Volume 6, Issue 11, November 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Novel Collusion-Resistant Technique Efficient Revocation on Identity Based Encryption in Cloud Computing

Dr. GVN. Prasad, M. Prashanti, M. Sudarani, Ch. Sandhya
Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology, Ibrahimpatnam, Telangana, India

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 or Identity based encryption is an important primitive of ID-Based Cryptography. It is an important alternative to public key encryption. Identity based encryption which simplifies the public key and certificate management. Propose a revocable Identity based encryption scheme in the server aided setting. It is achieved by utilizing a novel collusion resistant technique which means generating a hybrid private key for every user using AND gate it helps to connect and bound the identity and time component. In this paper aiming at tackling the critical issue of identity revocation we introduced the outsourcing revocation for the first time and the purpose of revocable IBE scheme in server aided sitting. Our scheme offloads most of the generation related operations during key issuing and key update process to a key update cloud service provider, leaving only a constant number of simple operations for PKG and user 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 it gives a secure under the recently formulised refereed delegation of computation model. Finally we provide extensive experimental results to demonstrate the efficiency of our proposed construction***

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

I. INTRODUCTION

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

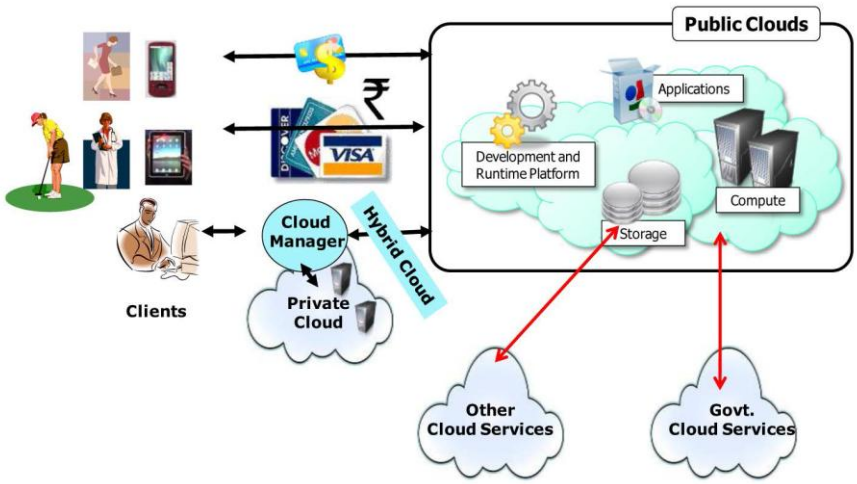


Fig.1: A bird's eye view of Cloud computing

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[2].Clouds can be classified into three categories, depending on their accessibility restrictions and the deployment model. They are:

- Public Cloud,
- Private Cloud, and
- Hybrid Cloud.

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. Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string[3]. A trusted third party, called the private key generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key. Given the master public key, any party can compute a public key corresponding to the identity *ID* by combining the master public key with the identity value[4]. To obtain a corresponding private key, the party authorized to use the identity *ID* contacts the PKG, which uses the master private key to generate the private key for identity *ID*. Let us have a glance on limitations of Identity-based systems. Identity-based systems have a characteristic problem in operation. Suppose Alice and Bob are users of such a system. Since the information needed to find Alice's public key is completely determined by Alice's ID and the master public key, it is not possible to revoke Alice's credentials and issue new credentials without either (a) changing Alice's ID (usually a phone number or an email address which will appear in a corporate directory); or (b) changing the master public key and re-issuing private keys to all users, including Bob[4].This limitation may be overcome by including a time component in the identity. Identity-based encryption (IBE), is an imperative primeval of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g. the text-value of the receiver's name or email address as a key. The receiver obtains its decryption key from a central authority, which needs to be trusted as it generates secret keys for every user.

