International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Identity-based cryptography with Outsourced Revocation in Cloud Computing

[1]Gaddipathi Bharathi, [2]Kota Sureshbabu
[*1]Associate Professor, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India
[2]PG Student, Department of MCA, St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

ABSTRACT

Identity-Based Encryption (IBE), which make simple to the public key and credential management at Public Key Infrastructure (PKI) is a significant option to public key encryption. However, one of the most important competence drawbacks of IBE is the transparency calculation at Private Key Generator (PKG) throughout user revocation. Well-organized revocation has been well intentional in conventional PKI setting, but the burdensome executive of certificates is accurately the trouble that IBE strives to improve. In this paper, aiming at tackling the significant concern of identity revocation, we set up outsourcing addition into IBE for the first time and recommend a revocable IBE proposal in the server-aided setting. Our proposal off-load the majority of the key making interrelated operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, departure only a regular number of operations for PKG and users to make locally. This goal is accomplish by exploit a novel collusion-resistant procedure: we take up a hybrid private key for every user, in which an AND gate is complicated to bond and jump the individuality component and the time constituent. Additionally, we suggest another creation which is incontestable secure under the Refereed Delegation of Computation model. In conclusion, we offer extensive untried results to express the efficiency of our projected construction.

Keywords: Identity-Based Encryption, Revocation, Outsourcing, Computing

I. 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 a 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 are 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 $\in \{0, 1\}*$. 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 cipher text *CT*.Decrypt (*CT*,*SK*ID_) : The decryption algorithm is run by receiver, which takes as input the cipher text *CT* and his/her private key *SK*ID_ . It returns a message *M* or an error.

II. Literature Survey

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, DISADVANTAGS are: However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation.

2.1 Revocable IBE

Introduced by and firstly implemented by Boneh and Franklin as well as IBE has been researched intensively in cryptographic community On the aspect of construction, these first schemes were proven secure in random oracle. Some subsequent systems achieved provable secure in standard model under selective-ID Security or adaptive-ID security. Recently, there have been multiple lattice-based constructions for IBE Systems

Nevertheless, concerning on revocable IBE, there is little work Presented. As mentioned before, Boneh and Franklin's suggestion is more a viable solution but impractical. Hanaoka et al. proposed a way for users to periodically renew their private keys without interacting with PKG. However, the assumption required in their work is that each user needs to possess

a tamper-resistant hardware device. Another solution is mediator-aided revocation

In this setting there is a special semi-trusted third party called a mediator who helps users to decrypt each cipher text. 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. Recently, Lin et al.proposed a space efficient revocable IBE mechanism from non-monotonic Attribute- Based Encryption (ABE), but their construction requires $O(r)$ times bilinear pairing operations for a single decryption where is the number of revoked users.

2.2 Other Revocation Technique

The authors utilized proxy re-encryption to propose a revocable ABE scheme. The trusted authority only needs to update master key according to attribute revocation status in each time period and issue proxy re-encryption key to proxy servers. The proxy servers will then re-encrypt cipher text using the re-encryption key to make sure all the unrevoked users can perform successful decryption. We specify that a third party service provider is introduced in both Yu et al. and this work. Differently, Yu et al. utilized the third party (work as a proxy) to realize revocation through encrypting cipher text which is only adapt to the special application that the cipher text is stored at the third party. However, in our construction the revocation is realized through updating private keys for unrevoked users at cloud service provider which has no limits on the location of cipher text.

2.3 Outsourcing Computation

The problem that how to securely outsource different kinds of expensive computations has drawn considerable attention from theoretical computer science community for a long time. Chaum and Pedersen firstly introduced the notion of wallets with observers, a piece of secure hardware installed on the client's computer to perform some expensive computations. Attalla et al. presented a framework for secure outsourcing of scientific computations such as matrix multiplication and quadrature. Nevertheless, the solution used the disguise technique and thus leaded to leakage of private information. Rosenberger and Lysyanskaya proposed the first outsource-secure algorithm for modular exponentiations based on pre-computation and serve raided computation. Atallah and Li investigated the problem of computing the edit distance between two sequences and presented an efficient protocol to securely outsource sequence comparison with two servers. Furthermore, Benjamin and Atallah addressed the problem of secure outsourcing for widely applicable linear algebraic computations. Nevertheless, the proposed protocol

Required the expensive operations of homomorphism encryption. Attalla and Frikken further studied this problem and gave improved protocols based on the so-called weak secret hiding assumption. Chen et al. made an efficiency improvement on the work and proposed a new scheme for outsourcing single/simultaneous modular exponentiations.

