International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Secure Key Generation in Attribute Based Encryption

[1] Ch. Nagamaheshwari & Ch. Madhu Babu[2]

[1] M.Tech Student, Department of CSE, B.V. Raju Institute of Technology, Medak, Telangana, India.
[2] Professor, Department of CSE, B.V. Raju Institute of Technology, Medak, Telangana, India.

[1]nagamaheshwari.ch@gmail.com; [2]madhubabu.chunduri@bvrit.ac.in;

ABSTRACT:

Attribute Based Encryption is one the cryptographic policy which is mainly suitable for access control in cloud storage system. In the existing ABE system, CP-ABE (Cipher text Policy Attribute Based Encryption) and KP-ABE (Key policy Attribute Based Encryption) are presented. Here the key-issuing policy and decryption are very high because of high expressiveness of the ABE (Attribute Based Encryption); also third party of the system is easily accepting the data and also modifies the data. There is a chance here that if the users are increases, then the AA (Attribute Authority) system will be overloaded some times for the key issuing and key modification for the user. So, the system is very slow due to these reasons. To reduce all these, we can propose the outsourced attribute based encryption here. The key issuing process and decryption are given to the KGSP (Key Generation Service Provider) and DSP (Decryption Service Provider) respectively to make the system secure and leaving only the simple operations to the AA (attribute authority). That means reduce the overloaded operation at the attribute authority side and also we can get the check ability results correct in this process.

Key words – Access Control; key issuing; ABE; Attribute Authority; KGSP; DSP; Check ability

I. INTRODUCTION

Cloud computing suggests that sharing of resources to totally different applications. We will store any data into the cloud i.e. it's merely works sort of a server. Cloud has mainly three service models. They are: Infrastructure–as-a-service, Software-as-a-Service, and Platform as a Service. In the storage service application data owner has to store his data into the cloud, and share this data with other users via the cloud, because what proportion quantity of the area you needed to store, then you'll be able to pay the rent for less than such area within the cloud system. Whenever user desires to use the files from the system then he will login to the system and regardless of the files he wish to access then he will take those files. Meaning in cloud computing not solely one user access the knowledge from the system however conjointly multiple users will access the info. In cloud more number of the data is presented. So, we need to provide the confidentiality for the data presented in this system. So, the data must be encrypted before stored into the cloud. Here we are using the Attribute Based Encryption for confidentiality of data. The ABE scheme used here as an identity attributes, and also CP-ABE [7], [8] scheme, KP –ABE scheme [6] is presented here. The cipher text of the data which is associated with in the CP- ABE scheme and in KP –ABE, access policy which is assigned in a private key. The particular key of the user can decrypt particular cipher text only if associate attributes are matched. The data owner here uses the authorized user's public key for

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

encryption of the data. The user's private key is built into the Key-policy attribute-based encryption (KP-ABE) scheme and the access policy which is built in the user's private key and the encrypted data described with user's attributes. The KP-ABE scheme more exhibit to control users than ABE scheme. But the disadvantage here is that in KP-ABE the access policy is associated with a user's private key, so data owner did not understand to choose who can decrypt the data except that the attributes which can describe this data. And it is not suitable in some application because a data owner here trust the key issuer [10]. In CP-ABE scheme it is reverse process. Here the access policy associated with the encrypted data and set of attributes are associated in a user's key. The main problem of CP-ABE scheme is, in KP-ABE the data owner only trusts the key issuer [10]. To evaluate the performance of our ABE scheme with verifiable results of outsourced decryption, we implement the CP-ABE scheme having verifiable outsourced decryption and conduct experiments. In recent days cloud may concentrate on the data security, the sensitive data which is presented in a cloud system, sometimes it may manage and maintained by the untreated CSP (cloud service provider). The main drawback here is the decryption process is more complex. So, we need to improve the efficiency of the ABE.

