IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Fusion-Identity Based Encryption with the Outsourced Withdraw in the Cloud Computing

Ashwini Bhosale[1], **S.T. Singh**[2] **and Prema Sahane**[3]

Department of Computer Sciences, P.K.Technical Campus, Pune[1,2,3]

Abstract: Cloud computing frequently introduce as the cloud is the delivery of on the demand computing resources everything from the applications to data centers above an internet on pay for use. The Cloud based applications rundown infrastructure and IT expense, growth accessibility, enable collaboration, and allow organizations more freedom in customizing their products. User or multi user data sharing should be secure and integrity should be derived on cloud. To achieve the data security the methods like IBE (Identity Based Encryption) and ABE (Attribute Based Encryption) are widely used in cloud computing environment. Still, the complication corresponding with IBE (Identity Based Encryption). The Private Key Generator is compromised all messages protected over the whole lifetime of the public-private key couple used by that server are also compromised. This makes the PKG an high-value target to adversaries. To limit the exposure due to an compromised server, the master private-public key couple could be updat with a new independent key couple. Still, this is an found the key-management problem where all the users must have been the most recent the public key for the server. From the recent studies, there are two main research problems for cloud computing security such as security improvement using IBE and efficient ABE withdraw process. The cause of this paper is to present framework to address both this research challenges. In this paper new fusion cloud security method is proposed in order to deliver both efficient withdraw and enhanced security. This fusion approach is combination of two well know security techniques such as IBE and ABE. The ABE method is combined with IBE to achieve the strong security against diverse warning. Adjacent with user identity attributes like country or type of subscription has are used for further process of IBE encryption, decryption and withdraw. Other complication of efficiency identity revocation is further addressed by presenting the outsourcing computation into fusion IBE (F-IBE) way at server dependent settings. The other components and ways of proposed F-IBE are discourse between this paper and evaluated the experiment against existing way.

Keywords: ABE, IBE, Cloud Computing, C-PABE C-IBE, Encryption, Decryption, Key Generation, PKG, KU-CSP.

1 INTRODUCTION

The Cloud computing means storing or accessing data and programs over the internet option of our computer hard disks. I have all become stakeholders in the computing movement and we are all affected when major changes chance. Remember how things changed when the Internet came contiguous changes in computer technology seem to move at lightning speeds. It wasn't that long ago those desktop computers had 20MB hard drives and users relied on floppy disks for storage. For that reasons, it wasn't that long ago that there were no desktop computers, and computing involved cardboard punch cards fed into a hopper. The possibilities [1] are growing even faster as the US government undertakes its rural broadband initiatives which in turn will push the possible of cloud extra to the masses. Why we put the applications and data in the cloud. Numbers of reasons depending on who you are. If you're just writing a document or working from home then you can probably find online apps to do the trick without buying costly office software. If you are an IT guy, even better the cloud [2] makes computing easier to manage drives down costs and allows end-users to obtain access to a large range of applications and services. Sure, PCs and dedicated servers have served but not without problems. They crash they [3] require us to buy, manually install, upgrade and uninstall expensive software. They become turgid, slow and loaded with viruses. Would no be so much better if someone could take care of all the difficulty with cloud computing we rent only what we need and somebody else manages the unclean work. Ask any IT person about their work schedule and you will find out quickly that expectations and workload often outrun the allowable amount of time anyone really wants to work. And more importantly ask the CFO who signs the paychecks. Do they want to cut costs absolutely? And cloud [4] computing will do it cutting cost while giving the IT staff a break at the same time. Identity-based systems allow any party to generate a public key from a known identity values such as an ASCII string. A trusted third party called the private key generator generates consistent private keys. To operate the PKG first publishes a master public key and retains the consistent master private key. Given the master public key any party can compute a public key consistent to the identity ID combining the master public key with the identity value. To gain consistent private key use the identity ID contact the PKG which uses the master private key to generate the private key for identity ID. As a result, parties may encrypt messages with no distribution of keys during individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient due to

