ABHIYANTRIKI
An International Journal of Engineering & Technology
(A Peer Reviewed & Indexed Journal)
Vol. 3, No. 5 (May, 2016) http://www.aijet.in/ eISSN: 2394-627X

Attribute based Encryption with Outsourced Revocation in Cloud Computing

Kiran P.
Associate Professor
Deptt. of Computer Science & Engineering
RNS Institute of Technology, Bengaluru, India

Rajani S. C.*
PG Student
Deptt. of Computer Science & Engineering
RNS Institute of Technology, Bengaluru, India

Abstract

Attribute Based Encryption (ABE) which simplifies the public key and authentication administration at Public Key Infrastructure (PKI) is a vital distinct option for open key encryption. Be that as it may, one of the fundamental effectiveness downsides of ABE is the overhead calculation at Private Key Generator (PKG) during user revocation. In this paper, going for handling the basic issue of personality renouncement, it brings outsourcing calculation into ABE for the first time and propose a revocable ABE plan in the server-helped setting. Our plan offloads the majority of the key related operations aimed key-issuing and key-upgrade procedures to a Key Upgrade Cloud Service Provider, leaving just a consistent number of basic operations for PKG and clients to perform locally. This objective is accomplished by using a novel conspiracy safe strategy: it utilizes a private key for every client, in which an AND entryway is included to associate and bound the character part and the time segment. Besides, we propose another development which is provable secure under the as of late formulized Refereed Delegation of Computation model. At long last, we give broad test results to exhibit the proficiency of our proposed development.

Keywords*: Attribute encryption, Revocation, Outsourcing, Cloud computing.*

****Author for correspondence*** rajanisc15@gmail.com

1. Introduction

Attribute Based Encryption (ABE) is a fascinating distinct option for public key encryption, which is proposed to simplify key administration in a declaration based Public Key Infrastructure (PKI) by utilizing human-coherent characters (e.g., interesting name, email address, IP address, and so forth) as public keys. In this way, sender utilizing ABE does not have to gaze upward open key and endorsement, yet specifically encodes message with collector's character. As needs be, recipient getting the private key connected with the relating character from Private Key Generator (PKG) can unscramble such cipher text. Despite the fact that ABE permits a self-assertive string as the general population key which is considered as engaging focal points over PKI, it requests an effective renouncement component. In particular, if the private keys of a few clients get traded off, It gives intend to disavow such clients from framework. In PKI setting, repudiation instrument is acknowledged by affixing legitimacy periods to declarations or

utilizing included blends of techniques. The bulky administration of declarations is definitely the weight that IBE endeavors to reduce. Despite the fact that ABE permits a subjective string as the general population key which is considered as engaging preferences over PKI, it requests an effective repudiation instrument. In particular, if the private keys of a few clients get traded off, we should give intend to repudiate such clients from framework. In PKI setting, denial component is acknowledged by annexing legitimacy periods to testaments or utilizing included mixes of strategies [1][2][3]. By and by, the lumbering administration of testaments is absolutely the weight that IBE endeavors to ease. To the extent we know, however denial has been completely contemplated in PKI, few denial instruments are known in ABE. In [4], Boneh and Franklin recommended that clients reestablish their private keys intermittently and senders utilize the collectors' personalities connected with current time period. In any case, this component would result in an overhead load at PKG. In another word, every one of the clients despite whether their keys have been denied or not, have to contact with PKG occasionally to demonstrate their personalities and upgrade new private keys. It requires that PKG is online and the secure channel must be kept up for all exchanges, which will turn into a bottleneck for IBE framework as the quantity of clients develops. In 2008, Boldyreva, Goyal and Kumar [5] displayed a revocable IBE plan. Their plan is based on the possibility of fluffy IBE primitive [6] yet using a double tree information structure to record clients' personalities at leaf hubs. In this way, key-redesign productivity at PKG can be essentially decreased from straight to the tallness of such double tree (i.e. logarithmic in the quantity of clients). In any case, we bring up that however the double tree presentation can accomplish a relative elite, it will bring about other issues: (a) PKG needs to create a key pair for every one of the hubs on the way from the personality leaf hub to the root hub, which results in unpredictability logarithmic in the quantity of clients in framework for issuing a solitary private key. (b) The measure of private key develops in logarithmic in the quantity of clients in framework, which makes it troublesome in private key stockpiling for clients. (c) As the quantity of clients in framework develops, PKG needs to keep up a parallel tree with a lot of hubs, which presents another bottleneck for the worldwide framework. In coupled with the advancement of distributed computing, there has risen the capacity for clients to purchase on-interest registering from cloud-based administrations, for example, Amazon's EC2 and Microsoft's Windows Azure. Along these lines it seeks another working worldview for bringing such cloud administrations into IBE repudiation to settle the issue of proficiency and capacity overhead depicted previously.

