International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S, October 2019

Revocable IBE combined with CRA to overcome the inadaptability problem

Latha.K, Sheela.T

Abstract— ***Identity based encryption (IBE) is an open key cryptographic system and takes out the requesting of the Public key infrastructure(PKI) and confirmation relationship by and large key settings. Due to the nonappearance in PKI, the cancelation problem has become a primary issue in the IBE settings. Two or three cancellable IBE plans have been already proposed concerning this point. As of late, by embeddings an outsourcing figuring framework into the IBE, Li et al. presented a cancellable IBE scheme with the feature of key-update cloud authority association (KU-CSP). Regardless, their arrangement faces two disadvantages. One demerit is that the costs of figuring, correspondence are more than past cancellable IBE designs. Alternate limitation is nonattendance of adaptability as in KU-CSP should maintain secret regard for individual customer. Here another cancellable IBE plot with cloud cancellation authority (CRA) to understand the two disadvantages in which the execution is by and large upgraded and the CRA has only a system puzzle for each one of their customers.***

Index Terms— ***Encryption technique, Cloud computing, outsourcing computation, Authentication, cancellation authority.***

I. INTRODUCTION

Cloud computing is one of the most popular technology which attracts the eyes of both researchers as well as industries. The cloud computing is a shared virtualized computing resource which may possess resources such as storage, infrastructure, services and software. The main reason for the usage of cloud computing is its utility. Here there is no need for any organization to purchase any components. Instead they can use all the required components virtually that are provided by other cloud services. Hence it reduces the expenditure cost on components as well as the maintenance cost. One of the main drawback of most cloud services is the security provided by those services. The recent survey done by oracle shows that 87% percent of the cloud users are feared of the security. One of the main concern is the integrity of the outsource file since the resource does not possess any physical link with that file or data. In order to face this crisis several key cryptography system were proposed.

A public key system based on identity is one the best alternative route for key cryptography. In an identity-based public key system setting will avoid the use of public key infrastructure (PKI). Usually a setting called ID-PKS will consist of user and trustable third party module which is responsible for the generation of private key. The private key generator is responsible for creating each user's private key with the help of certain information such as email id, name, security number etc. Hence no certificates and PKI is required this kind of cryptographic mechanism [9]. In ID based encryption the system the message is directly encrypted by the user using the receiver's ID. In the same way the receiver should use the private key which is present with him to decrypt the cipher text. Since the system should give a revocation mechanism, an issue of how to revoke unwanted or misbehaving user is raised. Certificate revocation list [2] is one of the most commonly used revocation approach in most of the public key settings[15]. Usually in CRL the user receives the public key and validates it to make sure that the obtained public key will not be revoked. This kind of procedure requires online facility in order to have a better communication. In order to enhance the performance of the revocation process, several approaches were proposed.

II. RELATED WORKS

In 2001, Bonie and Franklin proposed a identity based scheme [4] in which each and every user will be receiving a single and latest private key produced by the private key generator (PKG). The time duration may be of any range such as hours, days and even weeks. The user uses the ID of the receiver and the period for encrypting the data and the receiver uses the user's ID to decrypt the encrypted data using the private key. Therefore the user is asked to update the private key in a periodical range. If the system finds any misbehaving or other malfunction by the user, then the private key generator (PKG) will stop giving the private key to the user. Thus the service is stopped. But this process is done individually to each user which leads to high system load in the private key generator. Usually an online mediator assists the user. In this type of encryption both user and mediator are involved. Since the entire application uses online facility, neither the user nor the mediator will be able to cheat each other and when the number of users increases, the load on the PKG increases. In spite of being overloaded by the large number of user, the PKG produces separate keys to the user which leads to the decrease in the performance as well as the efficiency of the system. At the same time when the system revokes the service from the user then the online mediator stops assisting the user. Then again, in Boneh and Franklin's disavowal strategy, every one of the clients should occasionally refresh the new private keys which they receive from the PKG.

