iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Efficient and Secure Data Transactions Using AES in P2p Storage Cloud

S.I.Shaik Hussain[1], V.Yuvaraj[2]
[1]PG Scholar, [2]Assistant Professor, Dept. of Computer Science and Engineering,
Anna University Regional Centre, Coimbatore, India

Abstract*—P2P cloud storage is usually a combination of cloud computing and peer-to-peer computing mechanism, where it can offer and provide huge computing, storage services and at the same time it lowers the economic cost of the real time users. Generally, cloud server and cloud users lye outside the data owners trusted domain. The P2P cloud storage creates new challenges regarding the access control and the data security while the data owner usually stores the sensitive information for sharing them in the trusted domain of cloud storage. However there are no such mechanisms available for access control in P2P storage cloud. Hence we propose a system which produces double encryption namely ABE and PRE based on the user attributes, which provides an efficient, secure and fine-grained data access control for the P2P storage cloud. The performance mechanism shows highly efficient and practical for day to day life and also it reduces computation overheads during user revocation than the other schemes.

Index Terms*— Peer-to-peer computing, ABE, PRE, Access control

I. INTRODUCTION

Cloud Computing is one of the dreamt technology of utility computing. Multiple users can able to store their data remotely in the cloud. Hence, they can achieve on-demand quality services and applications from a shared pool of accountable resources. Some of the important storage services provided by SSP are Google drive, Dropbox and iCloud to the users [4]. Naturally high sensitive data are stored in the cloud . For example, medical database and genome datasets are kept safer than the ordinary one.Generally sharing the data in the cloud server storage is one of the most important significant functions, but usually it has many risks during the data manipulation. Because the data to be processed generally resides outside of the data admin. Even though the storage is a secured one, there may be a chance to file disclosure such that the cloud owner protect their files with a high degree of confidentiality. For encryption and decryption generally cryptography is used [1]. There are two broad categories of cryptographic techniques such as conventional technique and public key cryptography[3].

In P2P storage cloud, the most security mechanism needs to be checked is data access privilege, such that which type of data can be accessed by the users. To achieve this we propose a technique called Attribute Based Encryption (ABE) [2][6] which is a public key cryptography technique [3] that works according to the nature of the attributes of the user.[4][7].

Another important task is the user revocation which is used to revoke the access permission of the user to retrieve the data in the P2P storage cloud. To achieve this we put forth two new techniques called ABE and Proxy Re Encryption (PRE) here, for fine-grained data access control in P2P storage cloud. The CP-ABE logical diagram is shown in figure 1.

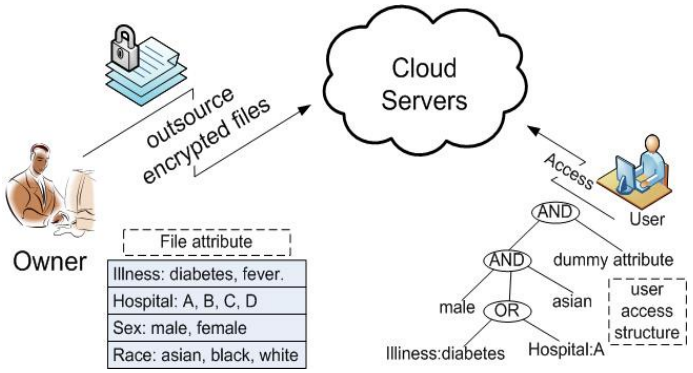


Fig 1. An example of the access tree in CP-ABE

©IJRASET 2015: All Rights are Reserved

II. RELATED WORKS

The research work related to these topics is yet to be identified in the reference. Already some of the work carried forward to check whether it achieves greater performance in terms of both cost and time. We will see some of the topics related to the attribute based encryption and proxy re-encryption.

A. Cp-Abe Evaluation Uses Tree

CP-ABE is one of the techniques of ABE. Here the data is encrypted with the help of the Access Control Policies (ACP) and the set of descriptive attributes. Bethencourt et al identified the first ABE technique were more versions of the ABE techniques are proposed later [17]. Here the ACP of each user can be represented by means of tree, over attributes of one another. The user's secret key is usually related to the set of attributes. The decryption of the ciphertext can be taking place with the particular user secret key. If and only if the associated attributes needs to satisfy the accessibility tree.

