International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT20668

An Efficient Identity Based Encryption in Cloud Computing with Outsourced Revocation

Dr. U. Vijay Sankar[1], M. Pavithra[2], R Suganya[3]
Associate Professor, Department of C.S.E, Nehru College of Engineering and Research Centre, Kerala, India[1]
Assistant Professor, Department of C.S.E, Jansons Institute of Technology, Coimbatore, India[2]
Assistant Professor, Department of Artificial Intelligence & Data Science, Jansons Institute of Technology, Coimbatore, India[3]

Article Info
Volume 6, Issue 6
Page Number: 72-82
Publication Issue :
November-December-2020

Article History
Accepted : 01 Nov 2020
Published : 10 Nov 2020

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 [2]. It 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 [3]. 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 [4]. 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. In public key encryption every user must have a pair of keys, public key and private key, for encrypting and decrypting messages. An Identity-based encryption (IBE) eliminates the need for a Public Key Infrastructure (PKI). IBE uses the human intelligible identities (e.g., unique name, email address, IP address, etc) as public keys [5]. The sender using IBE encrypts message with the receivers' identity rather than looking for receivers' public key and corresponding certificate. Accordingly, receiver decrypts ciphertext using private key associated with the corresponding identity [6]. The private keys of users are obtained from a trusted third party called as Private Key Generator (PKG). The motivation of this paper is to study and review an

efficient and secure Identity based encryption scheme with outsourced revocation for cloud computing [7].

Keywords : Identity-based encryption, Revocation, Outsourcing, Cloud computing. Public key encryption.

I. INTRODUCTION

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 [4]. Therefore, sender using IBE does not need to look up public key and certificate, but directly encrypts message with receiver's identity. Accordingly, receiver obtaining the private key associated with the corresponding identity from Private Key Generator (PKG) is able to decrypt such ciphertext. Though IBE allows an arbitrary string as the public key which is considered as an appealing advantage over PKI, it demands an efficient revocation mechanism. Specifically, if the private keys of some users get compromised, we must provide a mean to revoke such users from system. In PKI setting, revocation mechanism is realized by appending validity periods to certificates or using involved combinations of techniques [1][2][3]. Nevertheless, the cumbersome management of certificates is precisely the burden that IBE strives to alleviate.

It presented a revocable IBE scheme. Their scheme is built on the idea of fuzzy IBE primitive [6] but utilizing a binary tree data structure to record users' identities at leaf nodes. Therefore, 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) [7]. Nevertheless, we point out that though the binary tree introduction is able to achieve a relative high performance, it will result in other problems: 1) PKG has to generate a key pair for all the nodes on the path from the identity leaf node to the root node, which results in complexity 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 difficult in private key storage for users. 3) As the number of users in system grows, PKG has to maintain a binary tree with a large amount of nodes, which introduces another bottleneck for the global system

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 in [2], we realize revocation through updating the private keys of the unrevoked users. But unlike that work [4] 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 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 [3]. We also specify that 1) with the aid of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP. 2) No secure channel or user authentication is required during key-update between user and KU-CSP. Furthermore, we consider realizing revocable IBE with a semihonest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model [7]. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction

II. RELATED WORK

It [2] presents as cloud computing becomes prevalent, more and more sensitive data is centralized into cloud for sharing, which brings new challenges for outsourced data security and privacy. Attribute based encryption (ABE) is best cryptographic primitive for designing the fine-grained access control. ABE is criticized being as the computational cost grows with the complexity of the access formula. The drawback is more serious for mobile devices because they have constrained computing resources. It [6], presents Use linear algebra techniques in this system but disadvantage of this system is time complexity the number of user increases the it is difficult to maintain private key size. It [7] presents that Identity-Based Encryption (IBE) offers a best alternative to PKI-enabled encryption as it eliminates the need for digital certificates. The most convenient one was to augment identities with period of the numbers at encryption. It is used only for selective id .This scheme has disadvantage of bottleneck. It [9] presents the new scheme based on fuzzy IBE scheme but use binary tree data structure to records user's identities at leaf nodes. PKG has to generate the key for all the nodes on the path from the based on identity leaf node to the root node, which results in complexity logarithmic in the number of users in system for issuing a single private key. The size of private key increases in logarithmic in the number of users in system, which makes it difficult in private key storage for users. As the number of users in system grows, PKG has to maintain a binary tree with a large amount of nodes, which introduces another bottleneck for the global system. It [4] presents Mechanism would result in an overhead load at PKG. In another word, all the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys. It requires that PKG is online and the secure channel l must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows.