Manuscript published on 30 October 2019.
***** Correspondence Author (s)

Latha.K, Research scholar, Faculty of computer science and engineering, Sathyabama Institute of Science & Technology, Ch-119.
Assistant Professor, Department of Computer Science and Engineering Sri Sai Ram Engineering College. Email: klathasn@gmail.com
Sheela.T, Professor& HOD, Dept of ,IT, Sri Sai Ram Engineering College, Chennai 600 044,Tamil Nadu, India

While the quantity of clients increments, the heap of the key update turns into a problem for PKG. In the year 2008, Boldyreva et al. suggested a reversible IBE plot to enhance the key refresh productivity. The revocable IBE[27] conspire depends on the idea of fuzzy based IBE and receives the total subtree strategy in order to diminish the amount of key update from direct to logarithmic in the quantity of clients. In fact, through double tree information structure of clients, the conspire proficiently mitigates the key-refresh heap of PKG. Besides, Libert and Vergnaud enhanced the security suggested by Boldyreva et al's. revocable IBE conspire by showing a versatile ID secure plan. By the by Boldyreva et al's. plot still outcomes in a few issues: (1) The private key size of each client is about 3log n focuses in a elliptical bend, here n denotes the quantity of leaf hubs (clients) in the parallel tree. (2)The conspire likewise brings about huge calculation work for encrypting and decoding systems. (3) It serves a gigantic stack for PKG to keep up the twofold tree with a huge measure of clients.

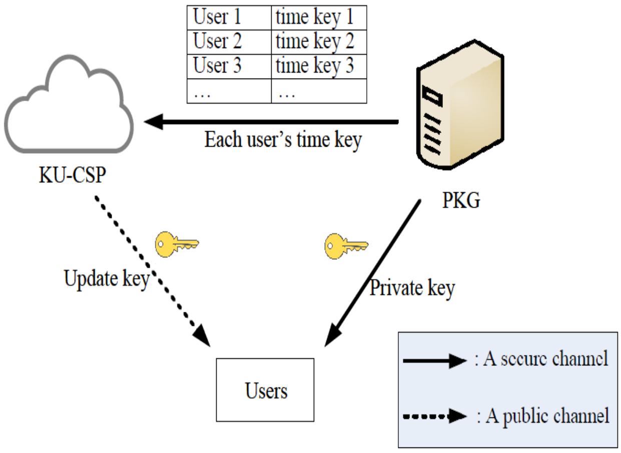


Fig.1 Li et al's model

In the meanwhile, an irregular mystery esteem (time key) must be produced by the PKG for clients and the PKG must send it to KU-CSP. At that point the KUCSP produces refresh key of client for the present time by making use of the related time key and then sends it to the client through open channel. In order to renounce a client, the PKG will be asking KU-CSP to quit providing the refresh key of the client based on the new time. Their framework demonstrate is delineated in. But, this plan has two defects. One defect is higher calculation and the correspondence costs when compared with the previous revocable IBE plans.

III. PROPOSED MODEL

We present a new revocable IBE conspire with the CRA (Cloud revocation authority). The suggested plot has the upsides of Tseng and Tsai's revocable IBE plan and Li et al's. conspire. In this specifically, private key of every client will still comprise the personality key and the time based period refresh key. Here we showcase the cloud revocation authority (CRA) to supersede the portion of Li et al's. KU-CSP plot. The CRA will have to just hold an irregular mystery esteem (ace time key) for all the clients such that it does not influence the security of revocable IBE conspire. The CRA will make use of the ace time key to create the refresh key based on current time occasionally for each of the permitted client and then sends them to client through a open channel. It is explicit that the proposed plan will take care of overcoming the inadaptability problem of KU-CSP. In this article, we initially propose the structure of the proposed reversible IBE conspire with the CRA and describe the security ideas to demonstrate conceivable dangers and assaults. As needs be, another revocable IBE plot with CRA is also proposed. The enemy demonstrate displayed and it comprises of two enemies, in particular, an insider foe (or a disavowed client) and an outside enemy. For the purpose of security examination, we show that the plan is semantically safe against versatile identity and picked cipher text attacks (CCA) in the irregular prophet demonstrate under bilinear choice[35]. At long last, with the suggested revocable IBE conspire with CRA, we build CRA-supported verification plan with limited advantages for handling with extensive amount of differing cloud administrations.

