



Efficient Revocation on Identity Based Encryption with Public Key Infrastructure in Cloud Computing

Dr. V.Goutham

Professor, Department of CSE TKREC,
Hyderabad, India

A. Sowmya

Department of CSE
Hyderabad, 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 (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

I. 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. 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).

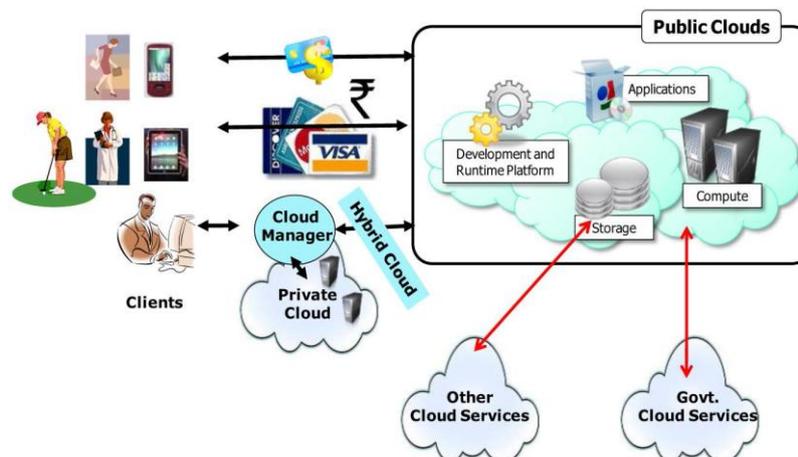


Fig.1: A bird's eye view of Cloud computing

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.

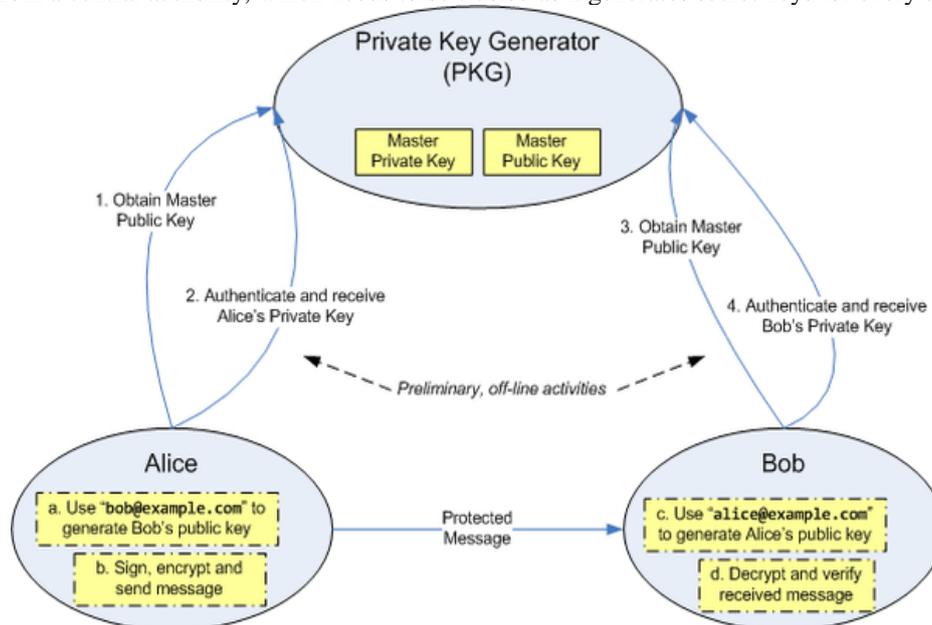


Fig: ID Based Encryption: Offline and Online Steps

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 decryptability, unrevoked users need 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. 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.

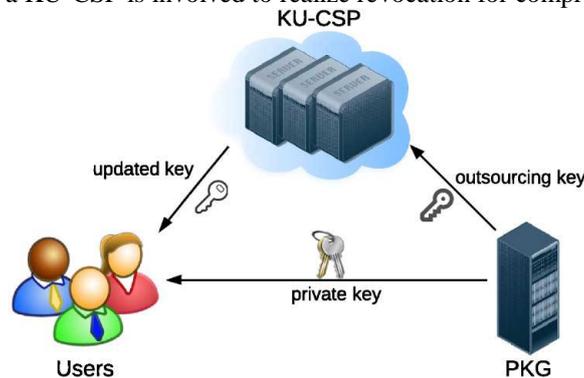


Fig. 1. System model for IBE with outsourced revocation.

The KU-CSP can be envisioned as a public cloud run by a third party to deliver basic computing capabilities 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 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 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].

III. 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 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 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} .

