isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 3 Apr,2017,ISSN_NO: 2321-3337

EFFICIENT REVOCATION IN CLOUD COMPUTING USING IBE (IDENTIFY BASED ENCRYPTION)

[1]E.Sam Jebasingh ,[2]R.Vijey Raj Jude
1(Information Technology, Loyola Institute of Technology, Chennai)
(Email: samjebasingh007@gmail.com)
2(Information Technology, Loyola Institute of Technology, Chennai)
(Emial: vijeyrajjude@gmail.com)

.

ABSTRACT - *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 : PKG, IBE, PKI ,CLOUD, KU-CSP

1.INTRODUCTION

Cloud computing has been coined as an umbrella term to describe a category of sophisticated on-demand computing services initially offered by commercial providers, such as Amazon, Google, and Microsoft. It denotes a model on which a computing infrastructure is viewed as a cloud from which businesses and individuals access applications from anywhere in the world on demand. The main principle behind this model is offering computing, storage, and software “as a service. In addition to raw computing and storage, cloud computing providers usually offer a broad range of software services. They also include APIs and development tools that allow developers to build seamlessly scalable applications upon their services. Indeed, the long-held dream of delivering computing as a utility has been realized with the advent of cloud computing. Cloud computing provides software as a service (saas), Platform as a service(paas), Infrastructure

as a service(Iaas). Cloud provides feature such as pay for usage (metering and billing), elasticity, self service, and customization. Further cloud provides deployment models such as Private cloud, Public cloud, Hybrid cloud. The important feature offered by the cloud is the users data resides anywhere in the world and which can be operated remotely in unknown machine by the user. In the day-to-day life the organizations produce large amount of data. The interest thing in cloud computing has been motivated by many factors such as the low cost of system hardware, the increase in computing power and storage capacity and the massive growth in data size generated by digital media(images, video, audio), Web authoring, scientific instruments, physical simulations,etc. To this end, still the main challenge in the cloud is how to effectively store, query, analyze, and utilize these immense datasets.

2, SYSTEM ANALYSIS

2.1 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.

2.2 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 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, 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).

2.2.1 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 thatwith 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.

3. IMPLEMENTATION

3.1 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 : The setup algorithm takes as input a security parameter and outputs the public key and the master key . Note that the master key is kept secret at PKG. KeyGen : The private key generation algorithm is run by PKG, which takes as input the master key and user's identity

Encrypt : The encryption algorithm is run by sender, which takes as input the receiver'sidentity and a message to be encrypted. It outputs the cipher text .

Decrypt : The decryption algorithm is run by receiver, which takes as input theciphertextand his/her private key . It returns a message or an error .

3.2 Efficient IBE with outsourced revocation :

We utilize a "hybrid private key" for each user in our system, which employs an AND gate connecting two sub-components namely the identity component and the time component respectively. is generated by PKG in key-issuing but is updated by the newly introduced KU-CSP in keyu pdate; In encryption, we take as input user's identity as well as the time period to restrict decryption, more precisely, a user is allowed to perform successful decryption if and only if the identity and time period embedded in his/her private key are identical to that associated with the cipher text.

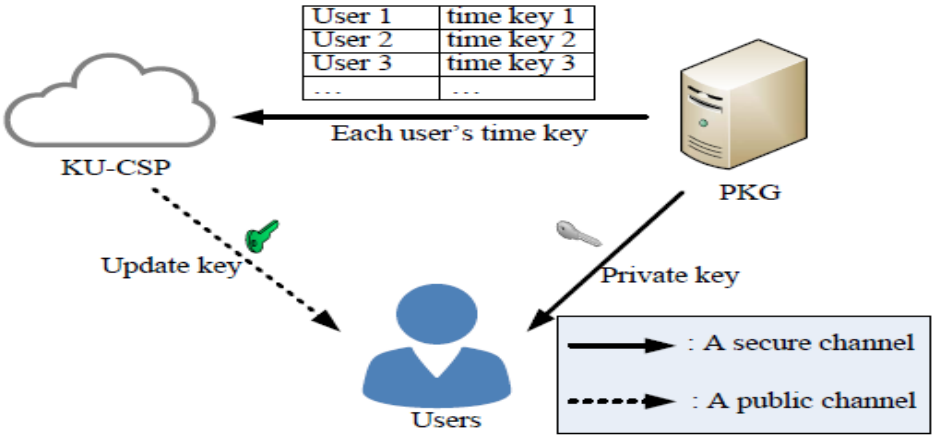
3.3 Key Service Procedures:

Based on our algorithm construction, the key service procedures including key-issuing, key-update and revocation in proposed IBE scheme with outsourced revocation work asfollows. Key-issuing. We require that PKG maintains a revocation list and a time list locally. Upon receiving a private key request on , PKG runs Key Gen to obtain private key and outsourcing key . Finally, it sends to user and ( ) to KUCSP respectively. As described in intuition, for each entry ( ) sent from PKG, KU-CSP should add it into a locally maintained user list . Key-update. If some users have been revoked at time period , each unrevoked user needs to send key-update request to KU-CSP to maintain decryptability.