II. RELATED WORKS

In Identity based encryption (IBE) without using the public key certificate the sender can encrypt a message here. By using the public key encryption without any certificate has some practical applications. Suppose a sender can send a mail to any recipient. Then the recipient may not be present in online or the sender no need to check his public key certificate for sending the mail. The mail will automatically send to the recipient without these.

Here we are using other type of Identity based encryption, that we call it as fuzzy Identity-Based Encryption [1]. Here we are considering identities as set of descriptive attributes. It will give new applications. They first one is as Identity based encryption; second one is Attribute based encryption. The Identity-Based Encryption uses the biometric identities and Attribute based encryption uses the set of attributes.

In Attribute based encryption the encryption of the message can send to all the users. Suppose in an Industry, the manager send a message to his department to recruit the people. The message can send an identity like this way {_recruit-employees_, _department_}. If any person want to decrypt the message, then he has the certain attributes are required to do the decryption.

Cloud computing transfer the traditional internet computing paradigm and IT industry. The development of the wireless technology it can expected to implement in the mobile environment [4] also. The main user concern is that security, because sensitive data is presented in the cloud systems, it is maintain and managed by the untrusted service providers.

Thus, new secure service architectures are needed for the security concerns of users for using these cloud computing techniques.

III. EXISTING SYSTEM

In this system mainly KP–ABE (Key policy Attribute Based Encryption) and CP–ABE (Cipher Text Policy Attribute based Encryption) are presented. In KP–ABE, access policy is given to the private key, where as in CP –ABE; access policy is given to the cipher text. Here KGC (Key Generation Centre) can decrypt every cipher text addressed to specific users by generating their attribute keys. This could be a potential threat to the data confidentiality or

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

privacy in the data sharing systems. And another problem here is key revocation problem. In this some users may want to change their attribute keys or some users need to update their key. Sometimes the attribute of the user is shared by the multiple users. This would affect the overall system; finally the system would be unsecure at this time. To avoid this we can enter into the proposed system.

IV. PROPOSED SYSTEM

The proposed system is most suitable for data sharing. In this system, some users may want to change their key or key update. The users cannot trust the KGC for protecting the data. So, here data confidentiality is also presented to make the system secure. During the key generation at the attribute authority, the partial private key of user can give to the KGSP to reduce the local overhead at the attribute authority side. And during the decryption phase the partial decryption is provided at Decryption Service provider (DSP) and the overall decryption is provided at local. Finally the users encrypt the data only once and the remaining task can be given to the data centre. The data storing centers can take care about the re-encryption and key revocation. The CSP can give the results here are correct way.

ARCHITECTURE:

Abbreviations:

KGSP – Key Generation Service Provider

DSP – Decryption Service Provider

SSP – Storage Service Provider

AA – Attribute Authority

U –User

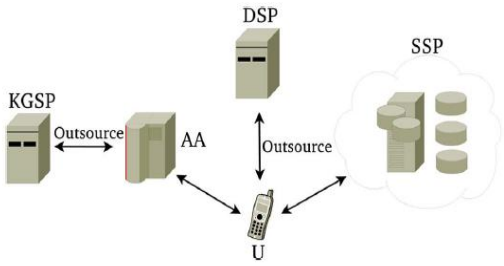

Fig 1: ABE Architecture

V. LITERATURE SURVEY

ATTRIBUTE AUTHORITY

It is also known as a data owner who has the permission to store the file into the cloud system. He can enter into the system by using his credentials and upload the file into the SSP (Storage Service Provider). While uploading the file data owner give the access permissions to the user based on the attribute. The data owner also give the checksum for the file, because of this the CSP may not give the results incorrectly.

KEY GENERATION SERVICE PROVIDER

Key generation service provider mainly associated with the user side and the attribute authority side. It is mostly used for the key generation. KGSP can reduce the overload at the attribute authority side when the user can request for the private key or key update. Key revocation and key update process are all under KGSP. Here, the KGSP can send the users encrypted password to his mail-id. The session password which is generated by the KGSP is used whenever user wants to download the file original file.