DOI10.17148/IJARCCE.2017.6686

technical restraints. Still, to decrypt messages the authentic user must gain the appropriate private key from the PKG. A caveat of this approach is that the PKG must be highly trusted as it is able of generating any user's private key and may therefore decrypt messages without authorization. Because any user's private key can be generated through the use of the third party secret this system has corresponding key escrow. From the literature study it is showing that IBE Revocation is not widely studied there are only little techniques introduced for IBE revocation. The author of [5] proposed that end users can renew private keys frequently as well as senders are using the receivers' identities together with the use of current time period. Because of this mechanism should be a result in an above load at the PKG. In other word, every user whether that keys have cancel or the not, it has been to contact with PKG periodically to prove their identities and update new private keys. It is wanted to that PKG is to online and secure channel must be continue for all transactions which will be getting the blockage for the IBE way as the more of users growth. Other request was proposed in [6] for revocable IBE method in cloud computing. Their system and way is being processed on the idea of fuzzy IBE primitive [7] but utilizing the binary tree data structure for the record users' of their identities at the leaf of nodes. Key-update capability at PKG is possible to expressively dwindle from the linear to the height of this type of binary tree. PKG is usage for generate a key pair for every nodes on the path from the identity leaf node to the current root node which is giving results in involution logarithmic in the number of users in system for issuing a single private key. In logarithm private key size has been growth into the number of users in system which makes it crucial into the private key storage for the users. As like the number of users in system growth, PKG has to sustain a binary tree with a large amount of the nodes, which present the distinct blockage for the world system.

Cloud computing surface skill for users in order to buy the on claim services from the cloud-based services like Windows Azure, Microsoft's, Amazon's EC2,etc. and IBE new working paradigm for supplying such cloud services into the IBE withdraw in order to fix the issues of storage and capability withdraw overhead as discussed in above paragraphs. A simple approach would be to simply hand over the PKG master key is to the given in Cloud Service Providers. The CSPs should after that easy to change all the private keys with the usage of the traditional key update technique [5] and transmit the private keys have been back to the un-abolishment users. Whatever, the easy method is based on an un-realistic assumption. CSPs are totally trusted and permitted to access the master key for IBE system. On the adverse, in practice the public clouds are normally outside of the similar trusted domain of the users & are inquisitive for users' personal privacy. Therefore, it is challenging research problem of designing the secure and capability withdraw IBE method to minimize the computation overhead at PKG with the un-trusted CSP.

In this paper we proposed the fusion approach for reduce the current research problems related to the cloud security. The proposed method is called as F-IBE which is based on recently presented method in [1]. To another extend the security of IBE, the properties of ABE (Attribute Based Encryption) way is combined with efficiency withdraw IBE proposed in [1]. In F-IBE, the key generation processing's handled during the process of key issuing and key update to the KU-CSP by leaving specific number of easy processing's for PKG as well as users to perform locally. The new complicity resistant approach is proposed in this paper to achieve the capability withdraws. Rest of paper is containing below sections. In section 1, we discussed the cloud security challenges and risk factors as well as discussed the related works on cloud security. In Section 4 presenting the architecture and algorithm details of proposed F-IBE approach. Section 5 presenting the practical simulations and results analysis. Section 6 presenting the conclusion and future direction of this work.

2 LITERATURE SURVEY

In the chapter we are been presenting the diffrent way those are the presented to mine high utility itemsets effectively.

- The D. Boneh, X. Ding, a G. Tsudik, and an C. Wong, A way for fast revocation of public key certificates or a security capabilities in the 10th USENIX Security Symposium, 2001, pp. 297–308.
- An C. Wang, K. Ren Secure and the practical outsourcing of linear programming in cloud computing in IEEE International Conference on the Computer Communications (INFOCOM), 2011, pp and dd.
- Dr .W. Aiello, S. Lodha, and R. Ostrovsky (1998)**,** the accessibility of quick and solid Digital Identities is a basic element for the effective execution of people in general key foundation of the Internet. All advanced personality plans must incorporate a strategy for denying somebody's computerized character for the situation that, this personality is stolen the (or crossed out) before its close a date (like the cancelation of a Mastercards for the situation that they are stolen).
- V. Goyal (2007), another endorsement disavowal framework is introduced. The fundamental thought is to separate the endorsement space into a few segments the quantity of segments being reliant on the a PKI environment. Every parcel contains the status of an arrangement of testaments. A segment may either lapse or be recharged toward the end of a vacancy. This is done proficiently utilizing hash the chains. We assess the execution of our plan taking after the system and numbers utilized as a part of past papers. We demonstrate that for some down to earth estimation of the framework parameters our plan is more proficient than the three surely understood authentication renouncement