III. FAST DIGITAL IDENTITY REVOCATION

Computerized characters are fundamental for business, private and government utilization of the web. Eg: they requirement for on-line shopping, business-to-business exchanges, on-line managing an account code validation, organization inside personalities, The U.S. Government, NIST, the U.S. Mail station, Visa and Master Card, some real banks, and privately-owned businesses like VeriSign, SIAC, IBM, GTE, and Microsoft are for the most part assembling computerized personality foundations [1]. While the general plan of every one of these plans is comparative, and depends on open key cryptography and Certificate Authority administrations, In 1995, it proposed a rich strategy for character denial which requires next to no correspondence amongst clients

and verifiers in the framework. they found that, plot by lessening the general CA to catalog correspondence, while as yet keeping up the same minor clients to seller correspondence [2]. To lessens the CA to catalogs correspondence costs significantly. It can be prove that the normal day by day cost is propositional to at most (R/365) log (365 N/R) this lessening the picked up at the costs of an expansive correspondence prerequisite for the verifier. This exclusive expanding the normal day by day correspondence cost of the CA by a factor [7].

CERTIFICATE REVOCATION USING FINE GRAINED CERTIFICATE SPACE PARTITIONING

A certificate is a digitally signed statement binding the key holder's name to a public key and various other features. At the point when an endorsement is issued, the CA announces the timeframe for which the authentication is legitimate [2]. However, there may be situations when the certificate must unusual to be declared invalid prior to its expiration date. Each partition contains the status of a set of certificates; our scheme is more efficient than the three well known certificate revocation techniques: CRL, CRS and CRT. Our scheme aims to something the right balance between CA to directory communication costs and query costs by carefully selecting the number of partitions. Certification Revocation List (CRL) is the first and the least difficult strategy for declaration denial. it is generally perceived that CRLs are too exorbitant and can't give a decent level of auspiciousness, Certificate Revocation System (CRS) [was presented by and could answer the client inquiries with extraordinary productivity [1].The main problem with CRS is that it is not suitable in case of a distributed query answering system, The CA to directory communication is too high shoot the overall cost of the system [NN98, ALO98]. It [ALO98] proposed an improvement to CRS aimed at decrease this communication but their approach had problems, Certificate Revocation Tree (CRT) [Koc98] is the third well known technique for certificate revocation [5]. Though the CA to directory communication is very low, the query cost is too high again shoot up the overall cost of the system, the above approach may be worth analyze in environments where the number of directories or updates per day is high. This is because it may reduce the CA to directory communication costs which are quite high in such environments, though at the price of increasing the query costs [4].

PRIVATE AND CHEATING-FREE OUTSOURCING OF ALGEBRAIC COMPUTATIONS

We give protocols for the secure and private outsourcing of straight variable based math calculations, that expert a customer to safely outsource broad arithmetical calculations to two remote servers, such that the servers learn nothing about the customer's private input or the result of the computation and any attempted corruption of the answer by the servers is identify the presence with high probability [8]. large-scale problems in the physical and life sciences are being radically by internet computing technologies, such of techniques for computational outsourcing in a privacy-preserving and cheating-resilient manner, in future work we will extend these results to different algebraic structures, such as the closed semi as grid computing, a weak computational device, once connected to such a grid, is no longer limited by its slow speed, small local storage, two major impediments to the use of —computational outsourcing are (i) the fact that the data in question is often influences, (ii) the quality of the computed answers, which is often poor (e.g., in seti random answers afflict around 40% of the computations). This provide the design -ring ones that arise in activity programming and in graph algorithms [3].

