International Journal for Modern Trends in Science and Technology
Volume: 03, Special Issue No: 02, March 2017
ISSN: 2455-3778
http://www.ijmtst.com

Attribute-Based Encryption with Hybrid Key and Outsourced Repudiation in Cloud Environment

K.Sai Sree[1] | P.Vinod[2] | Y.Rajasekhar[3] | A.Sravani[4]

[1,2,3]UG Scholar, Department of IT, Lakireddy Balireddy College of Engineering, Maylavaram, Andhra Pradesh, India.
[4]Assistant Professor, Department of IT, Lakireddy Balireddy College of Engineering, Maylavaram, Andhra Pradesh, India.

To Cite this Article
K.Sai Sree, P.Vinod, Y.Rajasekhar and A.Sravani, "Attribute-Based Encryption with Hybrid Key and Outsourced Repudiation in Cloud Environment", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Special Issue 02, 2017, pp. 06-11.

ABSTRACT

Attribute-based encryption is used for operative encryption of data multi authority based ABE for providing a high degree privacy partition of users into multiple domains condenses the difficulty of key management. But information and keys on clouds can be interrupted by semi reliable servers. Therefore for high data security refereed delegation of computation model is implemented in our proposed work. Our scheme rids most of the key generation related operations during key-issuing and key-update routes to a key update CSP, leaving only constant number of simple operations for PKG and users to perform locally. This goal is attained by employing an innovative conspiracy-sturdy procedure; we hire a hybrid private key for each user and in which an AND gate is involved to associate and bound the identity component and the time component. Cloud computing becomes increasingly popular for data owners to outsource their records to public cloud servers while allowing anticipated data users to regain these records deposited in cloud. Compared with previous work our pattern does not have to re-issue the unabridged private keys but just need to re-issue the whole private keys.

KEYWORDS: *Attribute-based encryption (ABE), repudiation, outsourcing, cloud environment*

Copyright © 2017 International Journal for Modern Trends in Science and Technology
All rights reserved.

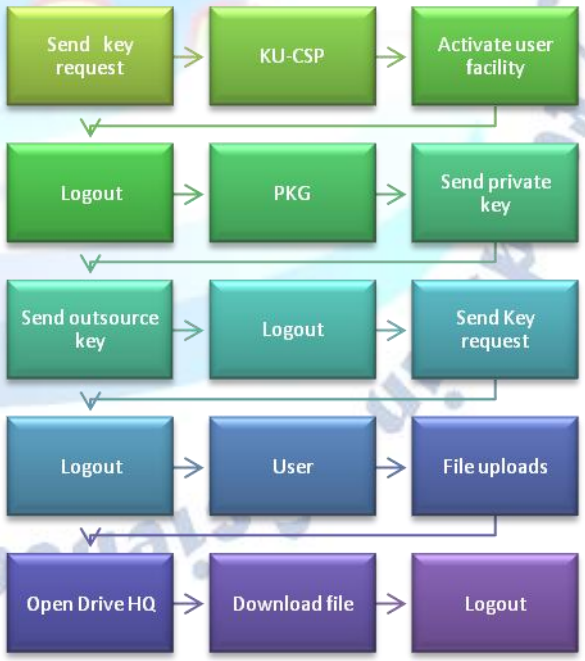
I. INTRODUCTION

Attribute-based encryption (ABE) is an appealing substitute to public key encryption, which is offered to simplify key management in a licence-based Public Key Infrastructure (PKI) by using person-logical identities (e.g., unique name, email address, IP address, etc) as public keys. Boneh and Franklin suggested that users restore their private keys occasionally and senders use the receivers individualities concatenated with current time period. Hanaoka et al. proposed a way for users to occasionally repeat their private keys without interrelating with PKG. Lin et al. projected a space efficient revocable ABE mechanism from non-monotonic Attribute-Based Encryption (ABE), but their construction requires times bilinear pairing operations for a single decryption where the number of revoked users are. Main hindrance of our system is Boneh and Franklin mechanism would result in an overhead load at PKG. In another word, all the users despite of whether their keys have been retracted or not, have to interact with PKG occasionally to verify their individualities and appraise new private keys. It requires that PKG is available and the sheltered channel must be maintained for all transactions, which will become a bottleneck for ABE system as the number of