STORAGE SERVICE PROVIER

All the files which are uploaded in cloud are stored here. The files here are accessed by only the authorized users. And it is also prevent the access of outside users to access the files, i.e.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

unauthorized users may not access the files here. When the authorized users want to access the file present in SSP, it will send the requested files to the user. Then only the user can download the files from SSP.

DECRYPTION SERVICE PROVIDER

The main role of DSP is to generate the decrypted key. Whenever the user can request for the decryption of the encrypted key, then the DSP will provide the decrypted key for it. The data owner who has to upload the files in SSP will store in an encrypted format, and then the file will be accessed by the authorized user only if associated attributes are matched. That means the user has the downloading permissions to access the file form the DSP. Finally the user can download the file in a decrypted format.

DATA USER

The Data User having his own id and password after register by himself. He can enter into the system by using these credentials. He has set of attributes to access the encrypted file from the system. Finally he will get the decrypted the cipher text i.e. access the original file.

A. ELLIPTIC CURVE CRYPTO GRAPHY (ECC)

Using Elliptic Curve Cryptography (ECC) algorithm data is encrypted and decrypted. It is mainly used for checking of exchanging cryptographic keys for encrypting the data and also decrypting the data. ECC is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size. ECC equation is created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Equations based on elliptic curves are very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse. An elliptic curve is the set of points that satisfy a specific mathematical equation.

An elliptic curve equation is here like this:

$y2 = x\,3 + ax + b$

B. ALGORITHM OF ECC DIFFIE-HELLMAN KEY EXCHANGE

1. Users select an elliptic curve Eq (a, b) with parameters a, b and q, where q is a prime and G is a point on Elliptic curve whose order is large value n.
2. Users A and B select private keys $nA<n$, $nB < n$.
3. The public keys are: $PA= nA \times G$, $PB = nB \times G$.
4. They calculate shared secret key: $K= nA \times PB$, $K= nB \times PA$.

The two calculations in step 4 produce the same result because $nA \times PB= nA\times (nB \times G) = nB\times (nA \times G) = nB \times PA$

To break this scheme, an attacker would need to be able cm = {kG, Pm + kPB}

Note that A has used B‘s public key PB.

To decrypt the cipher text, B multiplies the first point in the pair by B‘s secret key and subtracts the result from the second point:

$Pm + kPB- n\,(kG) = Pm + k\,(nBG) - nB\,(kG) = Pm.$

PROPOSED ALGORITHM:

1. The data owner has permission to upload the files into the cloud system.
2. The data owner will defines the file access policy by using the attribute based encryption.
3. The data owner also has the permission for which type of file he has to be placed in the system.
4. The data owner only will give the access permissions to the user.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

5. The file here gets encrypted by using the ECDH algorithm.
6. After uploading the file the data owner finds the checksum for the file.
7. To provide the check ability of the file we find the checksum for the file.
8. The user registered him and one password is generated and sent to his mail.
9. The password here is encrypted format and he can decrypt the password for login to the system.
10. Then the user login to the system with his valid id and password.
11. If the user satisfies associate attributes then only the file will be displayed to him.
12. The user wants to download the file from the system.
13. Here the user will search for the key to download.
14. The session key which is generated by using the KGSP for the user, and he enter this key to the system after that he download the file.
15. Finally DSP will decrypt the file into the original format while downloading for the user.
16. The user can download his file into his local machine.