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 $ID \in \{0, 1\}^*$. 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 \perp .

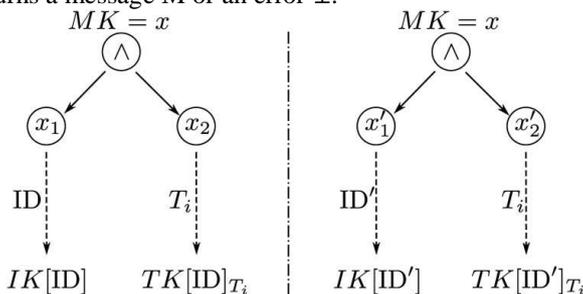


Fig 2: A comparison on generating private key for two different users

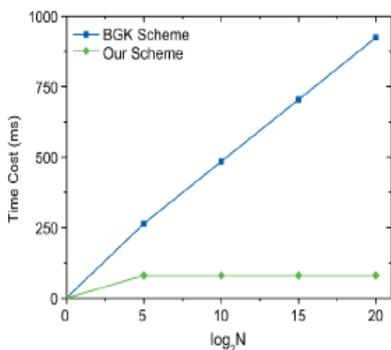
we emphasize that the idea behind our construction is to realize revocation through updating the time component in private key[11]. Therefore, the key point is to prevent revoked user from colluding with other users to re-construct this/her private key. As declaring in intuition, such collusion attack 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 complementary that $x_1 + x_2 = x \pmod q$ and $x_1' + x_2' = x \pmod q$. 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 perform decryption 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].

IV. IMPLEMENTATION: SECURITY ENHANCED CONSTRUCTION: RDOC MODEL

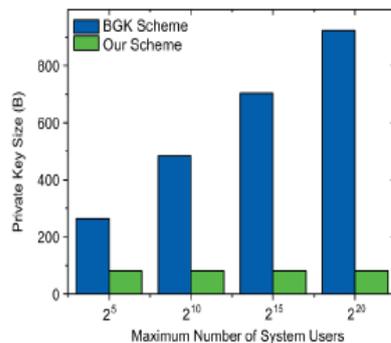
There exists $g_1, g_2 \in G$ with $e(g_1, g_2) \neq 1$, in other words, the map does not send all pairs in $G \times G$ to the identity in G . Upon receiving a key update request on ID, KU-CSP firstly checks whether ID exists in the revocation list RL, if so KU-CSP returns \perp and key-update is aborted. In RDoC (REFEREED DELEGATION 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

V. 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).

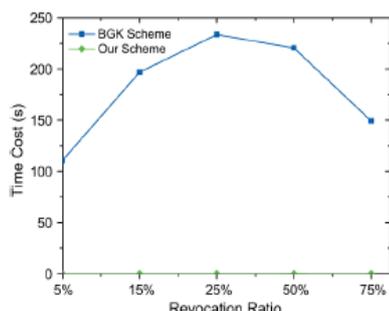


Fig.4: Key update at PKG

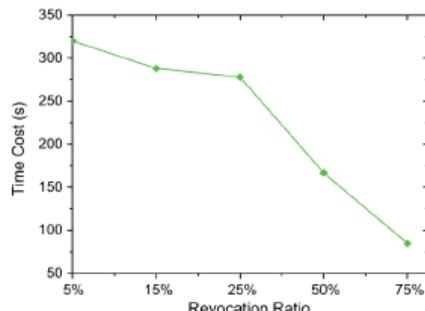


Fig.5: Key update at KU-CSP

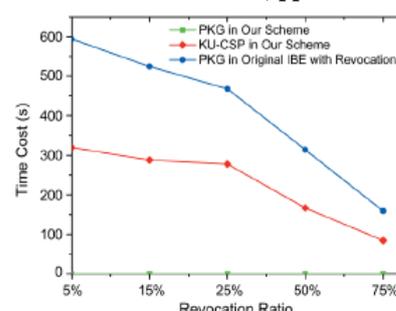


Fig.6:Key Update Comparison

VI. 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 KU-CSPs 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. 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 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," in *Proc. 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 V. Goutham is a Professor and Head of the Department of computer Science and Engineering at TKR Engineering College affiliated to J.N.T.U Hyderabad. He received M.Tech from Andhra University and B.Tech from J.N.T.U Hyderabad. He worked for various MNC Companies in Software Testing and Quality as Senior Test Engineer. His research interests are Software Reliability Engineering, software testing, software Metrics, and cloud computing.
- [2] Ms. A. Sowmya is a PG Scholar Department of computer Science and Engineering at TKR Engineering College affiliated to J.N.T.U Hyderabad.