users grows. Boneh and Franklin's suggestion is more a viable solution but not practical. In Hanaoka et al system, however, the assumption required in their work is that each user needs to possess a tamper-resistant hardware device. If an identity is revoked then the mediator is instructed to stop helping the user. Obviously, it is not practical since all users are unable to decrypt on their own and they need to be in touch with mediator for each decryption. In this paper, we introduce outsourcing computation into ABE repudiation, and formalize the security definition of outsourced revocable ABE for the first time to the most excellent of our information. We advise a scheme to offload all the key generation related operations during key-issuing and key update, leaving only an unvarying number of simple operations for PKG and qualified users to perform locally. In our scheme, as with the suggestion, we understand revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, This goal is attained by employing an innovative conspiracy-sturdy procedure; we hire a hybrid private key for each user and in which an AND gate is involved to associate and bound the identity component and the time component At first, user is capable 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). Main benefit of our implemented work is compared with the previous work, our method 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 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. No secure channel or user certification is required during key-update between user and KU-CSP. Furthermore, we consider to realize 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. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

Cloud computing is a just beginning promising technology and has been adopted on a large scale. One of the services of cloud computing used intensively is cloud storage system. In cloud, many records owners allocate their records to official user. This requires providing access control mechanism for approved user to right to use records and also defending the cloud service contributor and unofficial users. There are so many access control models to grant access control mechanism. This paper reviews various access control models that are used to provide privileges by records owner to the approved users .It also explains the different encryption techniques used to prevent the information from attackers. In access control models, ABAC (Attribute Based Access Control) is an existing model was modified in an ulti-authority -*access in a cloud storage system for security as well as scalability [3]. Access Control Lists (ACLs) are oldest and basic access control [20].This model is not apt for dynamic system. With an RBAC, The job can be assigned by their names, and also verify set of permissions to be granted to users [3].

Architecture



II. Related Work

By [13] and firstly implemented by Boneh and Franklin [4] as well as [14], IBE has been researched intensively in cryptographic community. On the aspect of construction, these

first schemes [4], [14] were proven secure in random oracle. Some subsequent systems achieved Introduced provable secure in standard model under selective-ID security [15], [16] or adaptive-ID security [17]–[19]. Newly, there have been many lattice-based constructions for IBE systems [20]–[22].However, regarding on revocable IBE, there is little work offered. As mentioned before, Boneh and Franklin's suggestion [4] is more a viable solution but not practical. Hanaoka et al. [23] proposed a way for users to at regular intervals renew their private keys without interacting with PKG. However, the best guess necessary in their work is that each user needs to possess a tamper-resistant hardware device. Another solution is mediator-aided revocation [24], [25]: 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. 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. [26] 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 the number of revoked users is. As far as we know, the revocable IBE scheme presented by Boldyreva et al. [5] remains the most effective solution right now. Libert and Vergnaud [27] improved Boldyreva's construction [5] to achieve adaptive-ID security. Their work focused on security enhanced, but inherits the similar disadvantage as Boldyreva's original construction [5]. As we mentioned before, they are short in storage for both private key at user and binary tree structure at PKG.

2.1 Outsourcing Computation:

The problem that how to secure outsource different kinds of expensive computations has drawn considerable attention from theoretical computer science community for a long time. Chaum and Pedersen [29] firstly introduced the notion of wallets with observers, a piece of secure hardware installed on the client's computer to perform some expensive computations. Atallah et al. [30] 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. Hohenberger and Lysyanskaya [9] proposed the first outsource-secure algorithm for modular exponentiations based on pre-computation and server-aided computation. Atallah and Li [31] 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 Atallah [32] addressed the problem of secure outsourcing for widely applicable linear algebraic computations. Nevertheless, the proposed protocol required the expensive operations of homomorphic encryption. Atallah and Frikken [12] further studied this problem and gave improved protocols based on the so-called weak secret hiding assumption. Chen et al. [11] made an efficiency improvement on the work [9] and proposed a new scheme for outsourcing single/simultaneous modular exponentiations.