DOI10.17148/IJARCCE.2017.6685

systems, CRL, CRS and CRT. Our plan strikes the right harmony between CA to catalog correspondence expenses and question costs via deliberately selecting the quantity of segments.

- F. Elwailly, C. Gentry, and Z. Ramzan, (2004), we present two new plans for effective authentication repudiation. Our first plan is an immediate change on a notable tree-based variation of the NOVOMODO arrangement of Micali. Our second plan is an immediate change on a tree-based variation of a multi-testament renouncement framework by Aiello, Lodha, and Ostrovsky. At the centre of our plans is a novel build named a Quasimodo tree, which resemble a Merkle tree yet contains a length-2 chain at the leaves furthermore specifically uses inside hubs. This idea is of free intrigue, and we accept such trees will have various different applications. The thought, while basic, instantly gives a strict change in the important time and correspondence complexities over already distributed plans.
- The D. Boneh and M. Franklin (2001), we propose a fully functional identity-based encryption diagram (IBE). An diagram has chosen the cipher text security in the random oracle the model assuming an elliptic inflection variant of the computational Dr.Diffie-Hellman problem.the Our system is based on the Weil pairing. We give just definitions for secure identity based encryption schemes give several applications for such systems.
- Dr.A. Boldyreva, V. Goyal, and V. Kumar (2008), The most commonsense arrangement requires the senders to likewise utilize eras when encoding, and every one of the collectors (paying little respect to whether their keys have been traded off or not) to climb their private keys frequently by reaching the trusted power. We take note of that this arrangement does not scale well - as the quantity of clients builds, the work on key redesigns turns into a bottleneck. We propose an IBE plot that altogether enhances key-redesign productivity in favor of the trusted party (from straight to logarithmic in the quantity of clients), while remaining proficient for the clients. Our plan expands on the thoughts of the Fuzzy IBE primitive and twofold tree information structure, and is provably secure.
- A. Sahai and B. Waters (2005), in these Authors present two constructions of Fuzzy IBE technique. Our constructions can viewed an Identity-Based Encryption of a message under several attributes that hush a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against cahoots attacks. Additionally, our general construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.
- R. Canetti, B. Riva, and G. N. Rothblum (2011), In this model, we demonstrate a 1-round actually stable convention for any log-space uniform \(\mathcal{NC}\, \) circuit. Interestingly, in the single server setting all known one-round compact Designation conventions are computationally stable. The convention expands the arithemetization methods of [Goldwasser-Kalai-Rothblum, STOC 08] and [Feige-Kilian, STOC 97]. Next we consider an improved perspective of the convention of [Goldwasser-Kalai-Rothblum, STOC 08] in the single-server model with a non-compact, however open, disconnected stage. Utilizing this rearrangements, we develop two computationally stable conventions for appointment of calculation of any circuit C with profundity d and info length n, even a non-uniform one, to such an extent that the customer keeps running in time n·poly(log(|C|), d). The primary convention is conceivably down to earth and less demanding to execute for general calculations than full convention and the second is a 1-round convention with comparative intricacy,however less effective server.
- 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 18th European Symposium on Research in Computer Security (ESORICS), 2013.