Let us take a simple example, construct a tree that satisfies the attributes and ACP of the user. The tree is a combination of both AND and OR gates. If the decryption of ciphertext needs to takes place means, it will check the ACP and attribute related to the ciphertext by validating the tree from top to bottom, which satisfies the condition. If the condition satisfies, decryption of the original ciphertext takes place. Otherwise returns an error message.

B. Pre An Additional Security Mechanism

PRE is one of the famous encryption technique which is used to re-encrypt the another encrypted ciphertext data. Usually the first encrypted ciphertext resides as per the policy that satisfies some conditions. If all the necessary conditions satisfy, the re-encryption takes place with the help of the first encrypted ciphertext data [8]. Thus it leads to another encryption, which produces the another ciphertext for the same plaintext on its own. The general mechanism proceeds that using a proxy re-encryption key $rK_a \leftarrow\!\!\rightarrow_b$ which can translate a ciphertext using the public key PK_a into an another ciphertext for the same plaintext value, where it is already encrypted first using the public key PK_b. It is noted that the plaintext data cannot be known by each other [11].

C. Bilinear Pairings For Advanced Encryption And Decryption

Consider 'P' be the prime order of two multiplicative cyclic groups G_0 and G_1 respectively. Let us assume that 'g' be a generator of G_0 and e be a bilinear pairing [13], such that, $e : G_0 * G_0 \rightarrow G_1$, which satisfies the following condition

1) Bilinear : for all $u,v \in G_0$, $a, b \in Z_p$, $e(u^a, v^b) = e(u, v)^{ab}$
2) Non-degeneracy : $e(g, g) \neq 1$.

If it satisfies, we can say that the group G_0 is a bilinear group, such that the group operation in e and G_0 are both produces an efficient computation [15]. But in general, the implementation says that, the G_1 is a multiplicative subgroup of finite fields and G_0 is the group of points on an elliptical curve.

D. Categories of P2P Reputation Systems

The P2P reputation system plays an important role in the several areas of computer networks, mainly in the P2P networks. The P2P reputation systems broadly classified into 3 major types, namely peer-to-peer reputation system, object reputation system and hybrid reputation system. In a peer-to-peer reputation system, generally the peers assign reputations to other peers based on their quality of service, whereas the malicious peers whom considered it as low reputation one and it can be easily identified. In object reputation system, naturally the peers assign reputation to their objects using the files and they usually downloaded, once it satisfies the authentication problem. Finally the particular object reputation decides, whether to download the object or not.

The hybrid reputation is a combination of both peer reputation and object reputation systems. The hybrid reputation simply maintains the integration of both the combined information of objects and peers, where it determines and identifies which peers provides high reliability and most secure in the essence of providing the best quality resources [5].

III. OUR CONTRIBUTION

The data access control mechanism in P2P cloud is totally formulated by two major encryption mechanism namely ABE and PRE. First through ABE, the data owner normally encrypt the original plaintext into ciphertext where it uses symmetric encryption using public key [9], with the help of the ACP and attributes of the user, environment and cloud. The most important factor in dealing with this process is the attributes of the user. Almost all the process carried over through this mechanism is controlled by the user attributes only. Once it successfully completed, another encryption, namely PRE is again done by the

©IJRASET 2015: All Rights are Reserved

same data owner to enforce the security of the data. Now the original information is available in the P2P storage cloud.

If a user comes into existence for the data which resides in the P2P storage cloud, the decryption mechanism takes place that conforms the ACP and attributes of the user first. Once all the information which is needed to perform the decryption successfully verified and guaranteed, the decryption takes place using the secret key of the user. The original data is retrieved by the user [14]. An example of data access control in P2P storage cloud is shown in figure 2.

