International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

IB Encryption ON Cloud Data Outsourcing computing by user Revocation

B.KALYAN BABU [1]& Ms.L.Sunitha Rani [2]

[1]M-Tech,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

[2]Asst.Professor,Dept. of CSE Geethanjali College of Engineering & Technology, Kurnool, AP

ABSTRACT

Identity-Predicated Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is a consequential alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Engenderer (PKG) during utilizer revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the encumbrance 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-availed setting. Our scheme offloads most of the key generation cognate operations during key-issuing and key-update processes to a Key Update Cloud Accommodation 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 utilizer, 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. Conclusively, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Keywords: -Cloud computing,IB Encryption, Revocation, Data Outsourcing.

1. INTRODUCTION

In this paper, fixating on the critical issue of identity revocation, we introduce outsourcing computation into IBE and propose a revocable scheme in which the revocation operationsare delegated to CSP. With the avail of KU-CSP, the proposed scheme is plenary-featured: It achieves constant efficiency for both computation at PKG and private key size at utilizer needs not to contact with PKG during key-update, in other words, PKG is sanctioned to be offline after sending the revocation list to KU-CSP No secure channel or utilizer authentication is required during key-update between utilizer and KU-CSP. Another work cognate to us originates from Yu et al. The authors utilized proxy re-encryption to

propose a revocable ABE scheme. The trusted ascendancy only needs to update master key according to attribute revocation status in each duration and issue proxy re-encryption key to proxy servers. The proxy servers will then re-encrypt ciphertext utilizing the re-encryption key to ascertain all the unrevoked users can perform prosperous decryption. We designate that a third party (proxy) accommodation provider is introduced in both Yu et al. and this work. However, in our construction the revocation is realized through updating private keys for unrevoked users at cloud accommodation provider which has no circumscriptions on the location of ciphertext.

2. RELATED WORK

Subsisting system

Identity-Predicated Encryption (IBE) is a fascinating alternative to public key encryption, which is proposed to simplify key management in a certificate-predicated Public Key Infrastructure (PKI) by utilizing human-intelligible identities (e.g., unique denomination, electronic mail address, IP address, etc) as public keys. Boneh and Franklin suggested that usersinstaurate their private keys periodically and senders utilize the receivers' identities concatenated with current duration. Hanaoka et al. proposed a way for users to periodically instaurate their private keys without interacting with PKG. Lin et al. proposed a space efficient revocable IBE mechanism from non-monotonic Attribute-Predicated Encryption (ABE), but their construction requires times bilinear pairing operations for a single decryption where is the number of revoked users.

Advantages

The Boldyreva, Goyal and Kumar presented a revocable IBE scheme. Their scheme is built on the conception of fuzzy IBE primitive but utilizing a binary tree data structure to record users' identities at leaf nodes. Ergo, key-update efficiency at PKG is able to be significantly reduced from linear to the height of such binary tree (i.e. logarithmic in the number of users). Nevertheless, we point out that though the binary tree prelude is able to achieve a relative high performance.

Disadvantages:

It will result in other quandaries:

1) PKG has to engender a key pair for all the nodes on the path from the identity leaf node to the root node, which results in involution logarithmic in the number of users in system for issuing a single private key.

2) The size of private key grows in logarithmic in the number of users in system, which makes it arduous in private key storage for users.

3) As the number of users in system grows, PKG has to maintain a binary tree with a substantial amount of nodes, which introduces another bottleneck for the ecumenical system.

As far as we ken, though revocation has been exhaustively studied in PKI, few revocation mechanisms are kenned in IBE setting. In Boneh and Franklin suggested that usersinstaurate their private keys periodically and senders utilize the receivers' identities concatenated with current duration. But this mechanism would result in an overhead load at PKG. 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. 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. For this reason,a challenge on how to design a secure revocable IBE scheme to reduce the overhead computation at PKG with an untrusted CSP is raised.

Propose 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 erudition. We propose a scheme to offload all the key generation cognate 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 that we realize revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates duration 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 utilizer, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component. At first, utilizer is able to obtain the identity component and a default time component (i.e., for current duration) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decrypt facility, unrevoked users needs to periodically request on key-update for time component to an incipiently introduced entity designated Key Update Cloud Accommodation Provider (KU-CSP). Compared with the antecedent 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.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

3. IMPLEMENTATION

Users:

In this system Users will be register and they will encrypt the files with receiver ID (i.e Email) and send to receiver. As well as when any utilizer revoked at timeperiod, each unrevoked utilizer needs to send key update request to KU-CSP (KeyUpdate Cloud Accommodation Provider) to maintain decrypt facility. The Receiver will decrypt the data utilizing of his Private Key which is engendered by PKG (Private Key Engenderer).

