INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 6 (2016) PAGES 1336 - 1340
RECEIVED : 29/10/2016. PUBLISHED: 7/11/2016
November 7, 2016

# IDENTITY-BASED ENCRYPTION WITH EFFICIENT REVOCATION FOR CLOUD SERVICE PROVIDER IN CLOUD COMPUTING

[1]Nadar Deepika Karthesan, [2]Dr.T.Priyaradhikadevi,

[1]PG scholar, Dept of CSC, Mailam College of Engineering, Villupuram

[2]HOD/CSE, Mailam College of Engineering, Villupuram.

## Abstract:

Cloud computing, the imminent need of computing as a finest utility has the latent to take an enormous leap in the IT industry, is structured and put to optimal use with regard to the current tendency. Identity-Based Encryption (IBE) which abridges the public key and certificate management at Public Key Infrastructure (PKI) is an imperative substitute to public key encryption. One of the main resourceful negative aspects of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in usual PKI locale, but the unwieldy management of certificates is exactly the trouble that IBE endeavour to lessen. Aiming at tackling the decisive concerns of identity revocation, it is commenced the outsourcing computation into IBE for the first time and recommended a revocable IBE scheme in the server-aided setting. Present scheme offloads the majority of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant numeral of simple operations for PKG and users to carry out locally. This objective is achieved by utilizing a novel collusion-resistant technique that has been employed a hybrid private key for each user, in which an AND gate is concerned to connect and leap the identity component and the time component. Discussed another construction which is provable secure under the recently formulized Refereed Delegation of Computation model.

Keywords: Identity-based encryption (IBE), Revocation, Outsourcing, IBE Scheme, Private Key Generator.

## 1. INTRODUCTION

Computing is being transformed to a model consisting of services that are commoditized and delivered in a manner similar to utilities such as water, electricity, gas, and telephony.

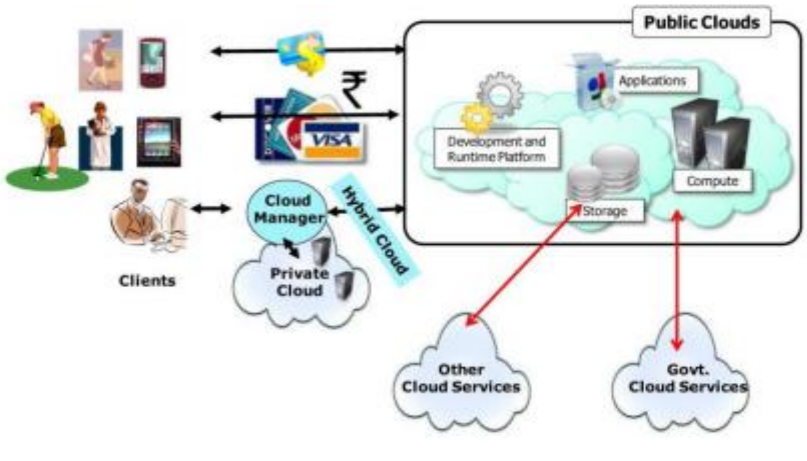

**Fig.1. A bird‟s eye view of Cloud computing**

In such a model, users access services based on their requirements regardless of where the services are hosted. Several computing paradigms have promised to deliver this utility computing vision. Cloud computing is the most recent emerging paradigm promising to turn the vision of "computing utilities" into reality. A service offering computation resources is frequently referred to as Infrastructure as a Service (IaaS) and the applications as Software as a Service (SaaS)[1]. An environment used for construction, deployment, and management of applications is called PaaS (Platform as a Service). Cloud computing delivers infrastructure, platform, and software (application) as services, which are made available as subscription-oriented services in a pay-as-you-go model to consumers. The price that CSPs (Cloud Service Providers) charge depends on the quality of service (QoS) expectations of CSCs (Cloud Service Consumers).Cloud computing fosters elasticity and seamless scalability of IT resources that are offered to end users as a service through the Internet. Cloud computing can help enterprises improve the creation and delivery of IT solutions by providing them with access to services in a cost-effective and flexible manner.A public Cloud is made available in a pay-as-you-go manner to the general public users irrespective of their origin or affiliation. A private Cloud"s usage is restricted to members, employees, and trusted partners of the organization. A hybrid Cloud enables the use of private and public Cloud in a seamless manner. Cloud computing applications span many domains, including business, technology, government, health care, smart grids, intelligent transportation networks, life sciences, disaster management, automation, data analytics, and consumer and social networks. Various models for the creation, deployment, and delivery of these applications as Cloud services have emerged.