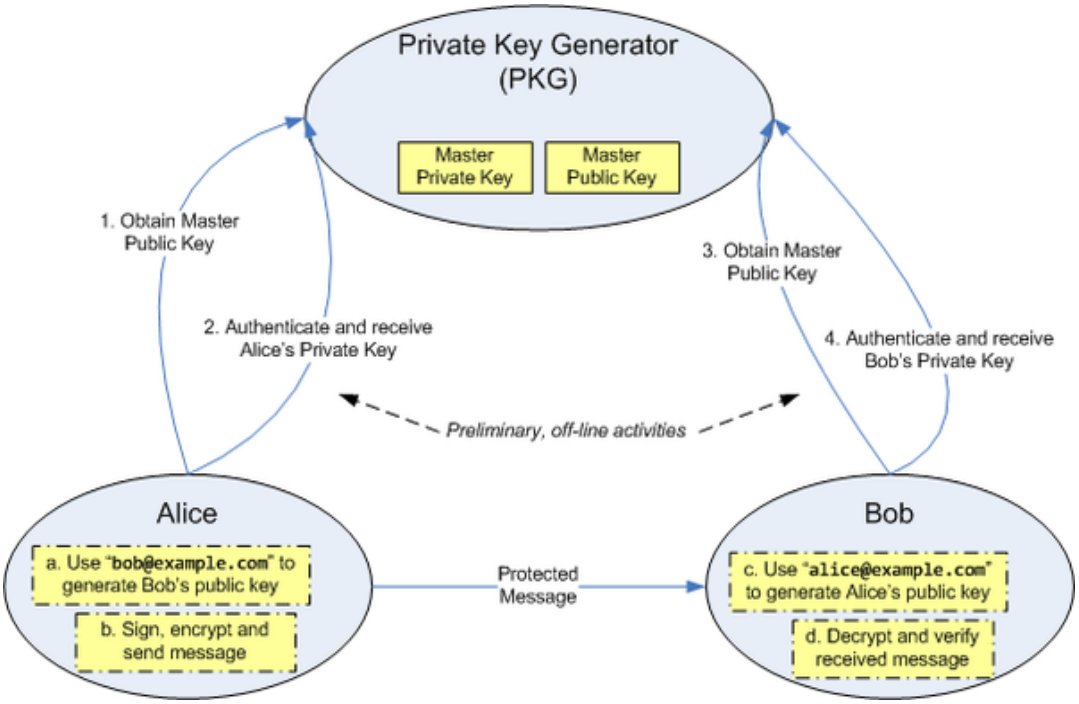


Fig: ID Based Encryption: Offline and Online Steps

One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. This can take place because this system assumes that, once issued, keys are always valid. The majority of derivatives of this system which have key revocation lose this benefit. In addition, as public keys are derived from identifiers, IBE eliminates the need for a public key distribution infrastructure [1]. The authenticity of the public keys is assured absolutely as long as the transport of the private keys to the subsequent user is kept protected. IBE offers interesting features originating from the prospect to encode supplementary information into the identifier. Formalizing the security definition of outsourced revocable IBE for the first time a scheme to offload all the key generation related operations during key-issuing and key update, leaving only a constant number of trouble-free operations for PKG and adequate users to execute locally [9]. Revocation through updating the private keys of the unrevoked users but contrasting point is that the work which trivially concatenates time

period with identity for key generation/update requires re-issuing the whole private key for unrevoked users. In order to overcome this issue a novel collusion-resistant key issuing technique is discussed [1]. A hybrid private key for each user ,in which an AND gate is implicated 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. In order to maintain decrypt ability ,unrevoked users needs to periodically request on key update for time 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 need not to contact with PKG in key-update. 2) No secure channel or user authentication is required during key-update between user and KU-CSP.

II. LITERATURE SURVEY

Revocable IBE introduced and implemented by Boneh and Franklin 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 [2]. 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[4]. 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[5]. 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[6].As far as we know, the revocable IBE scheme presented by Boldyreva et al. remains the most effective solution right now. 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. As we mentioned before, they are short in storage for both private key at user and binary tree structure at PKG. 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[7].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 to realize revocation through re-encrypting ciphertext which is only adapt to the special application that the cipherrtext 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 ciphertext. Outsourcing Computation: The problem that how to securely outsource different kinds of expensive computations has drawn considerable attentionfrom 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. At allah 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[8]. Hohenberger and Lysyanskaya proposed the first outsource-secure algorithm for modular exponentiations based on pre-computation and server-aided computation .At allah 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 At allah addressed the problem of secure outsourcing for widely applicable linear algebraic computations. Nevertheless, the proposed protocol required the expensive operations of homomorphic encryption. At allah 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 [9].Cloud Computing: Cloud computing is the latest term encapsulating the delivery of computing resources as a service. It is the current iteration of utility computing and returns to the model of" renting" resources. Leveraging cloud computing is today, the genuine means of deploying internet scale systems and much of the internet is tethered to a large number of cloud service providers. The KU-CSP provides computing service in the Infrastructure as a service (IaaS) model, which provides the raw materials of cloud computing, such as processing, storage and other forms of lower level network and hardware resources in a virtual, on demand manner via the Internet. Differing from traditional hosting services with which physical servers or parts thereof are rented on a monthly or yearly basis, the cloud infrastructure is rented as virtual machines one per-use basis and can scale in and out dynamically, based on customer needs [8]. Such on-demand scalability is enabled by the recent advancements in virtualization and network management. IaaS users do not need to manage or control the underlying cloud infrastructure but have control over operating systems, storage, deployed applications, and in some cases limited control of select networking components. Typical IaaS examples are Amazon EC2and S3 where computing and storage infrastructure are open to public access in a utility fashion [9]. We specify that in this work we also aim to utilize outsourcing computation technique to deliver overhead computation to KU-CSP so that PKG is able to be offline in key-update [7].Recently, a number of works have been proposed to tackle practical problems in the cloud aided model, which explores anoint point between cloud