SECURE AND PRACTICAL OUTSOURCING OF LINEAR PROGRAMMING IN CLOUD COMPUTING

The privacy cheating discouragement Sec-cloud is used for courage the greater aspects of security. Although the cloud computing is being used to obtain large-scale computations to the cloud, data privacy has become a major issue, the modern cryptographic techniques in secure outsourcing along with the research work, which has been proposed in past years has been presented, which is used for the activities non-demand network access to the shared pool of the computing a stock which is having the greater efficiency as well as large computational power [9]. Basic advantage of cloud computing is that it is having the benefits of centralized large computational power, space and efficiency, so that the customers/clients can outsource their complex problem to the cloud for computation, they have also presented several real time problems for secure outsourcing of complex matrix multiplication and quadrature scientific computations [10]. They have also mentioned the possibility of leakage of confidential and private information. It presented an efficient protocol to securely outsource the sequence comparisons between two servers to overcome the problem of computing using the edit distance between two sequences. Today, data privacy and security become an essential part of various cloud based applications, multiparty computation scenarios etc. Due to lack of computational resources, clients need to direct their computational problem parameters to cloud, in this area and the general architecture of secure outsourcing linear programming problems in cloud computing. The problem identification in this area has also discussed in this paper and has given the future research directions [4].

ATTRIBUTE BASED DATA SHARING WITH ATTRIBUTES REVOCATION

In CP-ABE, every client is related with an arrangement of properties and information are encoded with get to structures on characteristics. A client can unscramble a ciphertext if and just if his qualities fulfill the ciphertext get to structure, specifically; we settle this testing issue by considering more pragmatic situations in which semi-trustable on-line intermediary servers are accessible [2]. When contrasted with existing plans, our proposed arrangement empowers the expert to disavow client properties with insignificant exertion. The present processing innovations have pulled in an ever-increasing number of individuals to store their private information on outsider servers either for simplicity of sharing or for cost sparing [3]. At the point when individuals appreciate the focal points these new innovations and administrations realize, their worries about information security additionally emerge [4]. Normally, individuals might want to make their private information just open to approved clients. Much of the time, it is likewise attractive to give separated access administrations with the end goal that information gets to arrangements are characterized over client properties/parts. It first presented qualities-based encryption (ABE) for encoded get to control. In an ABE framework, both the client mystery key and the ciphertext are related with an arrangement of characteristics. One fascinating future work is to join a safe calculation strategy with our development to ensure the trustworthiness of intermediary servers. Another heading for future work is to enable intermediary servers to refresh client mystery key without unveiling client property data [5].'

SECURITY IN CLOUD USING CIPHER TEXT POLICY ATTRIBUTES-BASED ENCRYPTION WITH CHECK ABILITY

In (CP-ABE) is considered as a standout amongst the most appropriate plan for information get to control in distributed storage [6]. In spite of that the current Outsourced ABE arrangements can offload some serious processing intensive to an outsider, the unquestionable status of results came back from the outsider presently can't seem to be tended to. Going for handling the test over, another Secure Outsourced ABE framework is proposed, which underpins both secure outsourced key-issuing and decoding. In ABE framework, clients' private keys and ciphertext marked with sets of spellbinding characteristics and access arrangements separately, and a specific key can unscramble a specific ciphertext just if related qualities and approach are coordinated. Up to this point, there are two sorts of ABE having been proposed: key-approach quality-based encryption (KPABE) and ciphertext-arrangement trait-based encryption (CP-ABE). In KP-ABE, the entrance strategy is doled out in private key, while, in CP-ABE, it is determined in ciphertext, Identity-Based Encryption (IBE) enables a sender to encode a message to a character without access to an open keys endorsement [8]. The capacity to do open key encryption without declarations has numerous useful applications. The client denial should be possible by means of the intermediary encryption system together with the CP-ABE calculation [9].