## 2. PROBLEM STATEMENT

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 selectiveID security or adaptive-ID security. Recently, there have been multiple lattice-based constructions for IBE systems. 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 ciphertext[9].

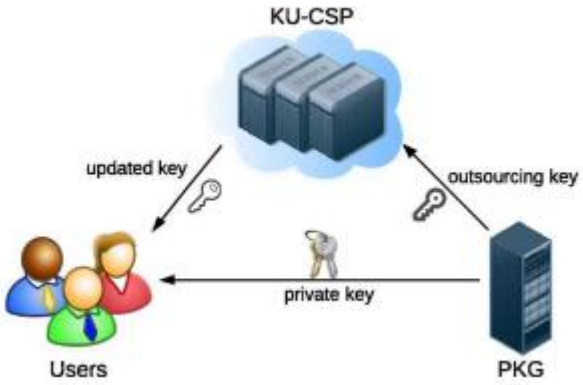

**Fig.2. .System model for IBE with outsourced revocation**

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 times bilinear pairing operations for a single decryption where is the number of revoked users[10]. Libert and Vergnaud improved Boldyreva‟s construction to achieve adaptive-ID security. Their work focused on security enhanced, but inherits the similar disadvantage as Boldyreva‟s original construction. They are short in storage for both private key at user and binary tree structure at PKG. We present system model for outsourced revocable IBE . Compared with that for typical IBE scheme, a KU-CSP is involved to realize revocation for compromised users. The KU-CSP can be envisioned as a public cloud run by a third party to deliver basic computing capabilities to PKG as standardized services over the network. Typically, KU-CSP is hosted away from either users or PKG, but provides a way to reduce PKG computation and storage cost by providing a flexible, even temporary extension to infrastructure [11]. When revocation is triggered, instead of re-requesting private keys from PKG, in unrevoked users have to ask the KUCSP for updating a lightweight component of their private keys. Though many details are involved in KU-CSP‟s deployment, logically envisioned it as a computing service provider, and concern how to design secure scheme with an untrust KU-CSP. The challenge in designing the outsourced revocable IBE scheme is how to prevent collusion between Bob and other unrevoked dishonest users. Specifically, a dishonest user can share her updated time component [11].

## 3. PROPOSED SYSTEM

In order to achieve efficient revocation, we introduce the idea of “partial private key update” into the proposed construction, which operates on two sides: 1) Utilized “hybrid private key” for each user in our system, which employs an AND gate connecting two sub-components namely the identity component (IK) and the time component respectively(TK)[12]. IK is generated by PKG in key-issuing but is updated by the newly introduced KU-CSP in key update; 2) In encryption, we take as input user‟s identity as well as the time period T 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 ciphertext. Using such skill, we are able to revoke user‟s decryptability through updating the time component for private key by KU-CSP. Moreover, we remark that it cannot trivially utilize an identical updated time component for all users because revoked user is able to re-construct his/her ability through colluding with unrevoked users[8]. To eliminate such collusion, randomly generated an outsourcing key for each identity, which essentially decides a “matching relationship” for the two sub-components [12]. KU-CSP maintain a list UL to record user‟s identity and its corresponding outsourcing key. In key-update, we can use OKID to up date the time component TK[ID]T for identity ID . Suppose a user with identity ID is revoked at Ti . Even if he/she is able to obtain TK[ID`]Ti+1for identity ID` , the revoked user still cannot decrypt ciphertext encrypted under Ti+1. we emphasize that the idea behind our construction is to realize revocation through updating the time component in private key.

