PRIVACY PRESERVING THROUGH MEDIATOR IN DECENTRALIZED CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION

Varsha Thanaji Mulik[1], Shinu Acca Mani[2], Saritha K[3], Suraj U Rasal[4]

[1] M.Tech Student, Department of Computer Science & Engineering, Nehru College of Engineering & Research Centre, Thrissur, India. ***varshasurajrasal@gmail.com***

[2]Assistant Professor, Department of Computer Science & Engineering, Nehru College of Engineering & Research Centre, Thrissur, India. ***shinuaccamani1022@ncerc.ac.in***

[3]Assistant Professor, Dept of Computer Science & Engineering, Nehru College of Engineering & Research Centre, Thrissur, India. ***Saritha.cse@ncerc.ac.in***

[4]Assistant Professor, Department of Computer Engineering, Bharati Vidyapeeth Deemed University's, College of Engineering, Pune, India. ***surasal@bvucoep.edu.in***

Abstract

In the previous cryptographic approach, network security is vigorously relied on user attribute based encryption, multiple authorities and cipher text policies to make it more sheltered to some extent. But to seal the lack of security level, cryptography shows keen to enhance the protective approach. Cipher text policy is one of the best cryptographic methods added to enhance the security level in recent networking trends. In this paper, both user attributes and data attributes are used as security credentials. File security is maintained by protecting data and its location. Multiple trusted authorities and Mediators are considered as validation users to make system more secure and reliable. Mediator concept is added to the proposed approach whose role is acting as a middleware between authorities and users for managing user rights. Data is stored in encrypted format and its regarding information can be accessed through the secrete key which is a combination of authority key and mediator key. Decryption speed is enhanced to balance the user waiting and response time. Since there is no storage of any user and data information in authority and mediator the entire data will be hidden. All these approaches enhance the encryption level to make system more secure and highly reliable.

Keywords: *Mediator, Trusted Authority, Data Attributes, User Attributes.*

---***---

I. INTRODUCTION

Networking is heavily based upon modern cryptographic technique which is a study of secret writing. Cryptography is an art which focuses on the methods of transforming original data into intelligible form and then transforming into original form.

Internet is also a source of data storage which shares the data only with the authenticated users. A user is said to be valid or authenticated user if and only if he have confirmed identity. Authentication can be also done by using certificates.

Traditional Asymmetric Cryptography is the previously existing public key encryption technique which uses certificate for identification purpose. Certificate is an electronic document which contains information about keys, user identity and digital signature. In this scheme, a certificate authority is used which provides an individual certificate for each user. Here a limitation occurs when number of users increase. As the number of users increases the number of certificates also increases. Due to which database used for certificate storage will get overloaded. As an alternative to traditional public key encryption techniques, in 1984 Shamir introduced a new concept of Identity Based Encryption (IBE) to eliminate certificate storage. Shamir's approach used user's own identity such as an email-id or phone number as the public key instead of using the certificates. The IBE approach was first practically implemented in 2001. However, one to one communication is possible only by using IBE approach; it is not applicable for one to many communications. To resolve this problem, Fuzzy IBE [14] was introduced in the seminal work of Sahai and Waters. In fuzzy IBE we view identities as a set of descriptive attributes. It is a public – key encryption system that leads to an Attribute based encryption (ABE). In an ABE scheme a single central authority is responsible for maintaining the access control level. It becomes a challenge for a single authority when the numbers of user's are huge. In order to solve this problem a multiple authority ABE (MABE) scheme was designed by Sahai and Waters and later extended by Melissa Chase [8][7] in 2009. MABE services are mostly applicable on distributed system. So MABE makes the use of cryptographic technique which is called as Ciphertext Policy Based Encryption.

In order to resolve the problems of fine grained access control on shared data in one to many communication, Ciphertext Policy Attribute Based Encryption (CPABE) [10][11] technique is proposed. Here MABE requires multiple authorities which depend upon a single central authority. Overall system failure may occur when central authority get's crashed. In order to reduce the trust on central authority, Decentralized Cipher text Policy-ABE (DCP-ABE) approach is proposed by Lewko and Waters [4].In this DCP-ABE scheme multiple authorities are used which works independently without any cooperation. It doesn't require central authority. These existing techniques can be extended using distributed policy along with Mediator. Section 2 describes literature survey followed by research methodology. Section 3 and section 4 contains implementation details and then conclusion.

II. EXISTING APPROACHES

Cryptographic approach was enhanced with IBE, FIBE, MA-ABE and DCP-ABE. This literature survey shows how such cryptographic parameters has been studied and referenced for further module.