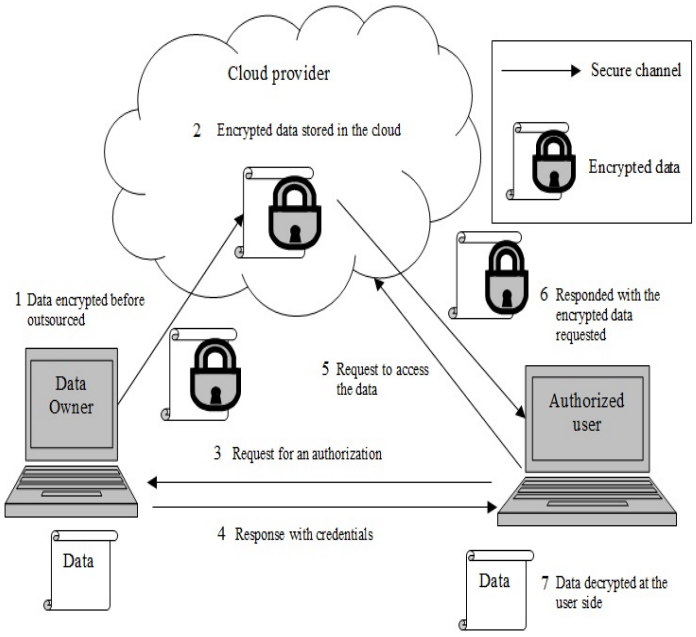


Fig 2. Overview of Data Access Control in P2P Storage cloud

IV. OPERATIONAL DESCRIPTION

A. *Overall System Formulation*

This is the first phase of the process where, the overall system setup takes place here. There are three major functionalities resides here such as storage cloud, data user and data admin. The data admin plays a major role in the process of encrypting the original plaintext by symmetric encryption using public key PK as well as the master key MK along with the user attributes [12]. Once the data admin uploads the encrypting content to the P2P cloud storage, the information is now available in the cloud. If a user wants the original data means, with the help of the user attributes along with the secret key SK, the decryption takes place to get back the original data.

B. *Encrypting and Uploading Data to the P2p Cloud*

In this phase, the data admin performs the encryption operation where the data admin uploads the original content to the P2P storage cloud [16]. The data owner formulates a symmetric encryption key K with the help of the symmetric encryption algorithm. Here we use Advanced Encryption Standard (AES) algorithm for encryption purpose in which the original plaintext is converted into ciphertext. The following is the AES algorithm which is used to encrypt the original data.

INPUT : System public key PK = (e,g,y, $\forall$,$a_j \in U : T_j$), plaintext M, access tree T over attribute U.

OUTPUT : Ciphertext C under T.

1) Randomly choose a secret $s \leftarrow Z_p^*$
2) Compute $C_0 = g^s$ $C_{1,} = M\, y^s = Me\ (g,g)^{as}$
3) Let r0 denote the root node of T.
4) For each node x in T,

4.1) Let k_x denote the threshold value of x.

4.2) If x is r0 then randomly choose a polynomial q_r with degree $d_{r0} = k_{r0} - 1$, let $q_{r0}(0) = s$, and then divide s using the secret sharing scheme, assigning each child node y a secret share $s_y = q_{r0}(\text{index}(y))$.

4.3) Else randomly choose a polynomial q_x with degree $d_x = k_x - 1$, let $q_x(0) = s_x = q_{parent}(x)\ (\text{index}(x))$, and for non-leaf node x, further divide s_x using the secret sharing scheme, assigning each child node y a secret share $s_y = q_x$

©IJRASET 2015: All Rights are Reserved

(index(y)).

5) Let X denotes the set of leaf nodes in T.
6) For each leaf node x ∈ X
   6.1) Let a_j denote the attribute associated with x.
   6.2) Compute $C_j = T_j^{qx(0)} = g^{qx(0)}$.
7) Return C = (T, C_0, C_1, ∀ x ∈ X:C_j).

C. Addition of new user to the Existing System

If a new user comes into this system to perform the file operation, the data admin first assigns some set of attributes to that particular user and finally generates a secret key SK corresponding to the attributes of that particular user. Once all this process successfully happens, now the new user can able to perform all the transactions in the cloud.