IV. SYSTEM OPERATION

We show the framework tasks of our suggested revocable IBE conspire with the CRA. The proposed framework comprise three parts, specifically, a cloud revocation authority (CRA), the private key generator (PKG), and clients (sender and beneficiaries). To start with, the PKG chooses a key called as master secret key, an master time key 'm' and an aggregate count z of periods, and will send the ace time key to CRA. PKG utilizes this ace mystery key to process the character key ID of the client along with the personality ID, and then send the character key to the client through a secure channel. Then, the cloud revocation authority[4] is dependable to deliver the time refresh key for all of their non-repudiated clients through utilization of the ace time key. In order to perform this, during the start of every I period, CRA will utilize the master time key and the personality ID of a non-repudiated client to create the current-time update key. It sends it to the client by means of an open channel (e.g. email). At the point when a transmitter needs to send the message M to the recipient with personality identity ID[1] at period I, the sender generates a cipher text which is then sent to the collector, here E means encryption calculation of the proposed revocable IBE conspire with CRA. After getting the cipher text, the beneficiary uses the personality key and time refresh key to unscramble the cipher text. Compared to previous IBE definition, the Key Generation, the Encrypt and Decrypt calculations are reclassified to incorporate time part.

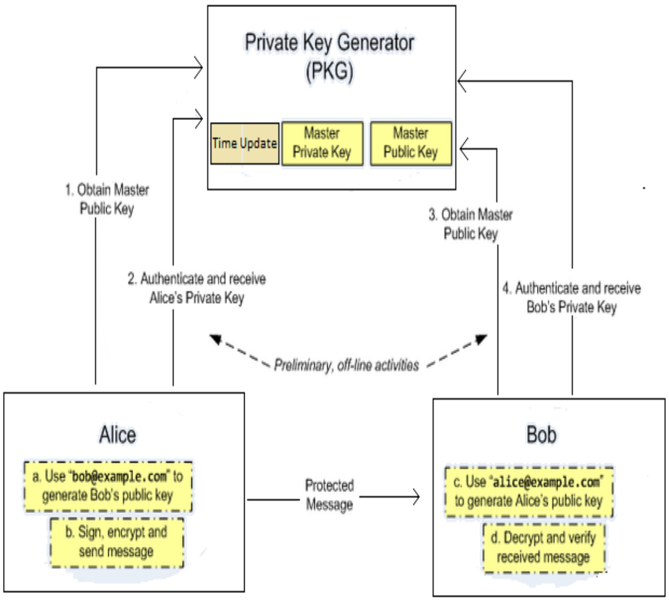

Private Key Generator (PKG)
Time Update
Master Private Key
Master Public Key
1. Obtain Master Public Key
2. Authenticate and receive Alice's Private Key
3. Obtain Master Public Key
4. Authenticate and receive Bob's Private Key
Preliminary, off-line activities
Alice
a. Use "bob@example.com" to generate Bob's public key
b. Sign, encrypt and send message
Protected Message
Bob
c. Use "alice@example.com" to generate Alice's public key
d. Decrypt and verify received message

Fig2 Architecture diagram

V. MODULES USED AND THE FLOW OF DATA

The proposed concept is categorized into four modules. These four modules construct the entire architecture of the proposed model. The modules used are as follows:

- User-interface
- Trustee
- Key-distribution centre

A. User-Interface:

The user interface (UI), in the recent field of human–computer interaction is where connections among human and the computer will take place. The main objective is to allow successful task and the control of this computer from the people end, In the machines all the while nourishes back the data that will guide the administrators' primary leadership process. The cases of the above said extensive scheme of UIs include the intuitive segments of PC working structure, hand apparatus, substantial hardware administration controls, and process controls. Different expressions for UI are man– machine interface (MMI) and when the machine being referred to is a human–computer interface.