2.2 Cloud Computing:

Cloud Computing is the latest term encapsulating the delivery of computing resources as a service [33]. It is the current iteration of utility computing and returns to the model of "renting" resources. Leveraging cloud computing is today, the defector means of deploying internet scale systems and much of the internet is tethered to a large number of cloud service providers. In this paper, 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 on a per-use basis and can scale in and out dynamically, based on customer needs. Such on-demand scalability is enabled by the recent advancements in virtualisation 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 (e.g. host firewalls) [34]. Typical IaaS examples are Amazon EC2 and S3 where computing and storage infrastructure are open to public access in a utility fashion. 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. Recently, a number of works have been proposed to tackle

practical problems in the cloud aided model, which explores a joint point between cloud computing and outsourcing computation. Wang et al. [35] presented efficient mechanisms for secure outsourcing of linear programming computation. Green et al. [36] proposed a new method for efficiently and securely outsourcing decryption of attribute-based encryption cipher texts. They also showed their performance evaluation in Amazon EC2 platform as the simulation of cloud environment. Some other works about outsourced ABE include [37]–[39]. Especially, [38] outsourced the encryption in ABE with the map-reduce technique in cloud computing. Zhang et al. [40] 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. Methodologies

3.1 Cloud Revocation Authority and Its Applications

Identity-based encryption (IBE) is a public key cryptosystem and eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. Due to the absence of PKI, the revocation problem is a critical issue in IBE settings. Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcing computation technique into IBE, Li et al. proposed a revocable IBE scheme with a key-update cloud service provider (KU-CSP). However, their scheme has two shortcomings. One is that the computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for each user. In the article, we propose a new revocable IBE scheme with a cloud revocation authority (CRA) to solve the two shortcomings, namely, the performance is significantly improved and the CRA holds only a system secret for all the users. For security analysis, we demonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. Finally, we extend the proposed revocable IBE scheme to present a CRA-aided authentication scheme with period-limited privileges for managing a large number of various cloud services.

As far as we know, though repudiation has been painstakingly intentional in PKI, few repudiation mechanisms are known in IBE setting. In [4], Boneh and Franklin 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. 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 ABE system as the number of users grows.

3.2 Other Revocation Technique

A further work related to us originates from Yu et al. [28]. The authors utilized proxy re-encryption to put forward a revocable ABE scheme. The confidential authority only wants to update master key according to attribute revocation rank in each time period and issue proxy re-encryption key to alternative servers. The alternative servers will then re-encrypt cipher text using the re-encryption key to make sure all the unrevoked users can execute unbeaten decryption. We identify that a third party service provider is introduced in both Yu et al. [28] and this job. In a different way, Yu et al. [28] utilized the third party (work as a proxy) to realize revocation through re-encrypting cipher text which is only adapt to the special application that the cipher text is stored at the third party. However, in our structure the repudiation is realized through updating private keys for unrevoked users at cloud service provider which has no limits on the location of cipher text.

IV. Experimental Results

In our experimental results we have five modules. We will implement all these in our project

4.1Registration

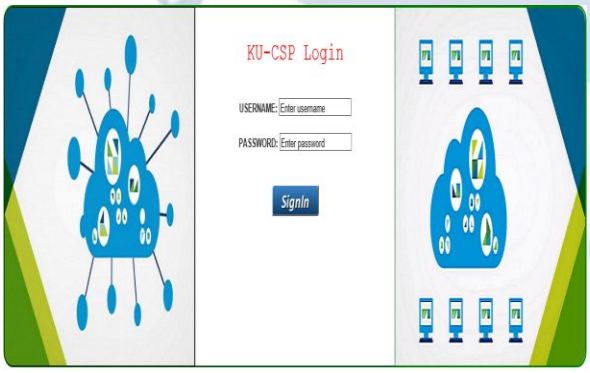
User registration is mandatory for who wants to access my project. And we need to give the proper username, mail id, password, contact no and location. Authorized users have only takes the further steps.

4.2 PKG (Private Key Generator):

In this system PKG will generate the Private Keys for all authorized Users and as well as send Outsourcing Key to KU-CSP. If any User compromised by Attacker then PKG will Revoke that User i.e. he can update the time component only for not accessing any resources which is sent to him.

4.3 KU-CSP

In this system KU-CSP will be update upon receiving a key update request on ID, KU-CSP firstly checks whether ID exists in the Revocation List (*RL)* , if so KU-CSP does not perform Key Updation process, Otherwise KU-CSP fetches Updated Key and send to User.