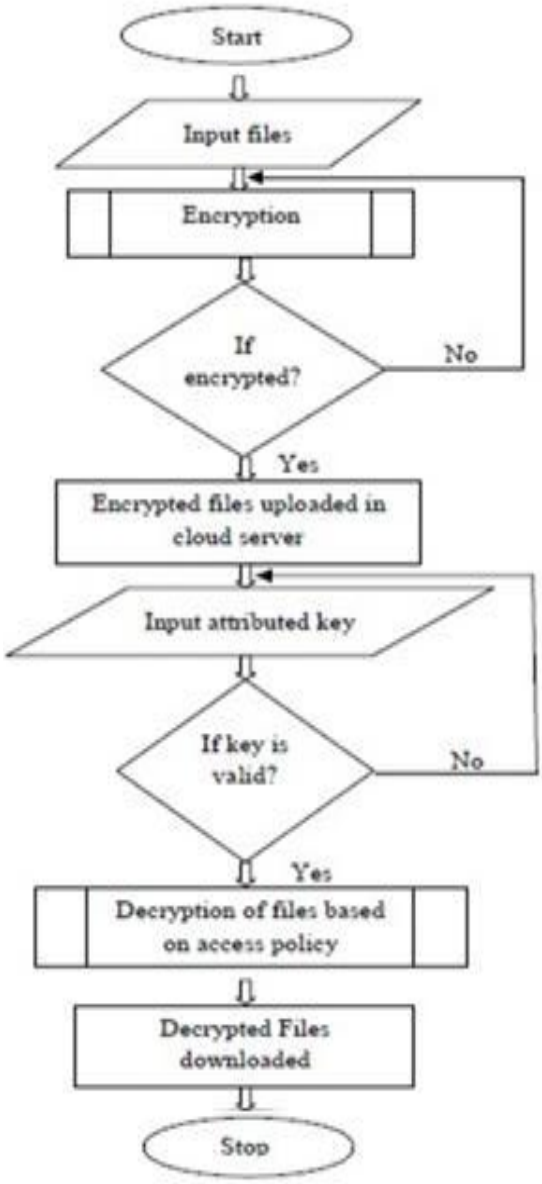

Fig 2: Flow chart for Proposed Algorithm

PERFORMANCE:

To evaluate the performance of the system, the encryption time, key generation time and decryption time are calculated. The time taken by CPABE outsourcing scheme is calculated on Integrated Development Environment (IDE) Visual Studio (C#.Net) while the database is kept in Microsoft Azure Database. Performance analysis is done by calculating Encryption and upload time, Decryption and download time and key generation time. Performance analysis is done using different file sizes and the results are

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

obtained by noting down the time taken for encrypting those files with different sizes, time taken for decrypting those files and time taken for key generation.

A.TIME FOR ENCRYPTION AND UPLOADING THE FILE

To evaluate CPABE performance, I have measured time taken to encrypt and upload the file on the SQL Azure Database by using different file sizes—1 KB, 2 KB, 5 KB, 50 KB, 100 KB. To capture time used for encryption and uploading the file, I have used the following code. String st, et;

et = DateTime.Now.Millisecond.ToString ();

// Here the module code and the query will run which will connect with the Microsoft Azure database

intiet = Convert.ToInt16(et);

intist = Convert.ToInt16(st);

Intft = iet - ist;

Label1.Text = ft.ToString ();

I have written this code in the essential class files of my project and then execute it. This code will take the current system time and then run the code and the query in it and then captures the time which it takes for doing so. Then it subtracts that system time from the time it captures and returns the result in the label which is placed for that purpose.

B. KEY GENERATION TIME:

Key generation time here is to generate key while downloading file form the system. Here the file sizes used are 1KB, 2KB, 5KB, 50KB, and 100KB. And by using the same files we have to note the time for generating the secret key which is used for the file downloading process.

C. DOWNLOAD AND DECRYPTION TIME:

To find the time for downloading process and decryption process files using both proposed system (CPABE) and existing system (IBE). These files were staged on SQL Azure Database file repository. The operations which are performed while downloading file are: the encrypted file is taken from Storage Service Provider, and the file is decrypted by using the user's private key. If the file size increases then decryption time is also increases.

