of IBE. is the overhead computation at private key generator during user abolishment? We introduce outsourcing computation into IBE for the first time and propose a revocable identity based Encryption. In the server-aided setting. our scheme offloads most of the key generation related operations during key-issuing and key update process to an on a key update cloud service provider. leaving only a constants number of simple operations for private key generator. This goal achieved by utilizing a novel collusion-resistant technique. We exercise a hybrid private key for each user. In cloud computing systems, there are two main research problems which we studied recently such as efficient IBE revocation and security enhancement in IBE method. By considering both research problems, in this project we proposed hybrid approach to deliver both efficient revocation and enhanced security. This hybrid approach is combination of two well know security techniques such as IBE and ABE. The ABE method is combined with IBE to achieve the strong security against different threats. Along with user identity, his/her attributes like country or kind of subscription he/she has are used for further process of IBE encryption, decryption and revocation. Another problem of efficient identity revocation is further addressed by presenting the outsourcing computation into hybrid IBE (H-IBE) method at server aided settings. In H-IBE, the key generation processing's handled during the process of key issuing and key update to the KU-CSP (key update cloud service provider) by leaving fixed number of easy processing's for PKG as well as users to perform locally. The new collusion resistant approach is proposed in this project to achieve the efficient revocation. The practical work is performed by creating different number of cloud users for file upload and downloads processing using proposed C-IBE method.

Index Terms: ABE, C-IBE, KU-CSP, PKG.

I. INTRODUCTION

IBE (Identity-Based Encryption) is a tempestuous substitute to public key encryption, which is projected to make simpler key managing in a certificate-basedPublic Key Infrastructure (PKI) by using human-intelligible characteristics (e.g., unique name, email address, IP address, etc.) as public keys. Therefore, sender using Identity Based Encryption does not require for to look up publickey and certificate, but instantly encrypts message significance with receiver's identity. Accordingly, receiver obtaining the private key coupling with the resultant identity from Private Key Generator (PKG) is able to decrypt such cipher text.

However, IBE allows a random string as the public key which is measured as earnable recompense over PKI, it trouble a resourceful revocation tool. Particular, if the private keys of a number of users get compromised, we must offera mean to cancel such users from system. In PKI setting, abolishment mechanism is realized by appending legality periods to certificates or usinginvolved combinations of techniques. On the other hand, the awkward management of certificates is accurately the saddle that IBE strives to improve. As far as we make out, however revocation has been systematically calculated in PKI, few abolishment mechanisms are branded in IBE in tandem with the enlargement 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 abolishment to fix the issue of efficiency and storage overhead described above. A plain 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 techniqueand transmit the private keys back to unrevoked users (using E-mail). However, the plain 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 adverse, in practice the public clouds are likely outside of the same trusted domain of users and are inquiring for users 'particular privacy. For this reason, a challenge on how to design a secure abolishment IBE scheme to reduce the overhead computation at PKG with an CSP is raised. In

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

this paper, we introduce outsourcing computation into IBE abolishment, and formalize the security definition of outsourced revocable IBE for the first time to the best of ourknowledge. 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 un-abolishment users, wepropose a novel collusion-resistant key issuing technique: we employ a crossbreed 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 isable to obtain the identity component and a default time component (i.e., for current time period) fromPKG as his/her private keying key-issuing. Afterwards, in order to maintain decrypt ability, un-abolishment users' needs to periodically request on key-update foretime 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 tocontact with PKG in key-update, in other words, PKG is allowed to be offline after sending the abolishment list to KU-CSP. 2) No secure channel or user authentication is required during key-update between user and KU-CSP. Furthermore, we consider to realize 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 model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction. Identity-based Encryption an IBE scheme which typically involves two entities, PKG and users 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 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 cipher text CT.Decrypt (CT, SKID_): The decryption algorithm is run by receiver, which takes as input the cipher text CTand his/her private key SKID_. It returns a message M or an error.

II. LITERATURE SURVEY

W. Aiello, S. Lodha, and R. Ostrovsky (1998)-The availability of fast and safe Digital Identities is an imperative ingredient for the successful implementation of the public-key infrastructure of the Internet. All digital identity schemes must include a method for revoking someone's digital identity in the case that this identity is stolen (or cancelled) before its expiration date (similar to the cancelation of a credit-cards in the case that they are stolen).

V. Goyal (2007)-A new certificate revocation system is presented. The basic idea is to divide the certificate space into separate partitions, the number of partitions being dependent on the PKI environment. Each partition contains the status of a set of certificates. A partition may either expire or be renewed at the end of a time slot. This is done efficiently using hash chains. We evaluate the performance of our scheme following the framework and numbers used in previous papers. We show that for many practical values of the system parameters, our scheme is more comp ability than the three well known certificate revocation techniques: CRL, CRS and CRT. Our scheme strikes the right balance between CA to directory communication costs and query costs by carefully selecting the number of partitions.