D. Denial of user rights by the Data Admin

The data owner is the central authority to revoke any number of attributes from a user, using the Attribute Revocation List (ARL) and stores all the PRE keys and its corresponding version numbers into it. For each user revocation, where each revoked attribute, a new PRE key will be generated for the corresponding revocation and also a version number associated with it [10]. The Attribute History List (AHL) maintains and stores all the information about the PRE and the corresponding version numbers.

E. Decryption and File Access from the P2P Storage Cloud by the User

Whenever a user request for the original file which resides in the storage, the cloud server responds to the user and checks whether any user revocation happens to that particular user. If there is any user revocation happens, the cloud server cannot able to respond to the user. Hence, for each revoked attribute, the cloud server needs to re-encrypt using PRE by the secret key SK of the user. Once it successfully happens the cloud server can decrypt the original file using the secret key SK of the user. Alternatively, if there is no user revocation happens and no entry in the URL means, it simply decrypts the original user content. The following algorithm is used for decryption.

INPUT : Ciphertext C = (T, C_0, C_1, ∀ x ∈ X:C_j) secret key SK = (d_0, ∀ a_j ∈ S:(d_{j1}, d_{j2})).

OUTPUT : Plaintext M or ⊥.

1) For each leaf node x ∈ X
   1.1) Let a_j denote the attribute associated with x.
   1.2) If a_j ∈ S then compute
   F_{r0} = ⊥ then T is not satisfied by s and return ⊥.
2) Else
   2.1) Compute

$$e(C_0,D_0)\ F_{r0} = e(C_0,D_0)\ e\ (g,g)^{rqr0(0)} = e(C_0,D_0)\ e\ (g,g)^{rs}$$
$$= e(g^{s}, g^{a-r})\ e\ (g,g)^{rs} = (g,g)^{as}$$
$$M = C_1 / e\ (g,g)^{as} = Me(g,g)^{as} / e\ (g,g)^{as}$$

V. PERFORMANCE EVALUATION

A. Data Integrity

Generally storage server ensures the availability of data at each and every time during the retrieval by the users. It ensures high authentication for the encrypted content from the unwanted users in the cloud. By this technique we can show that the confidentiality of the data is protected within the cloud storage as well as the data is available for the trusted users in the cloud.

B. Encryption and Decryption Time

Generally the total time requires to encrypt and decrypt the confidential content is slightly lower than the other encryption techniques. So this technique is somewhat efficient in case of large data samples. The performance comparison of total encryption time required between different algorithm is shown in figure 3.

©IJRASET 2015: All Rights are Reserved

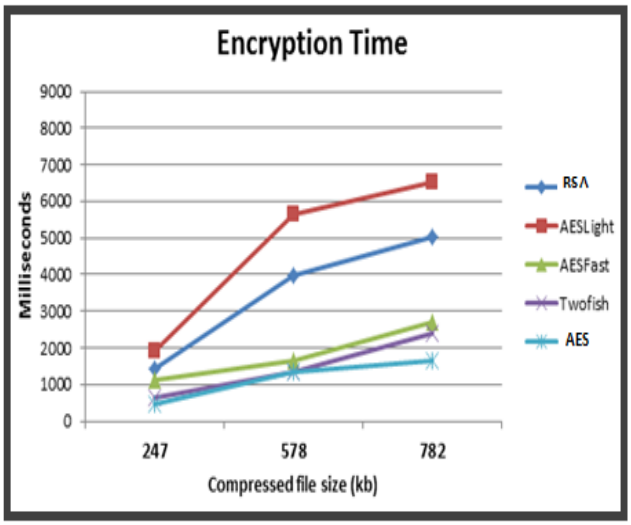
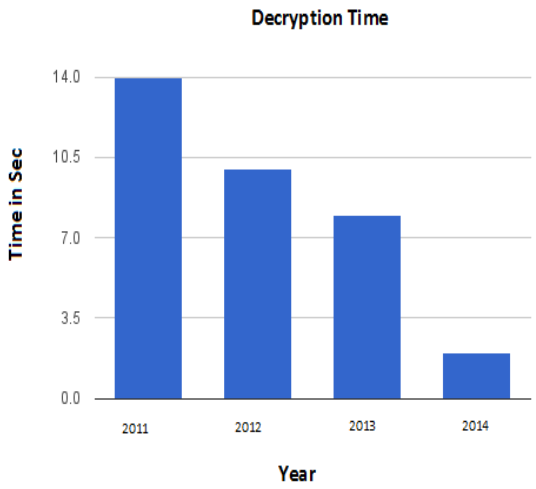