B. Trustee:

'Trust (or, symmetrically, doubt) is a specific level of the subjective likelihood with which a specialist surveys that another operator or gathering of specialists will play out a specific activity, both before he can screen such activity (or autonomously of his ability ever to have the capacity to screen it) and in a setting in which it influences his own activity'. The idea of trust, acclimated to the instance of two gatherings associated with a collaboration, can be displayed as takes after: An element A is supposed to assume the other element B when element A believes that element B will carry on precisely of course. Two elements engaged with a connection can be called Trustor and Trustee, individually. In a putting stock in activity, Trustor must choose whether and the amount to believe a Trustee in view of rather an evaluation of its chronicled involvement and the trustee's notoriety than a visually impaired figure. The Trust Degree shows the reliable level of a specific element which is likewise named two essential put stock in types, in particular, Direct Trust Degree and Indirect Trust Degree. Coordinate trust degree is to be refreshed by every history-based conduct and experience of the element in a given setting. Nonetheless, aberrant trust degree called Reputation additionally can be related with numerous wellsprings of incorrectness not present in a trustor's immediate affair, which is chosen by proposals from other at any point given assessment elements. General put stock in degree, when all is said in done, is utilized to assess the dependable level too, which is processed by weighted normal estimation of direct put stock in degree and backhanded confide in degree. When all is said in done, trust relationship is variable inferable from the dynamic idea of associations and conduct advancement in distributed computing condition. Cloud clients believe the capacity of cloud specialist co-ops to furnish administrations with the expansion of their fruitful collaborations. A cloud client will progressively change and alter its reliability to a cloud specialist organization over the long haul. In this manner, Trust is a constant procedure instead of a detached activity, in which one element's trust to another is to a specific degree, from low to medium, and after that to high, or from high to medium, and afterward to low. Trust show in distributed computing needs to confront numerous difficulties conversely with conventional model because of the assorted variety of put stock seeing someone in cloud condition, which includes such a large number of various connections between and among end clients, information proprietors and cloud specialist co-ops. Cloud clients may be characterized as trustor and Cloud servers or specialist organizations as trustee, and trustor tries to confide in the capacity of trustee to furnish some administration as per a concurred approach. Then, trustee as a reliable gathering ought to guarantee that its assets can be gotten to successfully and productively by trustor. Without a dependable processing condition, specialist co-ops will have minimal impetus to contribute their registering or administration assets and cloud clients may delay to cooperate with specialist co-ops in view of the likelihood of accepting tainted or harmed documents or being misused by malware.

C. Key Distribution Center:

Key distribution center (KDC) refers to the framework which is in the charge for providing keys to clients in a system which provides sensitive data. An association is set every time between two PCs which demand the KDC to produce a special secret phrase which will be used by the end framework client to check. Vitally, a key distribution is a symmetric encryption scheme that allows the entry of minimum of two frameworks for a system by producing an extraordinary ticket compose key to build a secured association for information exchange. KDC is the basic server recommended. Due to its focal framework, KDC is used where association needs do not overrule the framework. Here KDC is used instead of standard key encryption in light of the fact that key is produced every time an association is needed, which decreases the odds of the assault.

VI. PROPOSED CONSTRUCTION

The proposed model is constructed using an enhanced IBE concept. We had termed this concept as Key-Response Algorithm (KRA). This classified into five sections and each section carries out separate function.

A. Setup(A) :

The algorithm for setup is controlled by PKG. It chooses arbitrary generator g1 and an irregular whole number Z,sets g1=gx. Then PKG picks an arbitrary component g2 and two hash function h1 and h2.Finally, the public key (PK) and a master key is obtained as output .

B. KeyGen (MK,ID,RL,TL,PK) :

PKG checks whether the ask for character ID exists in RL for every client's private key demand on personality ID, if so then the key generation algorithm is prematurely ended. Then, PKG arbitrarily chooses Z furthermore, sets. It arbitrarily picks x1, furthermore, processes. At that time, PKG peruses the present day and time period T1 from TL (we require that PKG ought to make current day and age right off the bat if is exhaust). Likewise, it haphazardly chooses rTi and figures TK [ID]=(Dt0, Dt1), where Dt0=g2^x2 and, Dt1=g^x1 . At last, yield SK=(IK [ID], TK [ID)] furthermore, OK=x2.

C. Encrypt(M, ID, Ti, PK) :

Assume a client perform encryption to their message M under an identity ID and a time period Ti. They choose an arbitrary value s and processes C0=M(g1,g2), C1=g^s , E(ID)=(H1(ID)) and E(Ti)=(H2(Ti)) . At long last, distribute the ciphertext CT = (C0, C1, E(ID), E(Ti)).

d) Decrypt (CT, SK, PK) :

Assume that ciphertext (CT) is encoded with ID,Ti , and the client has private key SK(ID)=(IK[ID],TK[ID]), where IK[ID] = (d0,d1) Furthermore, TK[ID]=(dT0, dT1). Later the figure content is unscrambled utilizing CT, SK(ID) and public key.

e)Revoke (RL,TL,{ID1.ID2,…,IDk}) :

In the event that clients with the set characters {ID1,ID2,… ,IDk} should be renounced at the time period Ti, PKG restores renouncement list as RL' = RL U {ID1,ID2,… ,IDk} and also the time list by connecting the recently made time duration T(i+1) into the unique list TL. At long last send the duplicate for the refreshed denial list RL' and the new time duration T(i+1) to KU-CSP.