3 PROPOSED APPROACH AND DESIGN

3.1 Problem Definition

The KU-CSP is complex to the realize withdraw for compromised users. The an KU-CSP can be visualized as a public cloud run by a third party to deliver main computing capabilities to the PKG as standardized services above an network. The KU-CSP is hosted away from either users and the PKG but provides a method to the reduce PKG computation and storage expenditure by supplying a workable, even temporary supplement to infrastructure. When withdraw is triggered, instead of re-requesting private keys from the PKG in [4], un-revoked users have to ask the KU-CSP for updating a lightweight element of their private keys. Details are involved in KU-CSP deployment, In this paper we just logically visualize it as a computing service provider, and concern how to design secure scheme with an un-trust the KU-CSP.

3.2 Proposed System Architecture

In cloud computing systems, there are two main research problems which we studied recently such as efficient IBE withdraw and security improvement in IBE method. By considering both research problems, in this paper we proposed fusion approach to deliver both efficient withdraw and enhanced security. This fusion approach is combination of two well know security techniques such as IBE (Identity-Based-Encryption) and ABE (Attribute-Based-Encryption) to achieve. The ABE method is combined with IBE the strong security against different threats. Contiguous with user identity, his/her attributes like country or kind of subscription he/she has are used for further process of IBE encryption, decryption and withdraw. Other problem of efficient identity withdraw is further addressed by presenting the

DOI10.17148/IJARCCE.2017.6685

outsourcing computation into Fusion-Identity Based Encryption (F-IBE) method at server dependent settings. In F-IBE, the key generation processing's handled during the process of key(using E-mail) issuing and key update to the KU-CSP (the key update cloud service provider) by leaving fixed number of easy processing's for PKG as well as users to perform locally. The new collusion resistant approach is proposed in this paper to achieve the efficient withdraw (means to generate the key when cloud user wants to perform the operation like for upload and download file and handle the key using E-mail technique). The practical work is performed by creating different number of cloud users for file upload and downloads processing using proposed F-IBE (Fusion-Identity Based Encryption) method. The performance is evaluated in terms time cost in during existing efficient IBE withdraw method and our proposed F-IBE method.

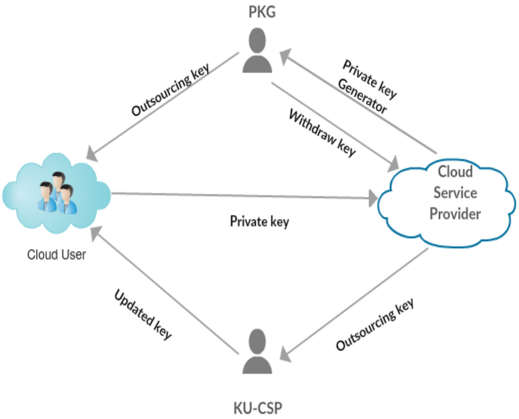


Fig. 1 System Architecture

4 MATHEMATICAL MODEL

4.1 Input Set

Input: P here P is Document file
Step 1: d1 = EscapingHtmlCharacters (P)
Step 2: d2 = DecodingData (d1)
Step 3: d3= Apostrophe_Lookup (d2)
Step 4: d4= RemovalOfStopWords (d3)
Step 5: d5= Apostrophe_Lookup (d2)
Step 6: d6= RemovalPunctuations (d5)
Step 7: d7= RemovalExpressions (d6)
Step 8: d8= SplitAttachedWords (d7)
Step 9: d9= Slangslookup (d8)
Step 10: d10= StandardizingWords (d9)
Step 11: d11= RemovalOf URL (d10)
Step 12: Stop

4.2 NP-Complete

In order to the achieve capability revocation we introduce the an idea of the partial private key update into the proposed construction which operates on two sides 1) we utilize an crossbreed the private key for all user in method, which is employs and gate connecting two sub-parts namely the personality element IK and the time component TK respectively. IK is generated by PKG in key-issuing but TK is updated by the newly introduced the KU-CS Pin key-update 2) In encryption we take as input user's identity ID as well as the time period T to restrict decryption more exactly a user is the allowed to perform successful decryption if and only If the identity and time embedded in his/her private key are identical to that associated with the ciphertext. Using such skill, we are able to revoke user's decrypt skill through updating the time component for private key by the KU-CSP. Moreover, we are remark that it cannot trivially utilize an identical updated time component for all users because revoked user is able to re-construct his/her skill through colluding with unrevoked users. To eliminate such collusion, we randomly generate an outsourcing key for each identity ID, which essentially decides a "matching relationship" for the two sub-components. Furthermore, we let the KU-CSP maintain a list UL to record user's identity and its corresponding outsourcing key generation. In key-update, we can use OKID to update the time component TK [ID] T for identity ID.