IV. EXISTING SYSTEM

As far as we know, though revocation has been thoroughly studied in PKI, few revocation mechanisms are known in IBE setting. It suggested that users renew their private keys periodically and senders use the receivers‟ identities concatenated with current time period. But this mechanism would result in an overhead load at PKG [6]. In another word, all the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys. 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 [7]. In 2008, it presented a revocable IBE scheme. Their scheme is built on the idea of fuzzy IBE primitive but utilizing a binary tree data structure to record users‟ identities at leaf nodes. Therefore, 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) [8]. Nevertheless, we point out that though the binary tree introduction is able to achieve a relative high performance, it will result in other problems:

PKG has to generate a key pair for all the nodes on the path from the identity leaf node to the root node, which results in complexity logarithmic in the number of users in system for issuing a single private key. The size of private key grows in logarithmic in the number of users in system, which makes it difficult in private key storage for users [2]. As the number of users in system grows, PKG has to maintain a binary tree with a large amount of nodes, which introduces another bottleneck for the global system. In tandem with the development of cloud computing, there has emerged the ability for users to buy on-demand computing from cloud-based services such as Amazon‟s EC2 and Microsoft‟s Windows Azure [3]. Thus it desires a new working paradigm for introducing such cloud services into IBE revocation to fix the issue of efficiency and storage overhead described above. A naive approach would be to simply hand over the PKG‟s master key to the Cloud Service Providers (CSPs) [4]. The CSPs could then simply update all the private keys by using the traditional key update technique and transmit the private keys back to unrevoked users. However, the naive approach is based on an unrealistic assumption

that the CSPs are fully trusted and is allowed to access the master key for IBE system [5]. On the contrary, in practice the public clouds are likely outside of the same trusted domain of users and are curious for users‟ individual privacy. For this reason, a challenge on how to design a secure revocable IBE scheme to reduce the overhead computation at PKG with an un trusted CSP is raised.

MAJOR DRAWBACKS OF THE EXISTING SYSTEM

- The mechanism would result in an overhead load at PKG (Private Key Generator)
- All the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys.
- 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.
- IBE revocation has the issue of efficiency and storage overhead.

V. PROPOSED SYSTEM

In this project, 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 [1]. 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 [3]. In our scheme, as with the suggestion in, we realize revocation through updating the private keys.

KEY UPDATE CLOUD SERVICE PROVIDER (KU-CSP)

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 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) [6]. 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 [7].

We also specify that 1) with the aid of KU-CSP, user needs not to contact with PKG in key-update, and in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP. 2) No secure channel or user authentication is required during key-update between user and KU-CSP [8].

Furthermore, we consider realizing revocable IBE with a semi-honest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model [9]. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

SUPPORTING DIAGRAM FOR REFERENCE

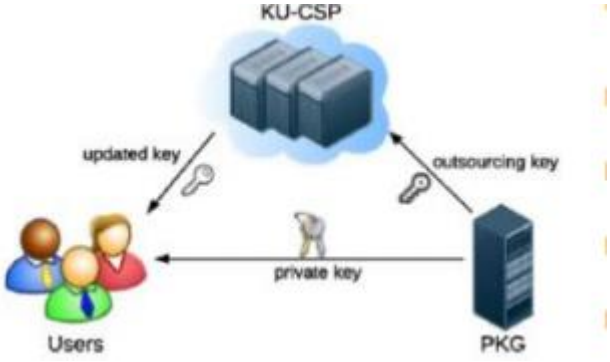


Fig 1. System model for IBE with outsourced revocation.

MAJOR ADVANTAGES OF THE PROPOSED SYSTEM

- We tackle 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
- We also consider realizing revocable IBE with a semihonest KU-CSP

THE BONEH-FRANKLIN IBE

Consider a basic encryption scheme based on the identity of the proposed Boneh and Franklin in 2001 [Boneh_Franklin_01]. This scheme is not resistant to the attack based on the selected ciphertext is the prototype of the complete circuit IBE, having this resistance [3].

VI. ALGORITHM

In the basic scheme generator IG of random parameters BDHP is used, satisfying hypothesis BDHP [4]. Let k - parameter of security is received by the protocol as an argument on th

Setting

1) On the basis k the IG generates the groups G, H of prime orders and the bilinear pairing $e: G \times G \to H$. Let q — the order of G, H. The algorithm chooses an arbitrary generator $P \in G$.

2) Selects a random $s \in Z_q^*$ and calculate $P_{pub} = sP$.