An innocent methodology would be to just hand over the PKG's lord key to the Cloud Service Providers (CSPs). The CSPs could then essentially overhaul all the private keys by utilizing the conventional key upgrade system [4] and transmit the private keys back to unrevoked clients. Notwithstanding, the innocent methodology depends on an unlikely suspicion that the CSPs are completely trusted and is permitted to get to the expert key for IBE framework. Unexpectedly, practically speaking the open mists is likely outside of the same trusted space of clients and is interested for clients' individual protection. Therefore, a test on the best way to outline a safe revocable IBE plan to decrease the overhead calculation at PKG with an untrusted CSP is raised. In this framework, bring outsourcing calculation into ABE disavowal, and formalize the security meaning of outsourced revocable ABE surprisingly to the best of our insight. This framework propose a plan to offload all the key era related operations amid key-issuing and key-upgrade, leaving just a consistent number of basic operations for PKG and qualified clients to perform locally. In this plan, as with the recommendation in, we understand disavowal through upgrading

the private keys of the unrevoked clients. In any case, dissimilar to that work [4] which insignificantly links time period with personality for key era/upgrade and requires to re-issue the entire private key for unrevoked clients, This framework propose a novel plot safe key issuing strategy: It utilizes a mixture private key for every client, in which an AND entryway is included to associate and bound two sub-segments, in particular the character segment and the time segment. At to start with, client can get the personality segment and a default time part (i.e., for current time period) from PKG as his/her private key in key-issuing. A short time later, keeping in mind the end goal to look after decrypt ability, unrevoked clients needs to intermittently ask for on key-overhaul for time part to a recently presented substance named Key Update Cloud Service Provider (KU-CSP). This plan does not need to re-issue the entire private keys, yet simply need to redesign a lightweight segment of it at a particular element KU-CSP. It additionally indicates that (a) with the guide of KU-CSP, client needs not to contact with PKG in key-overhaul, as such, PKG is permitted to be disconnected from the net in the wake of sending the renouncement rundown to KU-CSP. (b) No protected channel or client validation is required amid key-overhaul in the middle of client and KU-CSP.

2. Preliminary Work

In this segment, we give a brief audit on some cryptographic foundation and personality based encryption.

a. Cryptographic Background

Definition 1: (Bilinear guide) Let G, GT cyclic gatherings of prime request q, composing the gathering activity multiplicatively. g is a generator of G. Let e : G×G → GT be a guide with the accompanying properties:

- Bilinearity: e(ga 1, gb2) = e(g1, g2)ab for all g1, g2 ∈ G, and a, b ∈R Zq;
- Non-decadence: There exists g1, g2 ∈ G with e(g1, g2)= 1, at the end of the day, the guide does not send all sets in G×G to the personality in GT;
- Computability: There is an effective calculation to figure e (g1, g2) for all g1, g2 ∈ G.

Definition 2: (DBDH issue) The choice Bilinear Diffie-Hellman (DBDH) issue is that, given g, gx, gy, gz ∈ G for obscure arbitrary quality x, y, z ∈R Zq, and T ∈R GT , to choose on the off chance that T = e(g, g)xyz.

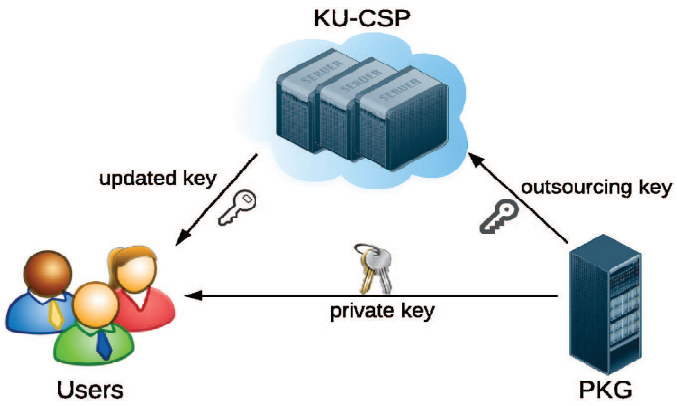


Fig.1: Framework Model for ABE with Outsourced Revocation

b. Attribute based Encryption

An ABE plan which commonly includes two substances, PKG and clients (counting sender and recipient) is comprised of the accompanying four calculations.