III. 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.

3.1 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.

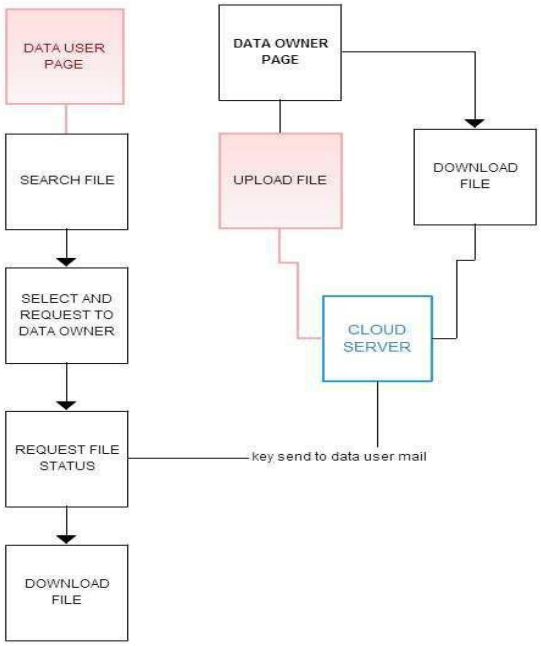


Figure 1 : Proposed Approach

3.2 Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple.

3.3 Objectives

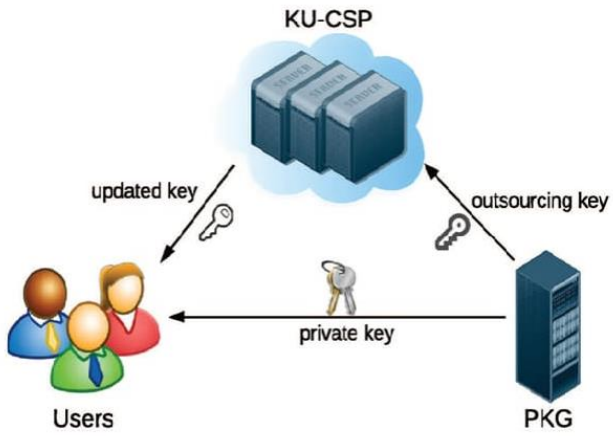
Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

3.4 Output Design

A quality output is one, which meet s the requirements of the end user and presents the information clearly. In any system, results of processing are communicated to the users and to other system through outputs. In output design, it is determined how the information is to be displaced for immediate need and the hard copy output. It is the most important t and direct source information to the user. Efficient not and intelligent output design improves the system m's relationship to help user decision-making. De signing computer output should proceed in an organized, well thought out manner; the right output must b e developed while ensuring that each output element is designed so that people will find the system ca n use easily and effectively.

When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.. Select meth ods for presenting information..Create document, report, or other formats that contain information produced by the system. The output form of an i nformation system should accomplish one or more of the following objectives. Convey information about past activities, current status or projections of the Future. Signal important events, opportunities, problems, or warnings. Trigger an action. Confir m an action.

3.5 System Architecture



1. The DFD is also called as bu bble chart. It is a simple graphical formalism th at can be used to represent a system in terms o f input data to the system, various processing c arried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These co mponents are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the sys tem.
3. DFD shows how the informati on moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow a nd the transformations that are applied as data moves from input to output.
4. DFD is also known as bub ble chart. A DFD may be used to represent a s ystem at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

IV. CONCLUSION

In this paper, center of attent ion 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; User desires not to drop a li ne to with PKG in key-update, in other words, PKG is permitted to be offline after transfer the revocation l ist to KU-CSP; 3) No protected channel or user veri fication 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. Therefo re, 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 competenc e of our anticipated construction.

V. REFERENCES

[1]. W. Aiello, S. Lodha, a nd R. Ostrovsky, "Fast digital identity revoc ation," in Advances in Cryptology - CRYPTO ’98 . Springer, 1998.

[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.