3.4 Advanced Construction:

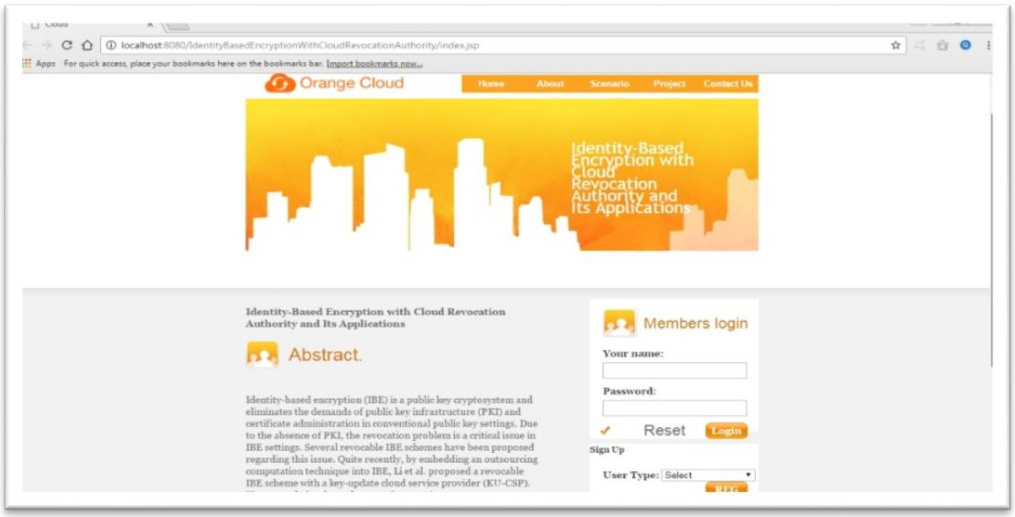
RDoC model originates from the model of refereed games , and is later formalized. In RDoC model, the client is able to interact with multiple servers and it has a right output as long as there exists one server that follows the proposed protocol. One of the most advantages of RDoC over traditional model with single server is that the security risk on the single server is reduced to multiple servers involved in. As the result of both the practicality and utility, RDoC model recently has been widely utilized in the literature of outsourced computation. In order to apply RDoC to our setting, we introduce another independent KU-CSPs.

3.5. System Architecture:

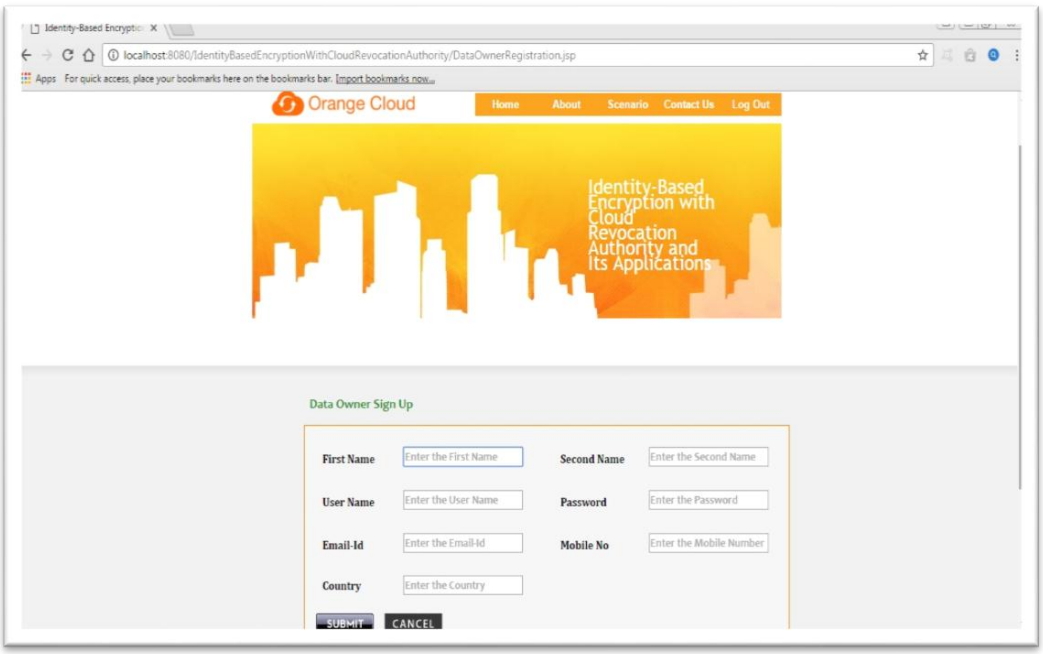


4. OUTPUT:

4.1 HOME PAGE:



4.2 DATA OWNER SING-UP



5. CONCULSION AND FUTUREWORK:

In this paper, focusing on the critical issue of identity revocation, we introduce outsourcing computation into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the proposed scheme is full-featured: 1) It achieves constant efficiency for both computation at PKG and private key size at user; 2) User needs not to contact with PKG during keyupdate, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP; 3)Nosecure channel or user authentication is required during key-update between user and KU-CSP. Furthermore, we consider to realize revocable IBE under a stronger adversary model. We present an advanced construction and show it is secure underRDoCmodel, in which at least one of the

KU-CSPs is assumed to be honest. Therefore, even if a revoked user and either of the KU-CSPs collude, it is unable to help such user re-obtain his/her decryptability. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

REFERENCES

#1. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology (CRYPTO'98). New York, NY, USA: Springer, 1998, pp. 137–152.

#2. V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security, S. Dietrich and R. Dhamija, Eds. Berlin, Germany: Springer, 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'04), F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany: Springer, 2004, vol. 2947, pp. 375–388.

#4. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology (CRYPTO '01), J. Kilian, Ed. Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.

#5. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15thACMConf. Comput. Commun. Security (CCS'08), 2008, pp. 417–426.

#6. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557–557.

BIOGRAPHY

E.Sam Jebasingh,B.Tech.Information Technology,Final Year,Loyola Institute of Technology,Chennai-123.

R.Vijey Raj Jude,B.Tech.Information Technology,Final Year,Loyola Institute of Technology,Chennai-123.