- Eigen (MK, ID, WL, TL, and PK): For each user's private key request on identity ID, PKG firstly checks whether the request identity ID exists in RL, if so the key generation algorithm is aborted. Next, PKG randomly

DOI10.17148/IJARCCE.2017.6685

selectsx1∈RZq and setsx2=x−x1modq. It randomly chooses r ID ∈ R Zq, and computes IK [ID] = (gx12 (H1 (ID)) r ID, g r ID). Then, PKG reads the current time period Ti from TL (we require that PKG should create current time period firstly if TL is empty). Accordingly, it randomly selects r Ti ∈RZ q and computes TK [ID] Ti= (dTi0, dTi1), where dTi0=g x22(H2 (Ti)) r Ti anddTi1=g r Ti. Finally, output SKID= (IK [ID], TK [ID] Ti) and OKID =x2.

- Encrypt (M, ID, Ti, and PK): Suppose a user wishes to encrypt a message M under identity ID and time period Ti. She/he selects a random values ∈R Zq and computes C0 =Me(g1,g2)s , C1 =gs, EID =(H1(ID))s and E Ti =(H2(Ti))s Finally, publish the ciphertext as CT=(C0,C1,EID,ETi).
- Decrypt(CT,SKID,PK):Suppose that the ciphertext CT is encrypted under ID and Ti, and the user has a private key SKID =(IK[ID],TK[ID]Ti), where IK[ID] = (d0,d1) and TK[ID]Ti =(dTi0,dTi1). She/he computes

$$\begin{gathered} M = C0e\ (d1, EID)\ e\ (dTi1, ETi) \\ E\ (C1, d0)\ e\ (C1, dTi0) \\ =\ \ Me\ (g1, g2)\ s \\ E\ (g, g2)\ x2se\ (g, g2)\ x1s \\ =\ \ M \end{gathered}$$

- Withdraw(WL,TL,{IDi1,IDi2,...,IDik}):If the users with identities in the set{IDi,IDi2,..., IDik}are to be revoked at time period Ti, PKG updates the withdraw list as the WL=WL∪{IDi1,IDi2,...,IDik}as well as the time list through linking the newly created time period Ti+1onto original list TL. Finally send a copy for the updated revocation list an dWL as well as the new time periodTi+1to KU-CSP.
- The Key Update(WL,ID,Ti+1,OKID):Upon receiving a key update request on ID, the KU-CSP firstly checks whether an ID exists in the cancel list WL, if so KU-CSP returns ⊥ and key-update is aborted. Otherwise, KU-CSP fetches the corresponding entry (ID, OKID =x2) in the user list UL. Then, it randomly selectsrTi+1 ∈R Zq, and the computes dTi+10 =gx22 (H2 (Ti+1)) rTi+1 and dTi+11 =g rTi+1.Finally, the output TK [ID] Ti+1= (dTi+10, dTi+11).

4.3 NP-Hard

Step 1: Proposed KeyGen (MK, ID, WR, TL)

1.1. The key generations algorithm running by the PKG is taking as the input – a master key MK, an identity ID (for realization of IBE), AR (for realization of ABE), a revocation list RL and a time list TL.

1.2. If ID ∈ RL, in the algorithm is refused.

1.3. Else, it is giving the private key SKID = (IK[ID], TK[ID]Ti) to user where IK[ID] is the identity component for private key SKID and TK[ID]Ti is its time component for current time period Ti. Additionally, the algorithm sends an outsourcing key OKID to KU-CSP.