3) Selects the cryptographic hash functions $H_1 : \{0,1\}^* \to G^*$ and $H_2 : H \to \{0,1\}^n$ for some n, $G^*=G\backslash\{1\}$. In the analysis of the security protocol, these functions are regarded as random oracles.

4) A space of massanges $\mu = \{0,1\}^n$. A ciphertext's space $C = G^* \times \{0,1\}^n$. System settings is set $params = \langle G, H, e, n, P, P_{pub}, H_1, H_2 \rangle$. The master-key $s \in Z_q^*$.

Removing

For a given line $ID \in \{0,1\}^*$ algorithm calculates:

1) $Q_{ID} = H_1(ID) \in G^*$.

2) Set the private key $d_{ID} = sQ_{ID}$.

Encryption

To encrypt a message M by the public key ID does the following:

1) Calculate $Q_{ID} = H_1(ID) \in G^*$.

2) Selects a random $r \in Z_q^*$.

3) Calculate $C = \langle rP, M \oplus H_2(g_{ID}^r) \rangle$, where $g_{ID} = e(Q_{ID}, P_{pub}) \in H$.

Decryption

Let $C = \langle U, V \rangle$ — a ciphertext obtained by encrypting plaintext on the public key ID. To decrypt C with the private key $d_{ID} \in G^*$ calculates:

$V \oplus H_2(e(d_{ID}, U)) = M$.

The correctness of the scheme is supported by the following expression:

$e(d_{ID}, U) = e(sQ_{ID}, rP) = e(Q_{ID}, P)^{sr} = e(Q_{ID}, P_{pub})^r = g_{ID}^r$.

e input.

Setting

1) On the basis k the IG generates the groups G, H of prime orders and the bilinear pairing $e: G \times G \to H$. Let q — the order of G, H. The algorithm chooses an arbitrary generator $P \in G$.

2) Selects a random $s \in Z_q^*$ and calculate $P_{pub} = sP$.

3) Selects the cryptographic hash functions $H_1 : \{0,1\}^* \to G^*$ and $H_2 : H \to \{0,1\}^n$ for some n, $G^*=G\backslash\{1\}$. In the analysis of the security protocol, these functions are regarded as random oracles.

4) A space of massanges $\mu = \{0,1\}^n$. A ciphertext's space $C = G^* \times \{0,1\}^n$. System settings is set $params = \langle G, H, e, n, P, P_{pub}, H_1, H_2 \rangle$. The master-key $s \in Z_q^*$.

Removing

For a given line $ID \in \{0,1\}^*$ algorithm calculates:

1) $Q_{ID} = H_1(ID) \in G^*$.

2) Set the private key $d_{ID} = sQ_{ID}$.

AN IBE SCHEME BASED ON THE FULLIDENT ALGORITHM

On the basis of the basic IBE scheme the full scheme IBE [Fujisaki 99] was received. This scheme is resistant to attacks based on the selected ciphertext under the assumption that the BDHP generator parameters satisfies hypothesis BDHP [5].

ALGORITHM

Let n - is the length of the encrypted message.

Root Setup

The root PKG selects generic groups $P_0 \in G$, random $s_0 \in Z_q^*$ and set $Q_0 = s_0 P_0$. Let $H_1: \{0,1\}^* \to G^*$ and $H_2: G_2 \to \{0,1\}^n$ — cryptographic hash functions. Space of messages $\mu = \{0,1\}^n$, space of ciphertexts $CS = G^t \times \{0,1\}^n$, where t — the level of the recipient.

For the root PKG $s_0 \in Z_q^*$ is a secret key. System settings $params = (G, H, e, P_0, Q_0, H_1, H_2)$.

Lower-level Setup

Objects $E_t \in Level_t$, select random $s_t \in Z_q^*$, which they keep a secret.

Extract

Let a object $E_t \in Level_t$, with set $(ID_1, ID_2, \dots, ID_t)$. Then the parent does the following:

1) Calculate $P_t = H_1(ID_1, ID_2, \dots, ID_t) \in G$.
2) Set as a secret E_t a point $S_t = S_{t-1} + s_{t-1} P_t = \sum_{i=1}^{t} s_{i-1} P_i$.
3) Gives to E_t value $Q_i = s_i P_0$, где $1 \le i \le t-1$.