At long last, we underline the thought behind our development is to acknowledge renouncement by refreshing the time part in the private key. Subsequently, the main point is to avert denied client from conspiring with different clients to re-develop their private key. As announcing in instinct, such agreement assault is safe in the proposed development because of the irregular split for every client. In particular, an AND gate associating two sub-segments, if two unique clients require the private keys, PKG will acquire two haphazardly parts (x1,x2) and (x1', x2') with the reciprocal that x1+x2=x mod q and x1'+x2'=x mod q. x1 and x2 are utilized to create the character part for the ID, ID' individually, whereas time segment is independently created from x2 and x2' . By the reason that the corresponding exists amongst x1 and x2 and in addition x1'and x2', the character part and time segment ought to in like manner have a "check" in private key. With such "check", regardless of whether an inquisitive client acquires time segment of different clients, he/she can't manufacture a substantial private key for themselves to perform decoding effectively.

VII. KEY SERVICE PROCEDURES

Depending on the algorithm development, the key service process comprising key-issue, key-updating and revocation in the proposed scheme with service cancellation work as below.

A. Key-Issuing:

We need that PKG keeps up a renouncement list and the time duration list TL locally. After getting a request for private key on ID, PKG runs the KeyGen to acquire private key SK(ID)and outsourcing key OK (ID). At last, it will send SK(ID) to client and (ID, OD(ID)) to KUCSP individually. As depicted in instinct, for every section (ID, OD(ID)) which is send from PKG, the KU-CSP should include it into a privately kept up client list UL .

B. Key-update:

On the off chance that a few clients are being disavowed at a time period Ti, each of granted client has to issue a key-update request to KU-CSP to look after decrypt ability. Upon the request accept on personality ID, the KU-CSP runs the KeyUpdate process (RL, ID, T(i+1), OK(ID))to get TK[ID]. At last, it sends such time part back to client who can update their private key SK(ID)=(IK[ID], TK[ID]).

C. Revocation:

Like key update, if a renounced client sends a key-update and ask for on character ID, KU-CSP will run the KeyUpdate function (RL, ID, T(i+1), OK(ID)) too, since KU-CSP will return. Subsequently, such a key update request is prematurely ended.

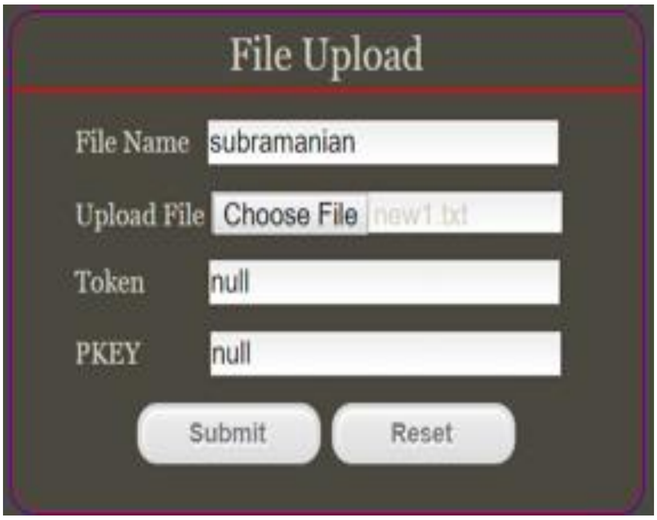
VIII. PERFORMANCE EVALUATION

Also, we endeavor to recreate the situation of multi-client disavowal, and demonstrate a broad correlation between the outsourced disavowal plot and other revocable IBE method– BGK plot. Take into point that we utilize a 32 bit number to distinguish every hub in paired tree in BGK conspire for overseeing clients. The examination is as far the key-issue stage and key update organize.

A. Key-Issuing Stage

We shift the greatest amount of clients in the framework and demonstrate the reacting period for a solitary key age ask. It isn't difficult to note that reacting time in the BGK plot is in proportion of O(log2(n)) where the variable n is the greatest number of clients in framework. It is on account of a twofold tree is used to deal with every one of the clients, each leaf hub of which is doled out to a solitary client in framework.