A. Identity based encryption

The initial IBE scheme was introduced by Boneh and Franklin, which was based upon random oracle model [17]. Further IBE is extended by using standard model [15], [16]. Shamir introduced an alternative to traditional public key encryption techniques in 1998 which is named as Identity Based Encryption (IBE) [19] .This approach eliminates certificate storage. Simplification of certificate management in email system was the original motivation for IBE [18]. Here sender generates cipher text by using receiver's public key and the receiver decrypt the data by using private key which is given by PKG. Here a single key generation sender is utilized by both the users. But IBE have some limitations, it can support only one to one communication not one to many communications.

B. Attribute based encryption

Multicast communication is possible by using FIBE scheme. Sahai and Waters [14] had introduced first ABE scheme in which a set of attributes are tied with ciphertext and secret key. Further, Amit Sahai and Brent Waters have proposed a new scheme in 2005 which is named as Fuzzy Identity Based Encryption. FIBE gives two interesting applications. IBE is the first application which uses biometric identities of user. For example: iris scan, finger print. We can't use IBE system because biometric measurements are noisy. Fuzzy IBE is the second application that we call "Attribute Based Encryption" ABE. ABE scheme encrypts a document to all users who have a certain set of attributes and also it is applicable for multicast communication. ABE have two complimentary forms which are given by Goyal Pandey, sahai and Waters [13]. They are: Key Policy ABE (KP-ABE) and Cipher text Policy ABE (CP-ABE) [9][12].

C. Multi-authority attribute based encryption

Multiauthority ciphertext policy ABE (MACP-ABE) scheme is constructed on the basis of standard model by Lin et al [5][6]. Further, to reduce the trust on central authority Chase [8] proposed a new scheme Multiple Authority Based Encryption (MABE). MABE approach aims to resist the collusion. Here user secret keys are tied to GID. In [8] a central authority is required which control all other multiple authorities. In order to initialize system, multiple authorities must cooperate with each other. This scheme guarantees the security of encrypted data. But this work had some problems related to collusion. The collusion problem is prevented by using the approach [10] which is given by Sahani and water. In multiple authority schemes, user attributes are shared between multiple authorities who gives multiple sub secret keys. These sub secret keys are linked using the Chase [8] concept of global identifiers.

D. Decentralized cipher policy attribute based encryption

Jinguang and Willy Susilo [1] introduced Improving privacy and security in Decentralized Cipertext Policy Attribute Based Encryption scheme which doesn't require a central authority for monitoring and initializing system. Existing decentralized cipher text policy ABE is [4] constructed on the basis of random oracle model while the PPDCP-ABE (Privacy Preserving DCP-ABE) is based upon standard model [2][3].

In PPDCP-ABE scheme a decentralized environment is utilized, which contains multiple authorities for generating the secret keys for the user without knowing anything about the user attributes and Global Identifier (GID). That is the user attributes and GID is hidden from the authorities. Here the user must convince each authority that the user attributes are monitored by the authority itself. This scheme uses an anonymous credential system in which an issuer provides a credential to user. The credential includes user's attributes and pseudonym. By using this credential the user convince the multiple authorities that, he is monitoring the user attribute and GID. This condition is implemented by using the set membership function proof technique. These multiple authorities work independently without any cooperation with each other and also can join or leave the system dynamically without effecting remaining authorities. An attractive feature of this system is, re initialization of the system and change in the secret key of the authorities are not required when any authority dynamically leave or join the system. Here each authority maintains a set of attributes of different users to generate secret keys for them. The architecture of DCP-ABE system is given below.