Encrypt

For encrypt a message $M \in \mu$ with a set of identifiers $(ID_1, ID_2, \dots, ID_t)$ execute:

1) Calculate $P_i = H_1(ID_1, ID_2, \dots, ID_t) \in G_1$, where $1 \le i \le t$.
2) Select random $r \in Z_q^*$.
3) Calculate ciphertext $C = \langle rP_0, rP_2, \dots, rP_t, M \oplus H_2(g^r) \rangle$, where $g = e(Q_0, P_1) \in G_2$.

Decrypt

Let $C = \langle U_0, U_2, \dots, U_t, V \rangle \in CS$ — ciphertext, has encrypted using $(ID_1, ID_2, \dots, ID_t)$. For decrypt C E_t calculates $V \oplus H_2\left(\frac{e(U_0, S_t)}{\prod_{i=2}^{t} e(Q_{i-1}, U_i)}\right) = M$.

Encryption

To encrypt a message $M \in \{0,1\}^n$ by the public key ID the algorithm does the following:

1) Calculate $H_1(ID) \in G^*$.
2) Selects a random $\sigma \in \{0,1\}^n$.
3) Calculate $r = H_3(\sigma, M)$.

Calculate the ciphertext $C = \langle rP, \sigma \oplus H_2(g_{ID}^r), M \oplus H_4(\sigma) \rangle$, where $g_{ID} = e(Q_{ID}, P_{pub}) \in H^*$.

Decryption

Let $C = \langle U, V, W \rangle$ — a ciphertext obtained by encrypting plaintext on the public key ID. If $U \notin G^*$, we do not accept ciphertext. Otherwise. for decrypt C with the private key $d_{ID} \in G^*$, calculates:

1) $V \oplus H_2(e(d_{ID}, U)) = \sigma$.
2) $W \oplus H_4(\sigma) = M$.
3) $r = H_3(\sigma, M)$. Check equality $U = rP$. If it is wrong, then to reject the ciphertext.
4) M — is the plaintext.

HIERARCHICAL IDENTITY BASED ENCRYPTION

The hierarchical encryption scheme based on the identity (HIBE) was proposed Gentry and Silverberg [Gentry_02], and allows the root PKG distribute the load, delegate to lower-level PKG the right of generate private keys and authentication [4].

ALGORITHM

PERFORMANCE EVALUATION

In this section, we will provide a thorough experimental evaluation of the construction proposed. We build our testbed by using 64-bit M2 high-memory quadruple extra-large Linux servers in Amazon EC2 platform as KU-CSP, and a Linux machine with Intel(R) Core(TM)2 Duo CPU clocked at 2.40 GHz and 2 GB of system memory as the user [4].

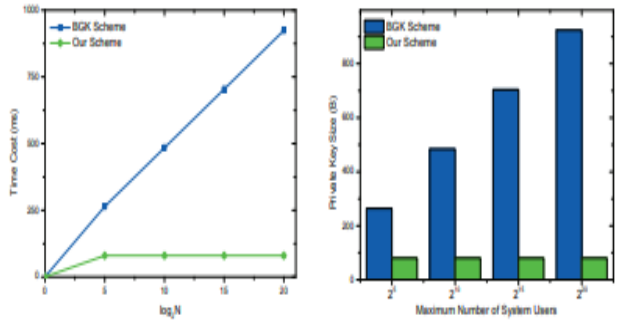
PERFORMANCE EVALUATION FOR OVERALL SCHEME

Firstly, we aim to evaluate the efficiency of our outsourced revocable scheme by comparing the total time taken during each stage with the original IBE [2] which does not consider revocation. In TABLE I, we examine the time cost of executing individual stage by the both schemes. It is not surprising to see that our scheme takes more time because we consider the revocability issue. Note that our scheme shares the same setup algorithm with the IBE scheme in [4]. Our key-issuing stage is relative longer than that in the IBE scheme [5]. This is because we embed a time component into each user's private key to allow periodically update for revocation, resulting that some additional computations2 are needed in our scheme to initialize this component. Our encryption and decryption is slightly longer than the IBE scheme [6], which is also due to the existence of the time component. 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 [7] (our execution time is still within millisecond).