computing and outsourcing computation. Wang et al. presented efficient mechanisms for secure outsourcing of linear programming computation. Green et al. [8], [9] proposed a new method for efficiently and securely outsourcing decryption of attribute-based encryption ciphertexts. They also showed their performance evaluation in Amazon EC2 platform [8] as the simulation of cloud environment. Some other works about outsourced ABE include. Especially, outsourced the encryption in ABE with the map-reduce technique in cloud computing. hang et al. proposed a novel outsourced image recovery service architecture, which exploits different domain technologies and takes security, efficiency, and design complexity into consideration from the very beginning of the service flow.

III. 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 selective-ID 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]. 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.

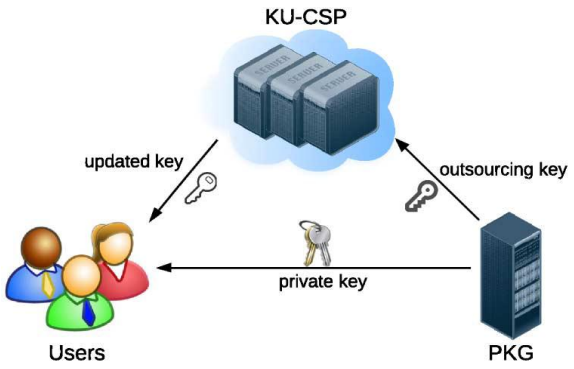


Fig. 1.System model for IBE with outsourced revocation.

The KU-CSP can be envisioned as a public cloud run by a third party to deliver basic computing capabilities toPKG 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 KU-CSP 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 un-trust KU-CSP. The challenge in designing the outsourced revocable IBE scheme is how to prevent a collusion between Bob and other unrevoked dishonest users. Specifically, a dishonest user can share her updated time component[11].

3.1 Proposed Architecture

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 keyupdate;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 decrypt ability 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 maintains a list UL to record user's identity and its corresponding outsourcing key. In key-update, we can use OK_{ID} to update the time component $TK[ID]_T$ for identity ID . Suppose a user with identity ID is revoked at T_i. Even if he/she is able to obtain TK[ID`]$T_{i+1}$for identity ID` , the revoked user still cannot decrypt ciphertext encrypted under T_{i+1}.

3.2 Algorithm

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.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[11].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 ciphertext CT. The decryption algorithm is run by receiver, which takes as input the ciphertext CT and his/her private key SKIDs . It returns a message M or an error ⊥.

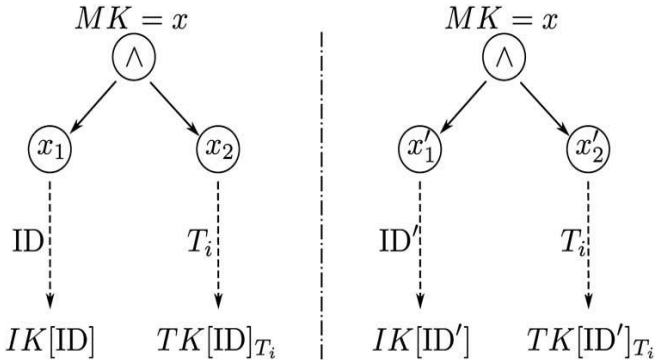


Fig 2: A comparison on generating private key for two different users

we emphasize that the idea behind our construction is to realize revocation through updating the time component in private key[11]. Therefore, the key point is to prevent revoked user from colluding with other users to re-construct his/her private key. As declaring in intuition, such collusion attack is resistant in our proposed construction due to the random split on for each user. Specifically, an AND gate connecting two sub-components, if two different users call for their private keys, PKG will obtain two randomly splits (x_1,x_2) and (x_1`,$x_2$`)with the complementarythatx_1+x_2=x mod q x_1`+$x_2$`=x mod q.$x_1$and x_1`are used to produce the identity component for while the time component is separately generated [12]. By the reason that the complementary exists between $x_1$ and $x_2$and as well as $x_1$` and x_2`and the identity component and time component should accordingly have a "verification" in private key. With such "verification", even if a curious user obtains time component of other users, he/she cannot forge a valid private key for himself to performed encryption successfully. Based on the algorithm construction, the key service procedures include key-issuing, key-update and revocation in proposed IBE scheme with outsourced revocation work[13].