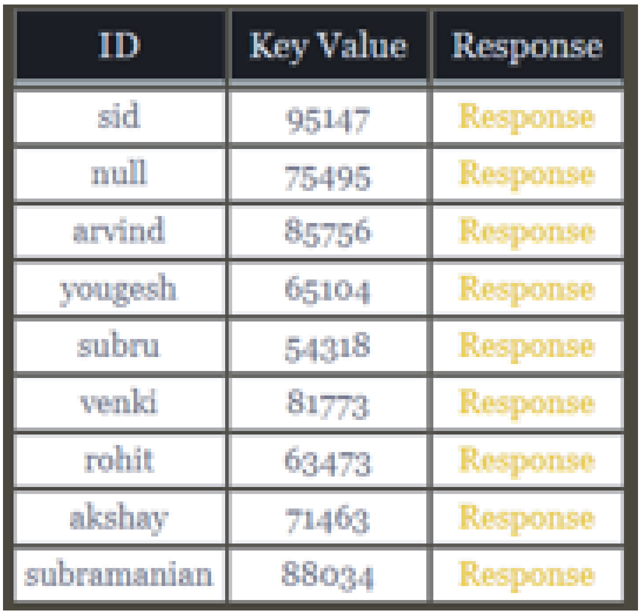
Amid key-issuing, the PKG needs to calculate on every one of the hubs in the way from comparing leaf hub to root hub.



File Upload

File Name	subramanian
Upload File	Choose File new1.txt
Token	null
PKEY	null

Fig. 3 File Upload



ID	Key Value	Response
sid	95147	Response
null	75495	Response
arvind	85756	Response
yougesh	65104	Response
subru	54318	Response
venki	81773	Response
rohit	63473	Response
akshay	71463	Response
subramanian	88034	Response

Fig 4. Key Generation

Contrasted with the logarithmically developing effectiveness in , our plan accomplishes steady effectiveness (almost six measured exponentiation in G) in case of single key-issuing. Because of a similar reason of requesting for calculation on every one of the hubs in way from leaf hub to root hub, the past method has an expanding private key estimate, though our own accomplishes consistent key size (almost four component in amass G). Other than the preferable execution in productivity and size of private key, the other preferred standpoint of the plan with the past work is about that it bolsters dynamic number of clients. In particular, the past work needs to settle the greatest number of clients in framework at first to encourage developing the parallel tree. When the most extreme number is settled, it will be troublesome to include clients surpassing this bound. Our own do not have such a downside, and adaptably bolsters dynamic administration of clients.

B. Key Update Stage

We arbitrarily consider 5% to 75% clients and look at the aggregate duration of refreshing private keys of the rest clients. To ensure straightforwardness, we outline a demo and look at the key refresh time in PKG in disavowal on account of 215 framework clients.It is seen that the effectiveness bend of BGK plot demonstrates an illustrative shape, and at the 25% denial proportion, the productivity accomplishes the most reduced point in our assessment. This is on account of the hole the leaf hubs to be repudiated has a substantial number however low collection degree, which needs to refresh a great deal of interior hubs for key update. On any case, such a conduct is maintained a strategic distance from, and only an immaterial steady duration is taken at PKG.