Step 2: Proposed Encrypt (M, ID, WR, Ti, and PK)

The encryption algorithm run by sender taken as the input – the message M, is an identity ID, attribute AR & the time period Ti. It outputs the ciphertext CT.

Step 3: Proposed Decrypt (CT, SKID)

The information given for algorithm is run by receiver takes as input – a ciphertext CT encrypted under identity ID, attribute AR and time period Ti and a private key SKID = (IK[ID'], TK[ID']Tj). It outputs the original message M if ID = ID' and Ti = Tj, otherwise outputs ⊥.

Step 4: Proposed Withdraw (WL, TL, and {IDi1. IDik})

1.1. The withdraw algorithm run by PKG takes as input – a withdraw list RL, a time list TL & the set of identities to be withdraw {IDi1, IDi2. IDik }.

1.2. It outputs an updated time period Ti+1 as well as the updated withdraw list WL' and time list TL'.

Step5: Proposed Key Update (WL, ID, Ti+1, OKID)

1.1. The algorithm of the key update running by the KU-CSP takes as input – a withdraw list WL, an identity ID, a time period Ti+1 and the outsourcing key OKID for identity ID.

1.2. It outputs user's updated time component in private key TK[ID]Ti+1 if his identity ID does not belong to WL, otherwise, outputs ⊥. And updated key and current time will be send to the user.

4.4 Output Set

$$\mathbf{y = [bn - anb0\ bn - 1 - an - 1b0..b1 - a1b0\begin{bmatrix} x1 \\ x2 \\ xn \end{bmatrix}] + b0u}$$

4.5the Hardware and the Software Used

The Hardware Configuration

-the Processor – an Pentium IV 2.6 GHz

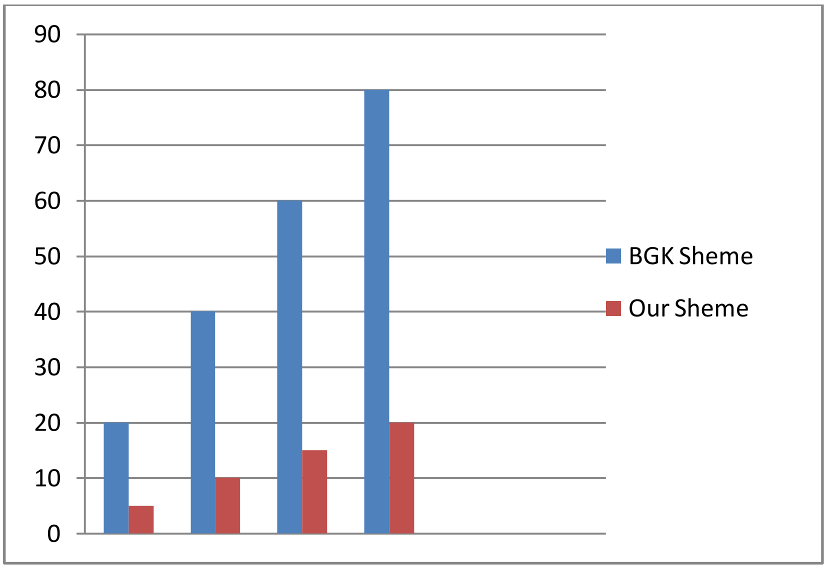
- the RAM - Ram 512 mb dd ram
- the Monitor - 15” colour
- the Hard Disk - 20 GB
- the Key Board - Standard Windows Keyboard