## 4. RESULT ANALYSIS

Scheme shares the same setup algorithm with the IBE scheme in key-issuing stage is relative longer than that in the IBE scheme .This is because we embed a time component into each user‟s private key to allow periodically update for revocation, resulting that some additional computations are needed in our scheme to initialize this component. With the fast improvement of adaptable cloud administrations, it turns out to be progressively defenseless to utilize cloud administrations to share information in a companion circle in the distributed computing environment. Since it is not attainable to execute full lifecycle protection security, access control turns into a testing assignment, particularly when we share information on cloud servers. Keeping in mind the end goal to handle this issue, we propose time determined qualities, a novel secure information self-destructing plan in distributed computing. Though, prior the information would not get erased consequently from cloud. In proposed framework the information gets erased from the cloud and space is made.

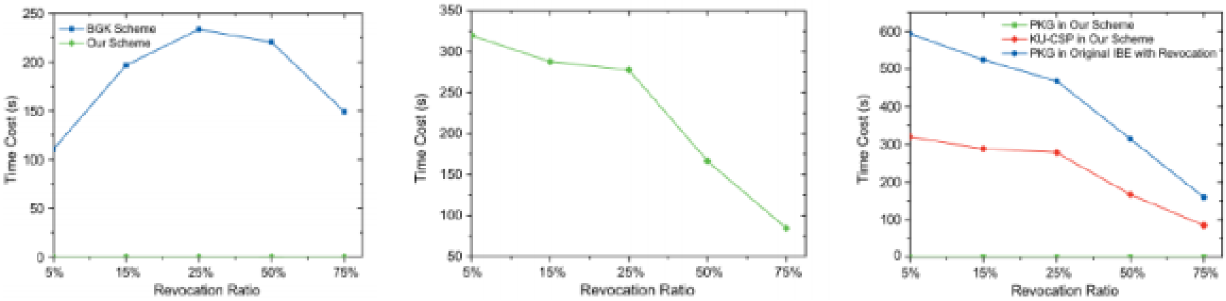

**Fig.3.Result analysis**

Our encryption and decryption is slightly longer than the IBE scheme, which is also due to the existence of the time component[6]. The user needs to perform an additional encryption/decryption for this component, rather than just encrypt/decrypt the identity component. To sum up, our revocable scheme achieves both identity based encryption/decryption and revocability without introducing significant overhead compared to the original IBE scheme.

## CONCLUSION

Here, focusing on the critical issue of identity revocation, outsourcing computation into IBE and proposed a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the present scheme is full featured in achieving steady efficiency for both computation at PKG and private key size at user. Here, User needs not to contact with PKG during key update, even offline feature is available. No secure channel or user authentication is required during key-update between user and KU-CSP. It is an advanced construction and shown that it is secure under RDoC model, in which atleast one of the KU-CSPs is assumed to be honest. Even if a revoked user and either of the KUCSPs collude, it is unable to help such user re-obtain his/her decryptability. An extensive experimental results are provided to demonstrate the efficiency of the present 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. Dietrichand 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 Weilpairing,” in Advances in Cryptology (CRYPTO „01), J. Kilian, Ed.Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.

[5] B. Libert and D. Vergnaud, “Adaptive-id secure revocable identity based encryption,” in Topics in Cryptology (CT-RSA‟09),M. Fischlin,Ed. Berlin, Germany: Springer, 2009, vol. 5473, pp. 1–15.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in Proc. 5th ACM Symp. Inf. Comput.Commun. Security (ASIACCS‟10), 2010, pp. 261–270.

[7] D. Chaum and T. P. Pedersen, “Wallet databases with observers,” inProc. 12th Annu. Int. Cryptology Conf. Adv. Cryptology (CRYPTO‟92),1993, pp. 89–105.