- Setup (λ): The setup calculation takes as data a security parameter λ and yields the general population keys PK and the expert key MK. Note that the expert key is kept mystery at PKG.

- KeyGen (MK, ID) : The private key era calculation is keep running by PKG, which takes as data the expert key MK and client's character ID ∈ {0, 1}∗. It gives back a private key SKID relating to the character ID.
- Encrypt (M, ID): The encryption calculation is controlled by sender, which takes as information the collector's character ID and a message M to be encoded. It yields the cipher-text CT.
- Decrypt (CT, SKID): The decoding calculation is controlled by beneficiary, which takes as info the cipher-text CT and his/her private key SKID. It gives back a message M or a mistake.

An ABE plan must fulfill the meaning of consistency. In particular, when the private key SKID produced by calculation KeyGen when it is given ID as the data, then Decrypt (CT,SKID) = M where CT = Encrypt(M, ID).

The inspiration of IBE is to disentangle endorsement administration. For instance, when Ali sends an email to Bober at bober@company.com, she essentially encodes her message utilizing Weave's email address "bober@company.com", however does not require acquiring Bober's open key testament. At the point when Bob gets the scrambled email he confirms himself at PKG to acquire his private key, and read his email with such a private key.

3. Problem Statement

a. Framework Model

We display framework model for outsourced revocable IBE in Fig. 1. Contrasted and that for normal IBE plan, a KU-CSP is included to acknowledge denial for traded off clients. Really, the KU-CSP can be imagined as an open cloud keep running by an outsider to convey fundamental registering capacities to PKG as institutionalized administrations over the system. Commonly, KU-CSP is facilitated far from either clients or PKG, yet gives an approach to lessen PKG calculation and capacity cost by giving an adaptable, indeed, even provisional expansion to foundation. At the point when denial is activated, rather than re-asking for private keys from PKG in, unrevoked clients need to approach the KU-CSP for upgrading a lightweight segment of their private keys. In spite of the fact that numerous points of interest are included in KU-CSP's arrangement, in this paper we just coherently imagine it as a registering administration supplier, and concern step by step instructions to plan secure plan with an untrust KU-CSP. In light of the framework model proposed, we can characterize the outsourced revocable ABE plan.

IBE definition, the KeyGen, Encrypt and Decrypt calculations are re-imagined as takes after to coordinate time segment. Note that two records RL and TL are used in our definition, where RL records the personalities of disavowed clients and TL is a connected rundown for past and current time period.

- KeyGen (MK,ID,RL,TL): The key era calculation keep running by PKG takes as information – an expert key MK, a personality ID, a repudiation list RL and a period list TL. In the event that ID ∈ RL, the calculation is prematurely ended. Else, it sends the private key Slide = (IK[ID], TK[ID]Ti) to client where IK[ID] is the personality part for private key SKID and TK[ID]Ti is its time part for current time period Ti. Furthermore, the calculation sends an outsourcing key OKID to KU-CSP.

- Encrypt (M,ID,Ti,PK): The encryption calculation keep running by sender takes as information – a message M, a character ID and a time period Ti. It yields the cipher-text CT.
- Decrypt (CT,SKID): The decoding calculation keep running by beneficiary takes as info – a cipher-text CT encoded under character ID and time period Ti and a private key SKID= (IK[ID], TK[ID]Tj). It yields the first message M on the off chance that ID = ID and Ti = Tj, generally yields ⊥. Furthermore, two calculations are characterized to acknowledge renouncement at KU-CSP through redesigning the private keys of unrevoked clients.
- Revoke (RL, TL, {IDi1, . . . , IDik }): The denial calculation keep running by PKG takes as information – a disavowal list RL, a period list TL and the arrangement of characters to be renounced {IDi1 , IDi2, . . . , IDik }. It yields an upgraded time period Ti+1 and additionally the upgraded denial list RL and time list TL.
- KeyUpdate (RL,ID,Ti+1,OKID): The key redesign calculation keep running by KU-CSP takes as data – a repudiation list RL, a character ID, a period Ti+1 and the outsourcing key OKID for character ID. It yields client's upgraded time segment in private key TK[ID]Ti+1 if his character ID does not have a place with RL, generally, yields error.