The Software Configuration

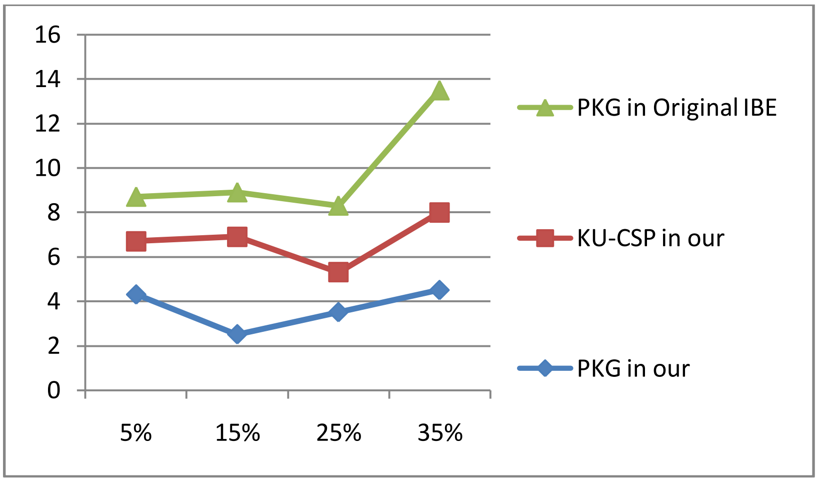
- an Operating System – the Windows Xp/7 /10
- the Programming Language – Java, JSP
- the Database - MYSQL
- Tools - Net Beans

5 RESULT

Following graphs explain the excepted practical results for proposed work C-IBE. The practical work is designed and implemented using Java platform under real time cloud deployment settings.



Maximum Number of System user.
Fig. 2 Private Key Size



Withdraw Ratio
Fig. 2 Key Update Comparison

6 CONCLUSION AND FUTURE WORK

We explanation of another technique called as Fusion-Identity based Encryption, to address the Identity based Encryption related issues. In this venture primary objective is to enhancing the security level of IBE technique. We proposed the F-IBE technique in light of outsourcing calculation into the Attribute based IBE strategy. Notwithstanding this, proposed the abolishment procedure in which the repudiation functionalities are allocated to CSP. The capacities KeyGen, encode (encrypt), decode (decrypt), deny and key overhaul are outlined, adjusted and executed in this paper. The execution is assessed to guarantee the perfectibility of proposed strategy. The renouncement productivity is enhanced by 40 % around when contrasted with existing technique. For future work, we recommend to take a shot at in detail down to earth examination and testing to check the possible outcomes of additional changes.

ACKNOWLEDGMENT

An authors would like to the thank all of the anonymous referees & the editor for their valuable remarks.

REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, “Fast digital identity revocation,”in Advances in Cryptology – CRYPTO’98. Springer, 1998.

[2] V. Goyal, “Certificate revocation using fine grained certificate space partitioning,” in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 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 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375–388.

[4] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in Advances in Cryptology – CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213–229.

[5] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS ’08. New York, NY, USA: ACM, 2008, pp. 417–426.

[6] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 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, Report 2011/518, 2011.

[8] U. Feige and J. Kilian, “Making games short (extended abstract),” in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC ’97. New York, NY, USA: ACM, 1997, pp. 506–516.

[9] S. Hohenberger and A. Lysyanskaya, “How to securely outsource cryptographic computations,” in Proceedings of the Second international conference on Theory of Cryptography, ser. TCC’05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 264–282.

[10] R. Canetti, B. Riva, and G. Rothblum, “Two protocols for delegation of computation,” in Information Theoretic Security, ser. Lecture Notes in Computer Science, A. Smith, Ed. Springer Berlin / Heidelberg, 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 17th European Symposium on Research in Computer Security (ESORICS), 2012.

[12] M. J. Atallah and K. B. Frikken, “Securely outsourcing linear algebra computations,” in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS ’10. New York, NY, USA: ACM, 2010, pp. 48–59.

[13] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in Cryptology – CRYPTO, ser. Lecture Notes in Computer Science, G. Blakley and D. Chaum, Eds. Springer Berlin /Heidelberg, 1985, vol. 196, pp. 47–53.

[14] C. Cocks, “An identity based encryption scheme based on quadratic residues,” in Cryptography and Coding, ser. Lecture Notes in Computer Science, B. Honary, Ed. Springer Berlin / Heidelberg, 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 2003, ser. Lecture Notes in Computer Science, E. Biham, Ed. Springer Berlin / Heidelberg, 2003, vol. 2656, pp. 646–646.**:**

DOI10.17148/IJARCCE.2017.6685