Figure 3. Encryption Time Comparison

Similarly the total time requires to complete the entire decryption process is gradually decreased from the past years. The total time required to completely decrypt the information was very large from the starting of 2011. But due to the invention of new techniques and proposed algorithms the total time required to completely decrypt the entire information content was gradually decreased and it is shown in the figure 4.



VI. AND FUTURE CONCLUSION WORK

In this paper, we discuss that the Attribute Based Encryption and Proxy Re-Encryption which is used to ensure the authentication for storing files. It guarantees high integrity and more security on the cloud users. This technique provides greater security by providing double encryption. Since using double encryption, the time required to encrypt the confidential data is much longer. Hence, in future we concentrate to reduce the total time required to encrypt the confidential data in the cloud storage. Also, we planned to test this technique using some other related algorithm for performance evaluation.

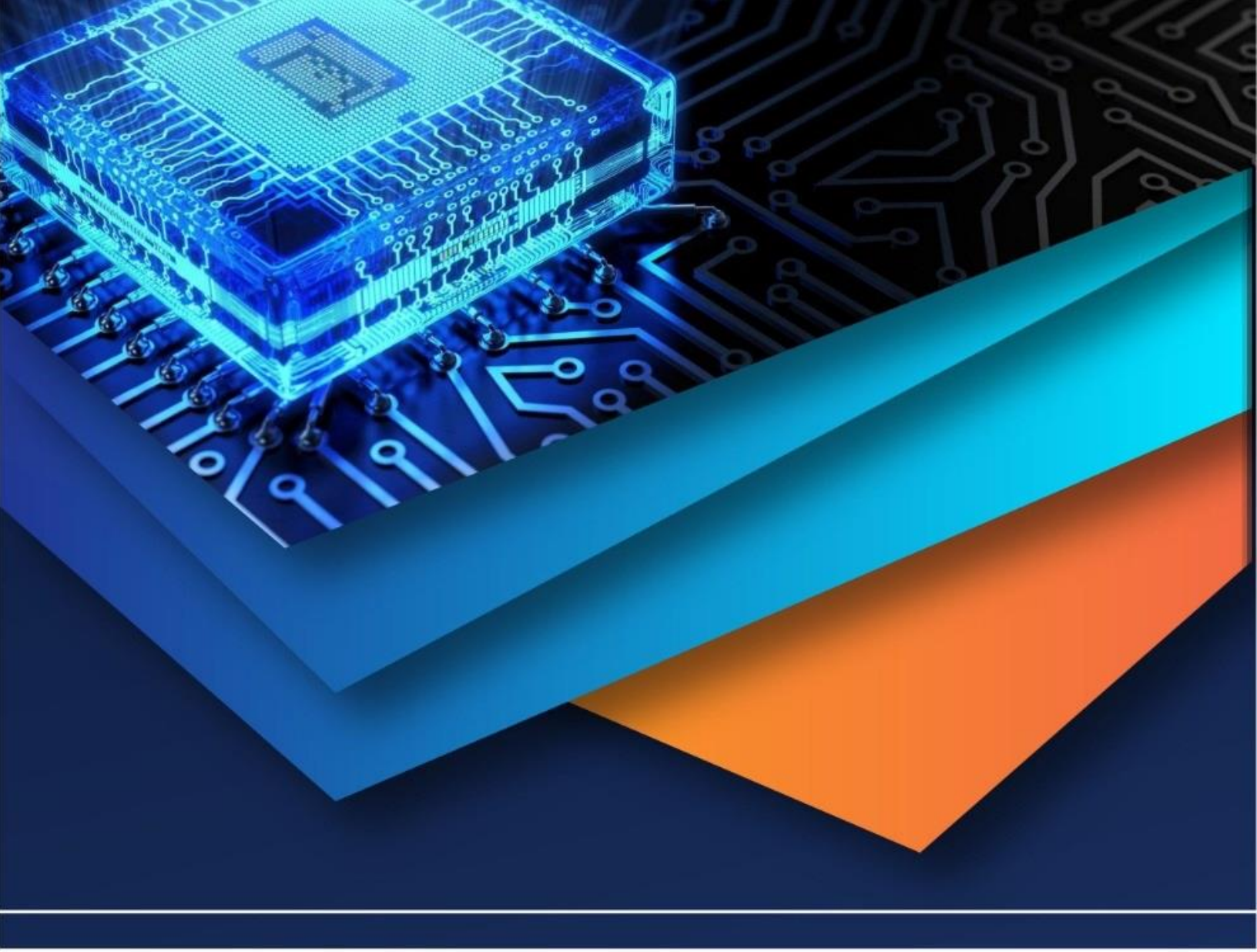
REFERENCES

[1] A.Sahaiand, B.Waters, "Fuzzy identity-based encryption," LNCS 3494 in Proc.EUROCRYPT, Aarhus, Denmark,2005,pp.457–473.
[2] D.Pointcheval and J.Stern, "Security arguments for digital signatures and blind signatures," J. Cryptology, vol.13, no.3, pp. 361–396, 2000.
[3] G.Miklau and D.Suciu, "Controlling access to published data using cryptography,"inProc.29thInt.Conf.VLDB,Berlin,Germany,2003,pp.898–909.
[4] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data

©IJRASET 2015: All Rights are Reserved

Sharing in Cloud Storage" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.
[5] J. Zhuge, T. Holz, C. Song, J. Guo, X. Han, and W. Zou. Studying malicious websites and the underground economy on the Chinese web. In Workshop on the Economics of Information Security, June 2008.