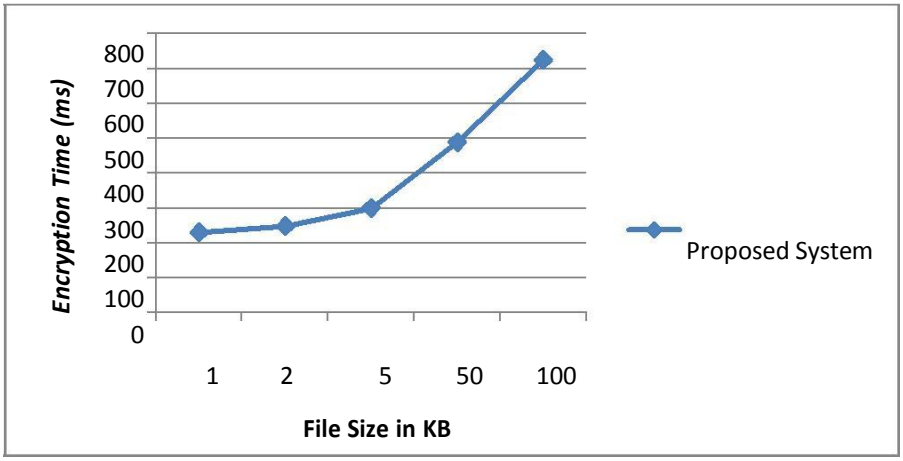

Fig 3: Encryption time taken by the proposed scheme

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

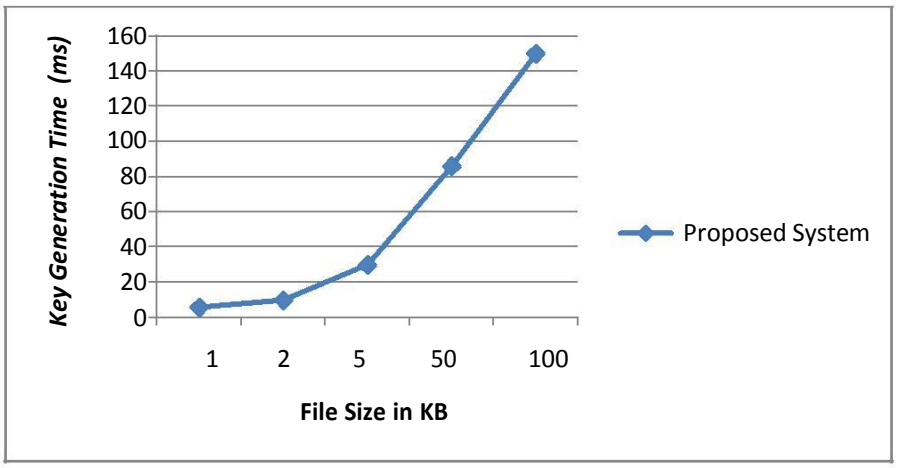

Fig 4: Key Generation time taken by the proposed scheme

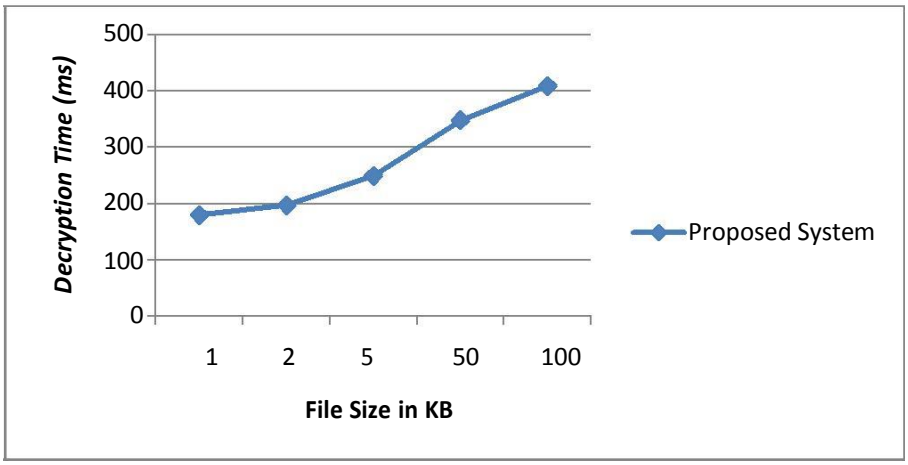

Fig 5: Decryption time taken by the proposed scheme

VI. CONCLUSION & FUTURE WORK

We are using the Outsourced ABE proposed. The KGSP and DSP are performed main role here. This will give constant efficiency at the user side and also at the attribute authority side. Depending on the size of the file the encryption and decryption time will be increases or decreases, i.e. if the file size is more, the time taken for encryption and decryption are more. If the file size is small the time taken for encryption and decryption are less. In the proposed system time taken for encryption, decryption and for key generation, is in milliseconds.

The overhead is reduced at both attribute authority side and the user side while key issuing. Here data owner can take care about the overall system. In the system multiple authorities in -an application is allowed. When encryption provides data confidentiality, it also greatly limits the flexibility of data operation. To address this issue, it is needed to combine ABE with cryptographic primitives such as searchable encryption, private information retrieval and homomorphism encryption to enable computations on encrypted data without decrypting.

VII.REFERENCES:

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Proc. Adv. Cryptol. EUROCRYPT, LNCS 3494, R. Cramer, Ed., Berlin, Germany, 2005, pp. 457-473, Springer.

[2] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," in Proc. 20th USENIX Conf. SEC, 2011, p. 34.

[3] 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 ESORICS, 2013.