F. Elwailly, C. Gentry, and Z. Ramzan, (2004)-We present two new schemes for efficient certificate revocation. Our first scheme is a direct improvement on a well-known tree-based variant of the NOVOMODO system of Micali. Our second scheme is a direct improvement on a tree-based variant of a multi-certificate revocation system by Aiello, Lodha, and Ostrovsky. At the core of our schemes is a novel construct termed a Quasimodo tree, which is like a Merkle tree but contains a length-2 chain at the leaves and also directly utilizes interior nodes. This concept is of independent interest, and we believe such trees will have numerous other applications. The idea, while simple, immediately provides a strict improvement in the relevant time and communication complexities over previously published schemes.

D. Boneh and M. Franklin (2001)-We propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model assuming an elliptic curve variant of the computational Diffie-Hellman problem. Our system is based on the Weil pairing. We give just definitions for secure identity based encryption schemes and give several applications for such systems.

A. Boldyreva, V. Goyal, and V. Kumar (2008)-The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (reckless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority. We note that this solution does not scale well -- as the number of users increases, the work on key updates becomes a bottleneck. We propose an IBE scheme that significantly improves key-update capability on the side of the trusted party (from linear to logarithmic in the number of users), while staying capability for the users. Our scheme builds on the ideas of the Fuzzy IBE primitive and binary tree data structure, and is provably secure.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

A. Sahai and B. Waters (2005)-In this Authors present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

R. Canetti, B. Riva, and G. N. Rothblum (2011)-In this model, we show a 1-round statistically sound protocol for any log-space uniform \(\mathcal{NC}\, \) circuit. In contrast, in the single server setting all known one-round succinct delegation protocols are computationally sound. The protocol extends the arithemetization techniques of [Goldwasser-Kalai-Rothblum, STOC 08] and [Feige-Kilian, STOC 97].

Next we consider a simplified view of the protocol of [Goldwasser-Kalai-Rothblum, STOC 08] in the single-server model with a non-succinct, but public, offline stage. Using this simplification, we construct two computationally sound protocols for delegation of computation of any circuit C with depth d and input length n, even a non-uniform one, such that the client runs in time n·poly(log(|C|), d). The first protocol is potentially practical and easier to implement for general computations than the full protocol of [Goldwasser-Kalai-Rothblum, STOC 08], and the second is a 1-round protocol with similar complexity, but less efficient server.

III. SYSTEM OVERVIEW

3.1-Problem Statement-As extreme expansion of cloud computing services in real time applications allows end users of cloud to share their data with each other easily. Multi user data sharing should be secure and integrity should be achieved on cloud. To achieve the data security the methods like IBE (Identity Based Encryption), ABE (Attribute Based Encryption) etc. widely used in cloud computing environment.

As per the recent studies, IBE becoming the vital approach forpublic key encryption as it simplifies the process of certificate management and public key at PKI (public key infrastructure). But the problem associated with IBE is extra overhead on private key generator (PKG) for computations required during the user revocation process. To alleviate the problem of efficient revocation widely studied in conventionalPKI environments, however certificates management is resulted into the extra burden for IBE.

In recent study to mitigate the problem of efficient IBE revocation, approach of outsourcing computation is introduced to deliver the efficient IBE revocation. This approach formalized the definition of security by presenting the outsourced revocable IBE. The practical results were showing the efficiency in terms time cost for each operation. However there is still scope of improvement for security as this approach is only based on user identity for security process. This is current research challenge to address.

3.2-Proposed System-We propose the C-IBE method based on outsourcing computation into the attribute based IBE method proposed abolishment technique in which the abolishment functionality assigned to the CSP. The function Keygen, encrypts, decrypt, abolishment, key update, are design, modified and implemented. The purpose of this project is to present improved scheme for cloud data security and efficient revocation by considering outsourcing computation and user attributes.

IV. CONCLUSION

We exposition another technique called as Crossbreed-Identity based Encryption, to address the Identity based Encryption related issues. In this venture primary objective is to beat the ebb and flow investigate issue of effective disavowal while enhancing the security level of IBE technique. We proposed the C-IBE technique in light of outsourcing calculation based into the Attribute IBE strategy. Notwithstanding this, proposed the abolishment procedure in which the repudiation functionalities are allocated to CSP. The capacities Keygen, encode(encrypt), decode(decrypt), deny and key overhaul are outlined, adjusted and executed in this paper. The execution is assessed to guarantee the perfectibility proposed strategy. The renouncement productivity is enhanced by 40.

REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, “Fast digital identity revocation, “inAdvances 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: Efficientcertificate validation and revocation,” in Public Key CryptographyPKC 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 theweil 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,” inAdvances in Cryptology EUROCRYPT 2005, ser. Lecture Notes inComputer 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.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 12, December 2016

[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsourcecryptographic 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 linearalgebra 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-keyencryption scheme," in Advances in Cryptology EUROCRYPT 2003,ser. Lecture Notes in Computer Science, E. Biham, Ed. SpringerBerlin / Heidelberg, 2003, vol. 2656, pp. 646–646.