PKG (Private Key Engenderer):

In this system PKG will engender the Private Keys for all sanctioned Users and as well as send Outsourcing Key to KU-CSP. If any Utilizer compromised by Assailant then PKG will Revoke that Utilizer i.e. he can update the time component only for not accessing any resources which is sent to Him.

KU-CSP (Key Update Cloud Accommodation Provider):

In this system KU-CSP will be update upon receiving a key update request on ID, KU-CSP firstly checks whether ID subsists in the Revocation List (RL) , if so KU-CSP does not perform Key Updating process, Otherwise KU-CSP fetches Updated Key and send to Utilizer.

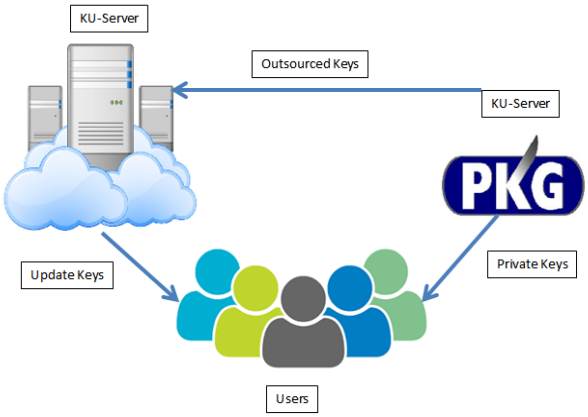

Fig: 1 System Model for IBE with Outsourced Revocation

4. EXPERIMENTAL RESULTS

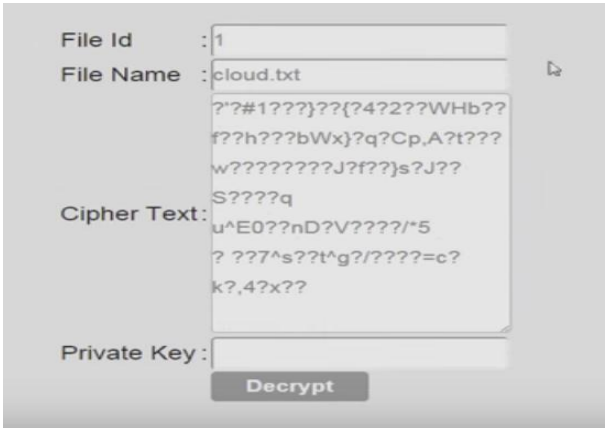

Fig 2: File Upload with Encryption.

Fig 3: Out Sourced Data

5. CONCLUSION

This paper formalizes the IBE system model and security model. IBE protocol works efficiently in multi cloud environment. Besides of the elimination of certificate management, our ID-DPDP protocol has adscititiously flexibility and high efficiency. Concurrently, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification predicated on the client's sanction.

6. REFERENCES

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on June. 3rd, 2009.

[2] G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and Efficient Provable Data Possession", SecureComm 2008, 2008.

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,D. Song, "Provable Data Possession at Untrusted Stores", CCS'07, pp.598-609, 2007.

[4] C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia, "DynamicProvable Data Possession", CCS'09, pp. 213-222, 2009.

[5] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, J.Quisquater, "Efficient Remote Data Integrity checking in Critical InformationInfrastructures", IEEE Transactions on Knowledge and DataEngineering, 20(8), pp. 1-6, 2008.

[6] H.Q. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, 2012.

[7] Y. Zhu, H. Hu, G.J. Ahn, M. Yu, "Cooperative Provable Data Possessionfor Integrity Verification in Multicloud Storage", IEEE Transactions on Parallel and Distributed Systems, 23(12), pp. 2231-2244, 2012.

[8] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds", CCS'10, pp. 756-758, 2010.

[9] R. Curtmola, O. Khan, R. Burns, G. Ateniese, "MRPDP: Multiple-Replica Provable Data Possession", ICDCS'08, pp. 411-420, 2008.

[10] A. F. Barsoum, M. A. Hasan, "Provable Possessionand Replication of Data over Cloud Servers", CACR,University of Waterloo, Report2010/32,2010.