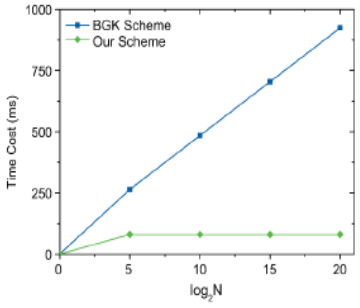
3.3 Implementation

3.3.1 Security Enhanced Construction: Rdoc Model

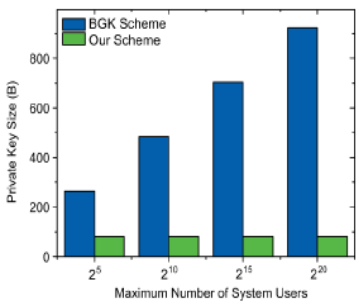
There exists g1, g2 ∈ G with e(g1, g2) 1, in other words, the map does not send all pairs in G×G to the identity in GT. Upon receiving a key update request on ID, KU-CSP firstly checks whether ID exists in the revocation list RL, if so KU-CSP returns ⊥ and key-update is aborted. In RDoC(REFEREEDDELEGATION OF COMPUTATION MODEL) 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[14]. 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[13].

Efficiency Comparison for Stages in Revocable IBE

	Our Scheme	IBE without Revocation [4]
Setup	83.764 ms	80.233 ms
Key-Issuing	40.369 ms	20.121 ms
Encryption	39.840 ms	24.595 ms
Decryption	21.278 ms	10.285 ms
Key-Update	10.300 ms[1]	—-



(a) Responding Time for Single Key Generation Request



(b) Private Key Size

Fig.3: Comparisons in key-issuing

3.4 Empirical Evaluation: Analysis And Reports

Scheme shares the same setup algorithm with the IBE scheme in key-issuing stage is relative longer than that in the IBE scheme [14].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. 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 [4] (our execution time is still within millisecond).

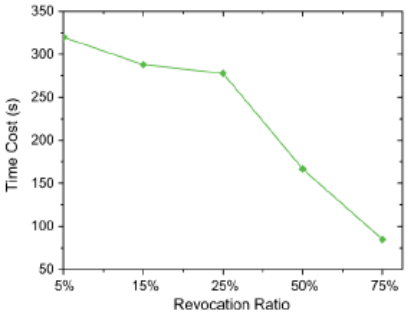


Fig.4: Key update at PKG

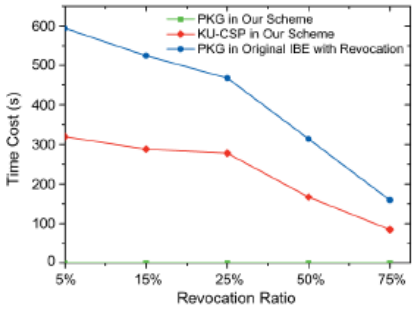


Fig.5: Key update at KU-CSP

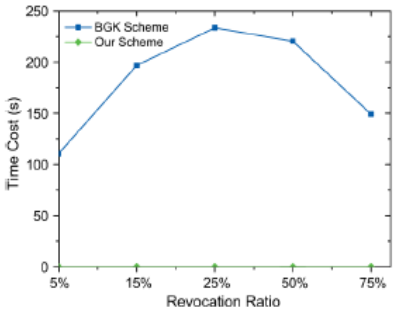


Fig.6:Key Update Comparison

IV. 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 at least one of the KU-CSPs is assumed to be honest. Even if a revoked user and either of the KU-CSPs collude, it is unable to help such user re-obtain his/her decryptability. An extensive experimental result 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 Weil pairing," 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.

[8] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," in Trends in Software Engineering ,M. V. Zelkowitz, Ed. New York, NY, USA: Elsevier, 2002,vol. 54, pp. 215–272.

[9] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE Int. Conf .Comput.Commun. (INFOCOM), 2011, pp. 820–828.

[10] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Conf. Security(SEC'11), 2011, pp. 34–34.

[11] Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in Proc. 8th Int. Conf. Netw. Service manager., 2012, pp. 37–45.

[12] J. Li, C. Jia, J. Li, and X. Chen, "Outsourcing encryption of attribute based encryption with map reduce," in Information and Communications Security. Berlin, Heidelberg: Springer, 2012, vol. 7618,pp. 191–201.

[13] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on outsourced attribute-based encryption," in Proc. 18th Eur. Symp. Res. Compute. Security (ESORICS), 2013,pp. 592–609.

[14] B. Zhang, J. Wang, K. Ren, and C. Wang, "Privacy-assured outsourcing of image reconstruction service in cloud," IEEE Trans. Emerging Topics Compute., vol. 1, no. 1, p. 166–177, Jul./Dec. 2013.

AUTHORS

[1] **Dr.GVN. Prasad Professor and HOD** Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology

[2] **M.Prashanti M.Tech Student** Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology

[3] **M.Sudarani M.Tech Student** Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology

[4] **Ch.Sandhya M.Tech Student** Department of Computer Science and Engineering, Sri Indu College of Engineering and Technology