In this paper, we talk about client repudiation that is the way to deny clients of decrypt ability regardless of the possibility that they have been issued their private keys. To this end, we insert a period into private key in a sharp way for repudiation. In particular, in the same sample outlined in Section II-B, Ali in our setting not just encodes message with Bober's email address "bober@company.com" yet additionally with current time period (e.g., "Thu Apr 28 2016"). At the point when gets the scrambled email, Bob then acquires his private key comprising of a personality segment and a period segment from PKG. With the both proper segments, the email can be perused. Assume Bober is traded off. At that point, the time parts of the various clients are redesigned by KU-CSP with another time period. From that point on, the message sent to Bober ought to be scrambled with Bob's email address and the overhauled time period. Since Bob does not have room schedule-wise part relating to the overhauled time period, the accompanying scrambled messages can't be decoded by Bob regardless of the possibility that they are planned for him. The test in outlining the outsourced revocable IBE plan is the way to keep a plot amongst Bob and other unrevoked exploitative clients. In particular, a deceptive client (named john) can share her upgraded time part (i.e., "Fri May 19 2016") with Bob, and Bob decode cipher-text regardless of the possibility that Bober simply has the past one (i.e., "Thu May 18 2016"). We will appear step by step instructions to stay away from such an intrigue later.

b. Security Definition

We expect that KU-CSP in the proposed framework model is semi-trusted. In particular, it will take after our convention yet attempt to discover however much mystery data as could be expected in view of its ownership. In this way, two sorts of foes are to be considered as takes after.

- Type-I: It is characterized as an inquisitive client with personality ID yet repudiated before time period Ti. Such foe tries to get valuable data from cipher-text expected for him/her at or after Ti (e.g. time period Ti, Ti+1, . . .) through conspiring with different clients regardless of the fact that they are unrevoked. Hence, it is permitted to request private key including character part and overhauled time segment for agreeable clients. We determine that under the presumption that KU-CSP is semi-trusted, sort I enemy can't get outsourcing key for any clients.

- Type-II: It is characterized as an inquisitive KU-CSP which expects to acquire helpful data from cipher-text proposed for some objective personality ID at time period Ti. Such foe not just have of outsourcing keys for all clients in the framework, additionally can get client's private key through conspiring with whatever other client with character ID. It is noted that to make such assault sensible, we should limit ID = ID. Having the instincts above, we can characterize CCA security diversion for sort I and sort II foe separately for our setting.

Definition 3: A character based encryption with outsourced disavowal plan is semantically secure against versatile chosen cipher-text assault (IND-ID-CCA) if no polynomial limited foe has a non-irrelevant point of interest against challenger in security diversion for both sort I and sort II foe. At last, past the CCA security, we likewise determine that 1) An IBE with outsourced disavowal plan is IND-ID-CPA secure (or semantically secure against picked plaintext assault) in the event that no polynomial time foe has non-immaterial point of interest in altered recreations for both sort I and sort II enemy, in which the decoding prophet in both stage 1 and stage 2 is evacuated; 2) An IBE with outsourced denial plan is secure in particular model if no polynomial time enemy has non negligible advantage in changed amusements for both sort.

4. Execution Evaluation

In this segment, we will give an exhaustive trial assessment of the development proposed in segment IV. We assemble our test bed by utilizing 64-bit M2 high-memory fourfold additional substantial Linux servers in Amazon EC2 stage as KU-CSP, and a Linux machine with Intel(R) Core(TM)2 Duo CPU timed at 2.40 GHz what's more, 2 GB of framework memory as the client and PKG. Note that in every one of the assessments, the gatherings G and GT are chosen in 160-piece what's more, 512-piece length individually.