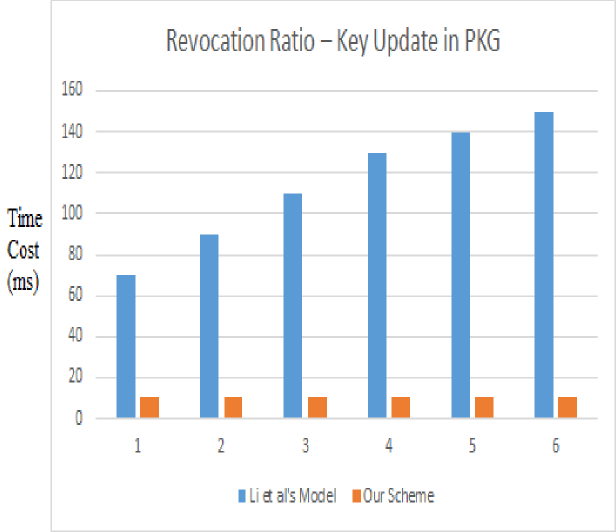


Fig.4 Revocation Ratio – Key Update in PKG

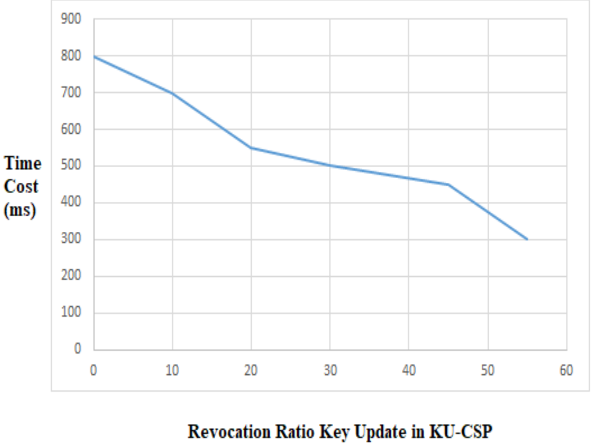


Fig.5 Revocation Ratio – Key Update in KU-CSP

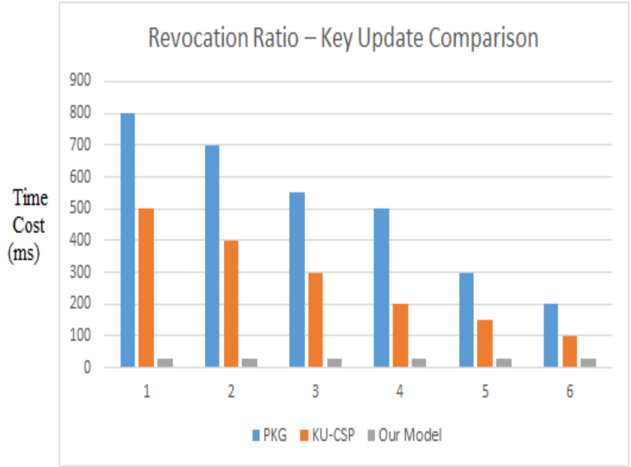


Fig.6 Revocation Ratio – Key Update Comparison

All the more by and large, this consistent key-update productivity is accomplished by our plan with in any case to the number of framework clients since here we assign the disavowal to KU-CSP, yet BGK plot expects an expanding time cost with the quantity of framework clients In like manner, we likewise demonstrate the time and cost in KU-CSP in proposed conspire for refreshing private keys for each of the unrevoked clients in the denial proportion running from over 5% to 75%. It should be called attention to, however, this period cost is developing with many of the clients for each circumstance as with the execution of PKG , this calculation is directed at the cloud, which normally has bounteous assets. Besides, we assess the correspondence price for every client's key-update ask for in Amazon EC2 cloud condition, which takes 87 ms. Take into account that, such a difficulty incorporates the tedious for transmitting and verification at Amazon EC2 cloud stage.

XI. CONCLUSION:

In this paper, this plan will need high expenses for computation and communication than the previous proposed IBE plans. The KU-CSP plot should maintain a mystery esteem for all client using the objective which is the not adaptable for the key time refresh strategy. In revocable IBE conspire with CRA, the CRA will have to hold an ace time key to carry out the time duration key refresh strategies for each one of clients without influence of security. From test results and investigation from, our proposed technique is suitable for mobile phones. For purpose of investigation regarding security, we explained that the suggested method is safe for all versatile ID assaults. On the whole, in accordance of this proposed revocable IBE plot with CRA, we designed a CRA aided confirmation conspire with time-restricted add-ons for handling with an extensive number of various cloud administrations.

REFERENCE:

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 Weil pairing," in Advances in Cryptology (CRYPTO '01), J. Kilian, Ed. Berlin, Germany: Springer, 2001, vol. 2139, pp. 213–229.
5. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. 15thACMConf. Comput. Commun. Security (CCS'08), 2008, pp. 417–426.
6. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 557–557.
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/2011/518.
8. U. Feige and J. Kilian, "Making games short (extended abstract)," in Proc. 29th Annu. ACM Symp. Theory Comput. (STOC'97), 1997, pp. 506–516.
9. S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. 2nd Int. Conf. Theory Cryptography (TCC'05), 2005, pp. 264–282.
10. R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, A. Smith, Ed. Berlin, Germany: Springer, 2012, vol. 7412, pp. 37–61.
11. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Security (ESORICS), 2012, pp. 541–556.
12. M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebra computations," in Proc. 5th ACM Symp. Inf. Comput. Commun. Security (ASIACCS'10), 2010, pp. 48–59.
13. A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology (CRYPTO), G. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, vol. 196, pp. 47–53.
14. C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, B. Honary, Ed. Berlin/Heidelberg: Springer, 2001, vol. 2260, pp. 360–363.
15. R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in Advances in Cryptology (EUROCRYPT'03), E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656, pp. 646–646.
16. D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'04), C. Cachin and J. Camenisch, Eds. Berlin, Germany: Springer, 2004, vol. 3027, pp. 223–238.
17. D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in Advances in Cryptology (CRYPTO'04), M. Franklin, Ed. Berlin, Germany: Springer, 2004, vol. 3152, pp. 197–206.
18. B. Waters, "Efficient identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127.
19. C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology (EUROCRYPT'06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.
20. C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proc. 40th Annu. ACM Symp. Theory Comput. (STOC'08), 2008, pp. 197–206.
21. S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (h)ibe in the standard model," in Advances in Cryptology (EUROCRYPT'10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.
22. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in Advances in Cryptology (EUROCRYPT' 10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 523–552.
23. Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-insulated encryption and its application," in Advances in Cryptology (ASIACRYPT'05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495–514.
24. D. Boneh, X. Ding, G. Tsudik, and C. Wong, "A method for fast revocation of public key certificates and security capabilities," in Proc. 10th USENIX Security Symp., 2001, pp. 297–308.