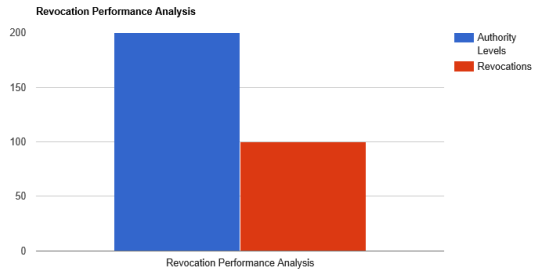


4.4 Users:

In this system PKG will generate the Private Keys for all authorized Users and as well as send Outsourcing Key to KU-CSP. If any User compromised by Attacker then PKG will Revoke that User i.e. he can update the time component only for not accessing any resources which is sent to Him.

V. PERFORMANCE ANALYSIS

5.1 Key-update Stage



In performance analysis we mainly focus on authority levels and revocation. And in our previous project the time cost is very high. We reduce the particular issue in our project. In the same we implemented KU-CSP, KEY-ISSUING and REPUDIATION.

5.2 key-issuing stage

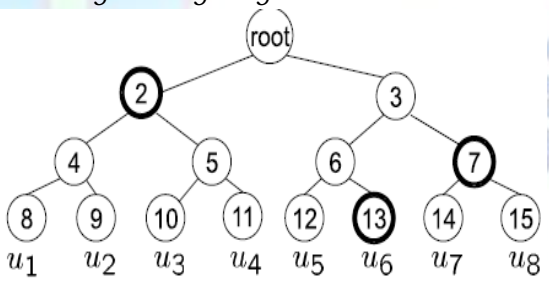


Fig. 1. Example of KUNode.

of KUNode is given below.

KUNode(BT, RL, T) :
X, Y ← ∅;
∀(η_i, T_i) ∈ RL
If $T_i \le T$ then add Path(η_i) to X;
∀x ∈ X
If $x_{left} \notin$ X then add x_{left} to Y;
If $x_{right} \notin$ X then add x_{right} to Y;
If $|RL| = 0$ then add root to Y;
Return Y;

In fig. 1 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 [5] 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. During key-issuing, PKG has to perform computation on all the nodes in the path from the corresponding leaf node to root node. Compared to the logarithmically growing efficiency in [5], our scheme achieves constant efficiency (nearly six modular exponentiation in G) in single key-issuing. Correspondingly, we show the comparison on private key size in Fig. 7(b). Due to the same reason of demanding for computation on all the nodes in path from leaf node to root node, the previous approach [5] has an increasing private key size, whereas ours achieves constant key size (nearly four element in group G).

Besides the better performance in efficiency and private key size, another advantage of our scheme over the previous work [5] is that it supports dynamic number of users. Specifically, the previous work [5] requires to fix the maximum number of users in system initially to facilitate building the binary tree. Once the maximum number is fixed, it is difficult to add users exceeding this bound. Ours does not have such a drawback, and flexibly supports dynamic management of users.

VI. Conclusion

In this paper, we introduce outsourcing computation into ABE and propose a repudiation scheme in which the operations are delegated to CSP. With abet of KU-CSP, our proposed scheme is full featured. The time complexity of our proposed system is very less compared with previous existing systems. We created a hybrid key for each user. So that we can overcome from the user security related issues. And we implemented RDOC model. Lastly, we provided our experimental results to verify the feasibility of our scheme.

References

[1] Aiello, William, Sachin Lodha, and Rafail Ostrovsky. "Fast digital identity revocation." *Annual International Cryptology Conference*. Springer Berlin Heidelberg, 1998.

[2] Goyal, Vipul. "Certificate revocation using fine grained certificate space partitioning." *International Conference on Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2007.

[3] Elwailly, Farid F., Craig Gentry, and Zulfikar Ramzan. "Quasimodo: Efficient certificate validation and revocation." *International Workshop on Public Key Cryptography*. Springer Berlin Heidelberg, 2004.

[4] Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." *Annual International Cryptology Conference*. Springer Berlin Heidelberg, 2001.

[5] Canetti, Ran, Ben Riva, and Guy N. Rothblum. "Two 1-Round Protocols for Delegation of Computation." *IACR Cryptology ePrint Archive* 2011 (2011): 518.

[6] Feige, Uriel, and Joe Kilian. "Making games short." *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*. ACM, 1997.

[7] Libert, Benoît, and Damien Vergnaud. "Adaptive-ID secure revocable identity-based encryption." *Cryptographers' Track at the RSA Conference*. Springer Berlin Heidelberg, 2009.

[8] Yu, Shucheng, et al. "Attribute based data sharing with attribute revocation." *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*. ACM, 2010.