ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Implementation of Identity-Based Encryption in Cloud Computing

Sudha Rani Nareddy
M.Tech (CSE)
Vignana Bharathi Institute of Technology.

Rajasekhar Jelli
Assistant Professor,
Vignana Bharathi Institute of Technology.

ABSTRACT:

Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address.

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 paper, 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: 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 recently formulized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

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

Introduction

Identity-Based Encryption (IBE) is an exciting substitute to public key encryption, which is projected to make simpler key managing in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible characteristics (e.g., unique name, email address, IP address, etc) as public keys. Therefore, sender with IBE does not call for to look up public key and certificate, but openly encrypts significance with receiver’s identity. Consequently, receiver obtaining the private key connected with the resultant identity from Private Key Generator (PKG) is able to decrypt such cipher text. However IBE allows an random string as the public key which is measured as likable recompense over PKI, it anxiety a resourceful revocation instrument. Expressly, if the private keys of a number of users get compromised, we must offer a mean to cancel such users from system. In PKI setting, revocation mechanism is realized by appending legality periods to certificates or using involved 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 revocation 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 revocation to fix the issue of efficiency and storage overhead described above. A naïve 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 entrusted 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 keying key-issuing. Afterwards, in order to maintain decrypt ability, unrevoked 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 [4], 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 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 (RDoC) model [7]. 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 (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 cipher text CT.Decrypt (CT,SKID_) : The decryption algorithm is run by receiver, which takes as input the cipher text CT and his/her private key SKID_. It returns a message M or an error.

EXISTING SYSTEM:

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.

Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period.
Hanaoka et al. proposed a way for users to periodically renew their private keys without interacting with PKG.
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 is the number of revoked users.

DISADVANTAGES OF EXISTING SYSTEM:

- Boneh and Franklin 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.
- Boneh and Franklin's suggestion is more a viable solution but impractical.
- In Hanaoka et al system, however, the assumption required in their work is that each user needs to possess a tamper-resistant hardware device.
- 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.

PROPOSED SYSTEM:

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 keyupdate, leaving only a constant number of simple operations for PKG and eligible users to perform locally.

In our scheme, as with the suggestion, 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 decryptability, unrevoked users needs to periodically request on keyupdate for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP).

ADVANTAGES OF PROPOSED SYSTEM:

- 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 with the aid of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKGis allowed to be offline after sending the revocation list to KU-CSP.
- 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.

SYSTEM ARCHITECTURE:

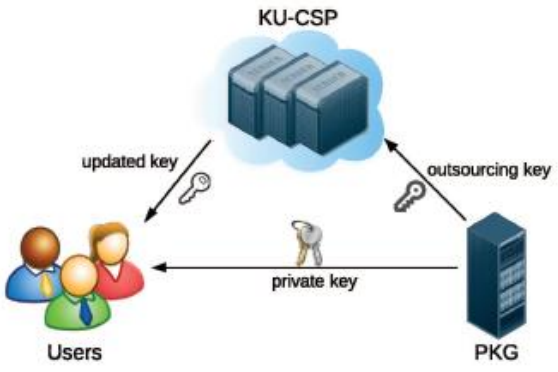

Fig. 1. System Model for IBE with Outsourced Revocation

Proposed Approach

Any application development follows the some software In this paper, intend at tackling the significant matter of identity revocation, we initiate outsourcing subtraction into IBE for the first time and put forward a revocable IBE format in the server-aided scenery. Our system off-load mainly of the key making related operations throughout key-issuing and key-update processes to a Key Update Cloud Service Provider, leave-taking only a invariable amount of simple functions for PKG and users to make locally. This goal is attain by operate a novel collusion-resistant technique: we occupy a hybrid private key for each user, in which an AND gate is implicated to connect and vault the identity constituent and the time constituent. Furthermore, we recommend another assembly which is verifiable protected under a moment ago formulized Refereed Delegation of Computation model. Finally, we present general investigational consequences to make obvious the effectiveness of our proposed edifice. ADVANTAGES it achieves constant competence for both calculation at PKG and private key size at user; User desires not to contact with PKG throughout key-update, in additional, PKG is permitted to be offline after conveyance the revocation list to KU-CSP,No protected canal or user confirmation is required during key-update among user and KU-CSP. The proposed approach is shown in Figure1.

Implementation:

Data Users:

In this module the data user can register with cloud server to access file search, file upload and download...

Data owner:

In this module the data owner can register to maintain their file into cloud server and allow access to data users to access the file.

File search:

In this module user can search needed file to download with proper key.

File upload:

User can upload their file into cloud server with high level security system.

File download:

In this module the user can download file with proper key which provided by data owner.

Conclusion

In this paper, center of attention on the significant concern of identity revocation, we initiate outsourcing division into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the projected IEEE TRANSACTIONS ON COMPUTERS format is full-featured: 1) It realize constant competence for both calculation at PKG and private key size at consumer; 2) User desires not to drop a line to with PKG in key-update, in other words, PKG is permitted to be offline after transfer the revocation list to KU-CSP; 3) No protected channel or user verification is required in key-update between user and KU-CSP. In addition, we think about to apprehend revocable IBE under a stronger opposition model. We present a sophisticated construction and demonstrate it is protected under RDoC model, in which at least one of the KU-CSPs is implicit to be honest. Therefore, even if a revoked user and each of the KU-C SPs collude, it is not capable to help such user re-obtain his/her decrypt capability.

Finally, we offer general tentative results to lay bare the competence of our anticipated construction.

REFERENCES

[1]Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, Senior Member, IEEE, “Identity-Based Encryption with Outsourced Revocation in Cloud Computing”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 2, FEBRUARY 2015.

[2]V. Goyal, “Certificate revocation using fine grained certificate s pace partitioning,” in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dh amija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247–259.

[3]F. Elwailly, C. Gen try, and Z. Ramzan, “Quasimodo: Efficien t certificate validation and revocation,” in Pu blic Key Cryptography PKC 2004, ser. Lectu re Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / H eidelberg, 2004, vol. 2947, pp. 375–388.

[4]D. Boneh and M. Fr anklin, “Identity -based encryption from the weil pairing,” in Advances in Cryptol ogy – CRYPTO 2001 , ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 2 13–229.

[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.