25. B. Libert and J.-J. Quisquater, “Efficient revocation and threshold pairing based cryptosystems,” in Proc. 22nd Annu. Symp. Principles Distrib. Comput., 2003, pp. 163–171.
26. H. Lin, Z. Cao, Y. Fang, M. Zhou, and H. Zhu, “Howto design space efficient revocable IBE from non-monotonic ABE,” in Proc. 6th ACM Symp. Inf. Comput. Commun. Security (ASIACCS’11), 2011, pp. 381–385.
27. B. Libert and D. Vergnaud, “Adaptive-id secure revocable identitybased encryption,” in Topics in Cryptology (CT-RSA’09),M. Fischlin, Ed. Berlin, Germany: Springer, 2009, vol. 5473, pp. 1–15.
28. 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.
29. [29] 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.
30. 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.
31. M. J. Atallah and J. Li, “Secure outsourcing of sequence comparisons,” Int. J. Inf. Security, vol. 4, pp. 277–287, 2005.
32. D. Benjamin and M. J. Atallah, “Private and cheating-free outsourcing of algebraic computations,” in Proc. 6th Annu. Conf. Privacy Security Trust (PST’08), 2008, pp. 240–245.
33. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.
34. P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” Nat. Inst. Stand. Technol., Tech. Rep. SP 800-145, 2011.
35. 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.
36. 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.
37. Z. Zhou and D. Huang, “Efficient and secure data storage operations for mobile cloud computing,” in Proc. 8th Int. Conf. Netw. Service manage., 2012, pp. 37–45.
38. J. Li, C. Jia, J. Li, and X. Chen, “Outsourcing encryption of attributebased encryption with mapreduce,” in Information and Communications Security. Berlin, Heidelberg: Springer, 2012, vol. 7618, pp. 191–201.
39. 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. Comput. Security (ESORICS), 2013, pp. 592–609.
40. B. Zhang, J. Wang, K. Ren, and C. Wang, “Privacy-assured outsourcing of image reconstruction service in cloud,” IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, p. 166–177, Jul./Dec. 2013.
41. Y.-M. Tseng. and T.-T. Tsai, “Efficient revocable ID-based encryption with a public channel,” Computer Journal, vol.55, no.4, pp.475-486, 2012.
42. J. Li, J. Li, X. Chen, C. Jia, and W. Lou, “Identity-based encryption with outsourced revocation in cloud computing,” IEEE Trans. On Computers, vol. 64, no. 2, pp. 425-437, 2015.

AUTHOR PROFILE:

K.Latha obtained B.E degree in computer science & engineering from Adhiparasakthi **Engineering College, Madras University,** TamilNadu, India in 2000 and M.Tech Degree in Computer science and engineering from Dr.MGR University , Tamilnadu in 2006 and pursuing Ph.D degree in Sathyabama Institute of Science and Technology . Currently working as a Assistant Professor in Sri SaiRam Engineering College. Chennai. Published research papers in international and national journals and seven papers in conference proceedings

T.Sheela obtained B.E degree in Computer Science & Engineering from Madurai Kamarajar University, Madurai TamilNadu, India, in 1989 and M.S Degree in Computer Science & Engineering from BITS – Pilani, Rajasthan, India, in 1993. She completed Ph.D. in Computer Science and Engineering in 2010.She is a Professor in Information Technology in Sri Sai Ram Engineering College Chennai. She has published research papers in international and national journals and seven papers in conference Proceedings. She authored books on Data Structure and Fundamentals of Computers. Her research work was selected for presentation at AICTE (Govt. of India), New Delhi.

Retrieval Number: A10141091S19/2019©BEIESP
DOI:10.35940/ijeat.A1014.1091S19