[6] J.Bethencourt, A.Sahai, and B.Waters, "Ciphertext-policy attribute-based encryption,"inProc.2007 IEEESymp.SP, Taormina,Italy,pp.321–334.
[7] J.Camenisch, M.Dubovitskaya, andG.Neven, "Oblivious transfer with access control," in Proc.16th ACM Conf.CCS, NewYork, NY, USA, 2009, pp.131–140.
[8] M. Kavitha Margret ,"International journal of advanced research in computer engineering and technology", vol.2 ,2013.
[9] S.Al-Riyami and K.Paterson, "Certificate less public key cryptography, "in Proc.ASIACRYPT2003,C.-S.Laih,Ed.Berlin,Germany: Springer,LNCS2894,pp.452–473.
[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation,"inProc.5thASIACCS, NewYork, NY, USA,2010,pp.261–270.
[11] R. Gennaro, C. Hazay, and J. S. Sorensen. Text search protocols with simulation based security in 13th International Conference on Practice and Theory in Public Key Cryptography, pages 332–350, 2010.
[12] Curtmola, R., Garay, J., Kamara, S., Ostrovsky, R.: Enhancing Definition and Efficient Constructions using Searchable Symmetric Encryption In: 13th ACM Conference on Computer and Communications Security, pp. 79–88 (2006)
[13] Boneh, D., Lynn, B., Shacham, H.: Generate Short signatures Using weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001)
[14] Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In: 19th ACM Symposium on Theory of Computing, pp. 218–229 (1987)
[15] Yao, A.C.: Protocols for secure computations. In: 23rd IEEE Symposium on Foundations of Computer Science, pp. 160–164 (1982)
[16] C. Gentry. Fully homomorphic encryption using ideal lattices. In 41st ACM Symposium on Theory of Computing, pages 169–178, 2009.
[17] V.Goyal, O.Pandey, A.Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc.13th ACMConf.CCS, NewYork, NY, USA, 2006, pp.89–98.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)