a. Execution Evaluation for Overall Scheme

Firstly, we plan to assess the effectiveness of our outsourced revocable plan by contrasting the aggregate time taken amid each stage with the first ABE [4] which does not consider repudiation. It is not astounding to see that our plan takes additional time since we consider the revocability issue. Note that our plan has the same setup calculation with the IBE plan in [4]. Our key-issuing stage is relative longer than that in the IBE plan [4]. This is on account of we implant a period part into every client's private key to permit intermittently redesign for denial, coming about that some extra computations are in our execution, this reads and hash the framework time for current time period, and create the time component in a way comparative that for personality required in our plan to introduce this segment. Our encryption also, decoding is somewhat more than the ABE plan [4], which is likewise because of the presence of the time part. The client needs to perform an extra encryption/decoding for this part, as opposed to simply scramble/unscramble the personality part. To aggregate up, our revocable plan accomplishes both attribute based encryption/unscrambling and revocability without presenting huge overhead contrasted with the first IBE plan.

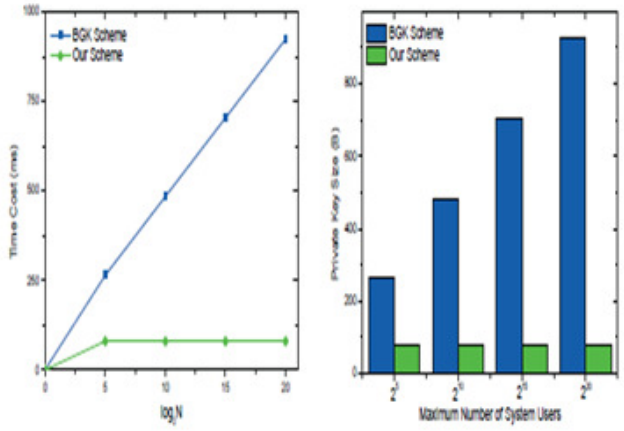
b. Execution Evaluation for Revocation

Besides, we endeavor to recreate the situation of multi-client repudiation, and demonstrate a broad correlation between our outsourced repudiation plan and another revocable IBE plan – BGK plan [5]. Note that in this arrangement of trials, we utilize a 32- bit whole number to

recognize every hub in double tree which is used in BGK plan [5] for overseeing clients. Our correlation is in wording of the key-issuing stage and the key-upgrade stage.

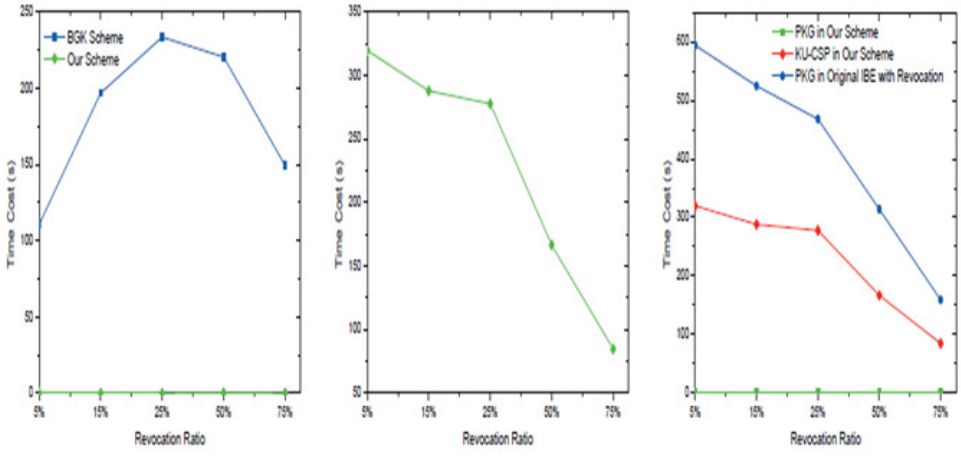
(1) Key-Issuing Stage: In Fig. 2(a), we fluctuate the most extreme number of clients in the framework and demonstrate the reacting time for a solitary key era demand. It is not hard to see that the reacting time in BGK plan [5] is in proportion of O(log2(N)) where N is the most extreme number of clients in framework.