[4] Z. Zhou and D. Huang, "Efficient and Secure Data Storage Operations for Mobile Cloud Computing," in Cryptology ePrint Archive, Report 2011/185, 2011.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, Fine-Grained Data Access Control in Cloud Computing," in Proc. IEEE 29th INFOCOM, 2010, pp. 534-542.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine Grained Access Control of Encrypted Data," in Proc. 13th ACM Conf. Comput. Commun.

[7] L. Cheung and C. Newport, "Provably Secure Ciphertext Policy ABE," in Proc. 14th ACM Conf. CCS, 2007, pp. 456-465.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext- Policy Attribute-Based Encryption," in Proc. IEEE Symp. Security Privacy, May 2007, pp. 321-334.

[9] A. Beimel. "Secure Schemes for Secret Sharing and Key Distribution". PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[10] . R. Canetti, B. Riva, and G. Rothblum, "Two Protocols for Delegation of Computation," in Proc. Inf. Theor. Security, LNCS 7412, A. Smith, Ed., Berlin, Germany, 2012, pp. 37-61, Springer Verlag.

[11] J. Lai, R. Deng, C. Guan, and J. Weng, "Attributebased Encryption with Verifiable Outsourced Decryption," IEEE Trans. Inf. Forensics Security, vol.8, no. 8, pp. 1343-1354, Aug. 2013.

[12] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

[13] R. Canetti, B. Riva, and G. N. Rothblum, "Practical Delegation of Computation Using Multiple Servers," in Proc. 18th ACM Conf.CCS, 2011, pp. 445-454.

[14] N. P. Smart. Access control using pairing based cryptography. In CT-RSA, pages 111–121, 2003.

[15] A. Shamir. How to share a secret. Commun. ACM, 22(11):612–613, 1979.

[16] A. Shamir. "Identity Based Cryptosystems and Signature Schemes. In Advances in Cryptology – IJRECS @ July – Aug 2015, V-3, I ISSN-2321-5485 (Online) 2371 www.ijrecs.in CRYPTO, volume 196 of LNCS, pages 37 Springer, 1984.

[17] R. Canetti, S. Halevi, and J. Katz. "Chosen Cipher text Security from Identity Based Encryption. In Advances in Cryptology – Eurocrypt," volume LNCS, pages 207–222. Springer, 2004.