PERFORMANCE EVALUATION FOR REVOCATION

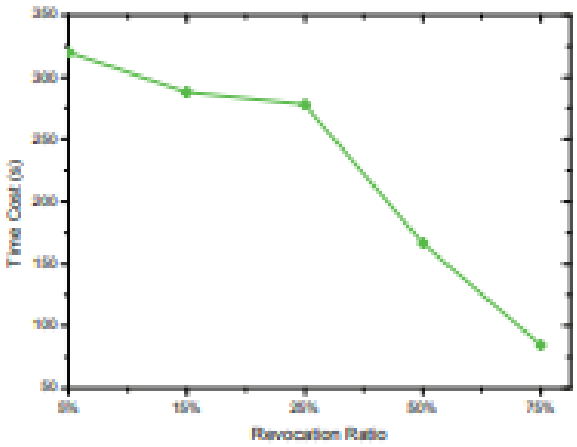
Secondly, we attempt to simulate the scenario of multi-user revocation, and show an extensive comparison between our outsourced revocation scheme and another revocable IBE scheme – BGK scheme [5]. Note that in this set of experiments, we

use a 32- bit integer to identify each node in binary tree which is utilized in BGK scheme [3] for managing users. Our comparison is in terms of the key-issuing stage and the key-update stage. 1) Key-Issuing Stage: In, we vary the maximum number of users in the system and show the responding time for a single key generation request. It is not hard to see that the responding time in BGK scheme [2] is in proportion of O(log2(N)) where N is the maximum number of users in system. This is because a binary tree is utilized to manage all the users, each leaf node of which is assigned to a single user in system.



(a) Responding Time for Single Key Generation Request

(b) Private Key Size



Revocation Ratio	2^5	2^{10}	2^{15}	2^{20}
5%	132.646 ms	3.66 s	1.845 min	0.998 h
15%	212.162 ms	6.607 s	3.283 min	1.879 h
25%	194.135 ms	7.232 s	3.894 min	2.15 h
50%	189.851 ms	9.63 s	3.674 min	1.99 h
75%	133.072 ms	4.186 s	2.488 min	1.207 h

VII. CONCLUSION

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 [4]. 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 key update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP; 3) No secure channel or user authentication is required during key-update between user and KU-CSP [6]. Furthermore, we consider realizing revocable IBE under a stronger adversary model. We present an advanced construction and show it is secure under RDoC model, 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 [7].

VIII. REFERENCES

[1]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology (CRYPTO‟8). New York, NY, USA: Springer, pp. 137–152, 2008.

[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, vol. 4886, pp. 247–259, 2007.

[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, vol. 2947, pp. 375–388, 2004.

[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, vol. 2139, pp. 213– 229,2001.

[5]. A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proc. 15thACMConf. Comput.Commun.Security (CCS‟08), pp. 417 426,2008.

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

[7]. R. Canetti, B. Riva, and G. N. Rothblum, “Two 1-round protocols for delegation of computation,” Cryptology ePrint Archive, Rep. 2011/ 518, 2011 online]. Available: http://eprint.iacr.org/2011/51

[8]. D. Chaum and T. P. Pedersen, “Wallet databases with observers,” in Proc. 12th Annu. Int. Cryptology Conf. Adv. Cryptology (CRYPTO‟92), pp. 89–105, 2013.

[9]. M. J. Atallah and J. Li, “Secure outsourcing of sequence comparisons,” Int. J. Inf. Security, vol. 4, pp. 277–287, 2005.

[10]. M. J. Atallah and K. B. Frikken, “Securely outsourcing linear algebra computations,” in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS‟10), pp. 48–59, 2010.

Cite this article as :

Dr. U. Vijay Sankar, M. Pavithra, R Suganya, "An Efficient Identity Based Encryption in Cloud Computing with Outsourced Revocation", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 6, pp. 72-82, November-December 2020. Available at

doi : https://doi.org/10.32628/CSEIT20668

Journal URL : http://ijsrcseit.com/CSEIT20668