(2) Key Update Stage: In this examination, we arbitrarily pick 5% to 75% clients and think about the aggregate time of overhauling private keys for the rest clients. For effortlessness, we simply show a case also, look at the key-redesign time at PKG in denial for the situation of 215 framework clients. It can be seen that the effectiveness bend of BGK plan [5] demonstrates an allegorical shape, and at the 25% denial proportion, the proficiency accomplishes the most minimal point in our assessment. This is on the grounds that the hole the leaf hubs to be disavowed has an extensive number yet low conglomeration degree, which requires that we need to redesign a considerable measure of inner hubs for key update. Be that as it may, in our plan, such a conduct is evaded, and only an irrelevant steady time is taken at PKG. All the more for the most part, this steady key-upgrade effectiveness is really accomplished by our plan with in any case to the quantity of framework clients since we delegate the renouncement to KU-CSP, however BGK plan [5] requires an expanding time cost with the quantity of framework clients. As needs be, we likewise demonstrate the time cost at KU-CSP in our plan for upgrading private keys for all the unrevoked clients in the repudiation proportion going from 5% to 75%.



(a) Responding Time for Single Key Generation Request (b) Private Key Size

Fig. 2: Comparisons in Key-Issuing (*N* is the maximum number of users in system)



(a) Key Update at PKG (b) Key Update at KU-CSP (c) Key Update Comparison with [4]

Fig. 3: Comparisons in Key Update (Case: 2^{15} System Users)

5. Related Work

a) Revocable IBE Presented by [13] and firstly actualized by Boneh and Franklin [4] and in addition [14], IBE has been investigated seriously in cryptographic group. On the part of development, these first plans [4], [14] were demonstrated secure in arbitrary prophet. Some consequent frameworks accomplished provable secure in standard model under specific ID security or versatile ID security. As of late, there have been various cross sections based developments for IBE frameworks. In any case, worried on revocable IBE, there is little work exhibited. As specified some time recently, Boneh and Franklin's proposal [4] is progressively a suitable arrangement however unrealistic. Hanaoka et al. proposed a path for clients to occasionally restore their private keys without interfacing with PKG. Be that as it may, the suspicion required in their work is that every client needs to have an alter safe equipment gadget. Another arrangement is middle person helped renouncement: In this setting there is an uncommon semi-trusted outsider called a middle person who helps clients to unscramble each cipher-text. On the off chance that a character is disavowed then the go between is told to quit making a difference the client. Clearly, it is illogical since all clients can't decode all alone and they have to speak with go between for every decoding. As of late, Lin et al. proposed a space productive revocable IBE component from non-monotonic Attribute-Based Encryption (ABE), however their development requires O(r) times bilinear blending operations for a solitary decoding where r is the quantity of denied clients. To the extent we know, the revocable IBE plan exhibited by Boldyreva et al. [5] remains the best arrangement at this moment. Libert and Vergnaud enhanced Boldyreva's development [5] to accomplish versatile ID security. Their work concentrated on security upgraded, yet acquires the comparative detriment as Boldyreva's unique development. As we said some time recently, they are short away for both private key at client and paired tree structure at PKG.

b) Other Revocation Technique another business related to us starts from Yu et al. The creators used intermediary re-encryption to propose a revocable ABE plan. The trusted power just needs to redesign expert key as indicated by trait repudiation status in every time period and issue intermediary re-encryption key to intermediary servers. The intermediary servers will then re-scramble cipher-text utilizing the re-encryption key to make beyond any doubt all the unrevoked clients can perform fruitful unscrambling. We determine that an outsider administration supplier is presented in both Yu et al. and this work. In an unexpected way, Yu et al. used the outsider (work as an intermediary) to acknowledge disavowal through re-encrypting cipher-text which is just adjust to the exceptional application that the cipher-text is put away at the outsider. Be that as it may, in our development the repudiation is acknowledged through upgrading private keys for unrevoked clients at cloud administration supplier which has no limits on the area of cipher-text.

c) Outsourcing Computation: The issue that how to safely outsource various types of costly calculations has drawn impressive consideration from hypothetical software engineering group for quite a while. Chaum what's more, Pedersen firstly presented the thought of wallets with eyewitnesses, a bit of secure equipment introduced on the customer's PC to perform some costly calculations. Atallah et al. exhibited a structure for secure outsourcing of investigative calculations, for example, grid increase and quadrature. All things considered, the arrangement utilized the camouflage strategy and accordingly leaded to spillage of private data. Hohenberger and Lysyanskaya [9] proposed the principal outsource-secure calculation for measured

exponentiations taking into account pre-calculation and server aided calculation. Atallah and Li researched the issue of figuring the alter separation between two successions and exhibited a proficient convention to safely outsource grouping correlation with two servers. Besides, Benjamin and Atallah [32] tended to the issue of secure outsourcing for generally appropriate direct mathematical calculations. In any case, the proposed convention required the costly operations of homomorphic encryption. Atallah and Frikken [12] further considered this issue and gave enhanced conventions in light of the purported feeble mystery covering up supposition. Chen et al. [11] made a proficiency change on the work [9] and proposed another plan for outsourcing single/concurrent measured exponentiations.

6. Conclusion

In this paper, concentrating on the basic issue of character denial, it bring outsourcing calculation into IBE and propose a revocable plan in which the repudiation operations are assigned to CSP. With the guide of KU-CSP, the proposed plan is full-highlighted: (1) It accomplishes consistent effectiveness for both calculation at PKG and private key size at client; (2) User needs not to contact with PKG amid key-upgrade, at the end of the day, PKG is permitted to be disconnected from the net in the wake of sending the repudiation rundown to KU-CSP; (3) No safe channel or client confirmation is required amid key-upgrade amongst client and KU-CSP. Besides, we consider acknowledging revocable IBE under a more grounded foe model. We exhibit a propelled development also; indicate it is secure under RDoC model, in which no less than one of the KU-CSPs is thought to be straightforward. Consequently, regardless of the fact that a repudiated client and both of the KU-CSPs intrigue, it can't help such client re-get his/her decrypt ability. At long last, we give broad test results to illustrate the proficiency of our proposed development.

References

[1] W Aiello, S Lodha, & R Ostrovsky. (1998). Fast digital identity revocation. *Advances in Cryptology – CRYPTO'98*. Springer.

[2] V Goyal. (2007). Certificate revocation using fine grained certificate space partitioning. *Financial Cryptography and Data Security (LNCS).* Berlin: Springer. Vol. 4886, pp. 247–259.

[3] F Elwailly, C Gentry, & Z Ramzan. (2004). Quasimodo: Efficient certificate validation and revocation. *Public Key Cryptography (LNCS).* Berlin: Springer. Vol. 2947, pp. 375–388.

[4] D Boneh, & M Franklin. (2001). Identity-based encryption from the weil pairing. *Advances in Cryptology – CRYPTO 2001 (LNCS)*. Berlin: Springer. Vol. 2139, pp. 213–229.

[5] A Boldyreva, V Goyal, & V Kumar. (2008). Identity-based encryption with efficient revocation. *In:* Proceedings of the 15th ACM Conf. on Comp. and Comm. Security. NewYork: ACM. pp. 417–426.

[6] A Sahai, & B Waters. (2005). Fuzzy identity-based encryption. *Advances in Cryptology EUROCRYPT 2005 (LNCS)*. Berlin: Springer. Vol. 3494, pp. 557–557.

[7] R Canetti, B Riva, & GN Rothblum. (2011). Two 1-round protocols for delegation of computation. *Cryptology ePrint Archive*, Report 2011/518.

[8] U Feige, & J Kilian. (1997). Making games short. Proceedings of the 29th annual ACM Symp. on Theory of Computing. New York: ACM. pp. 506–516.

[9] S Hohenberger, & A Lysyanskaya. (2005). How to securely outsource cryptographic computations. Proceedings of the 2nd Inter. Conf. on Theory of Cryptography. Berlin: Springer-Verlag. pp. 264–282.

[10] R Canetti, B Riva, & G Rothblum. (2012). Two protocols for delegation of computation. *Information Theoretic Security (LNCS)*. Berlin: Springer. Vol. 7412, pp. 37–61.

[11] X Chen, J Li, J Ma, Q Tang, & W Lou. (2012). New and secure outsourcing algorithms of modular exponentiations. 17th European Symp. on Research in Computer Security, 2012.

[12] MJ Atallah, & KB Frikken. (). Securely outsourcing linear algebra computations. Proceedings of the 5th ACM Symp. on Information, Computer and Communications Security. New York: ACM. pp. 48–59.

[13] A Shamir. (1985). Identity-based cryptosystems and signature schemes. *Advances in Cryptology – CRYPTO (LNCS).* Berlin: Springer. Vol. 196, pp. 47–53.

[14] C Cocks. (2001). An identity based encryption scheme based on quadratic residues. *Cryptography and Coding (LNCS)*. Berlin: Springer. Vol. 2260, pp. 360–363.