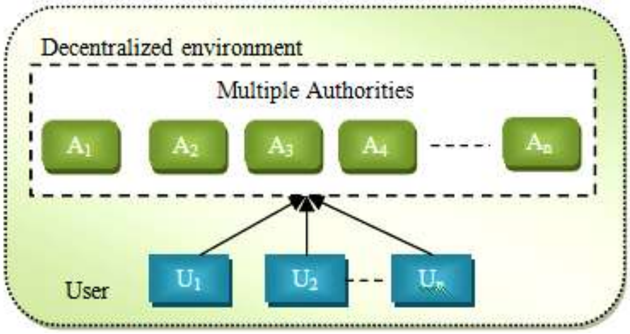

Fig.1. DCP-ABE System Architecture

III. PROPOSED SYSTEM

Newly proposed DCP-ABE-M system provides a crucial improvement in security as well as efficiency. Authorized mediators and authorities are the two essential parts of our system which are organized based upon some specific attributes. Mediator is an important stepping stone of our system which we have newly added to the existing DCP-ABE scheme in order to increase the security. Here we have allocated a number of authorities whose functionality is based upon some specific attributes. The main purpose of authorized authority is to generate secret keys for the user by using his data and user attributes. This secret key is divided into two parts and then one half part is stored in authority table of authority and remaining part is stored in mirror table of mediator. Our system doesn't store any user information such as user attributes, data attributes, GID, complete secret key either in mediator or in authority. In case, if any one of the authorities gets crashed, then the proposed system will automatically allocate a new authority which has same attributes and functionality as the crashed one. If the new authority is eligible or satisfies the given policy and protocol suit of our system then the system will provide authority membership to the new authority [1]. After confirming the authority membership, the system will provide a secret key for the new authority which will allow the new authority to get entered into our system. The purpose of monitoring and controlling of mediator is done by using Trusted Authority (TA). In case, any mediator get's failed the proposed system will use TA for mediator backup purpose. Instead of accessing the main DB, this proposed system will utilize TA for information retrieval in less time.

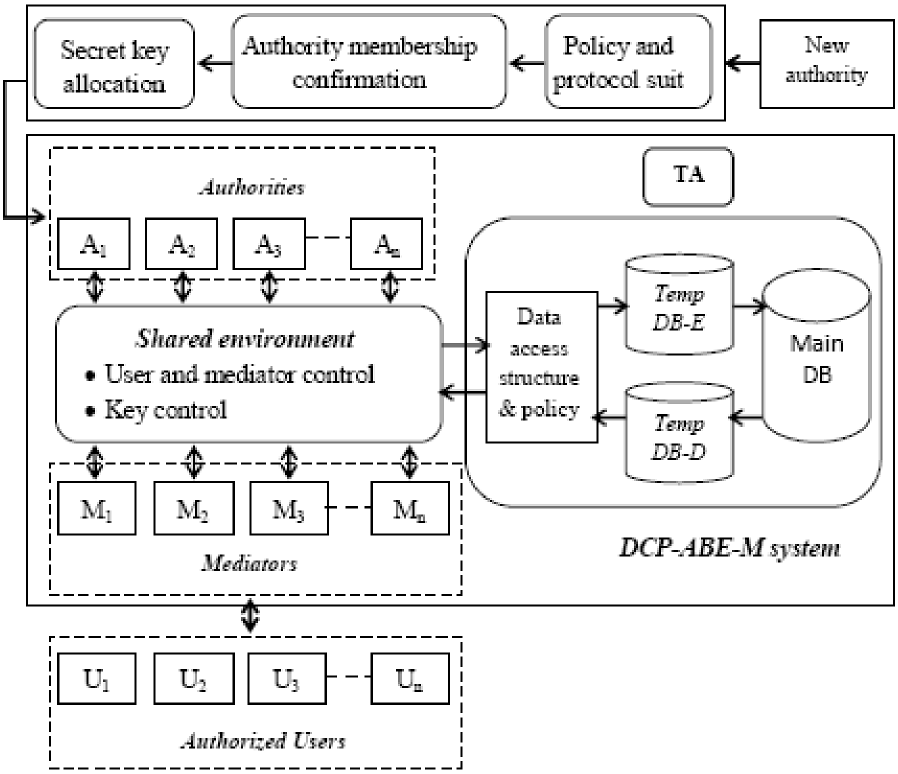

Fig.2. DCP-ABE-M System Architecture

In above given fig.2 authorized users are the verified users who have the ability to access the system. Any user can become a verified user if and only if he satisfies all the conditions given by system. When the new user enters into system, system will automatically generate user ID and user key for the new user for identification purpose. In this scheme, encryption is performed two times in order to increase the security level. The proposed scheme is implemented by using two algorithms: Deffi Hellman and RSA. These two algorithms together provide more secure system as compared to previous DCP-ABE.

The proposed DCP-ABE-M scheme creates temporary data bases: Temp DB-E and Temp DB-D for encryption and decryption purpose. Temp DB-E is build for each and every user to store his user attributes, data attribute, jar files, directories when he enter into the system. After secret key generation entire information is stored in main database and then the temp DB-E is deleted. Similarly, Temp DB-D is build for each and every user for decryption purpose and after decryption the temp DB-D is deleted. In this proposed scheme authorities and mediators don't have contact with main DB. Since there is no direct access to main data base our system is more secure than previously existing techniques. Here data access structure and policies are applied during the data retrieval. The data can be recovered if and only if the user gets the secret key and satisfies the access policies. The below given figure shows data base access method.

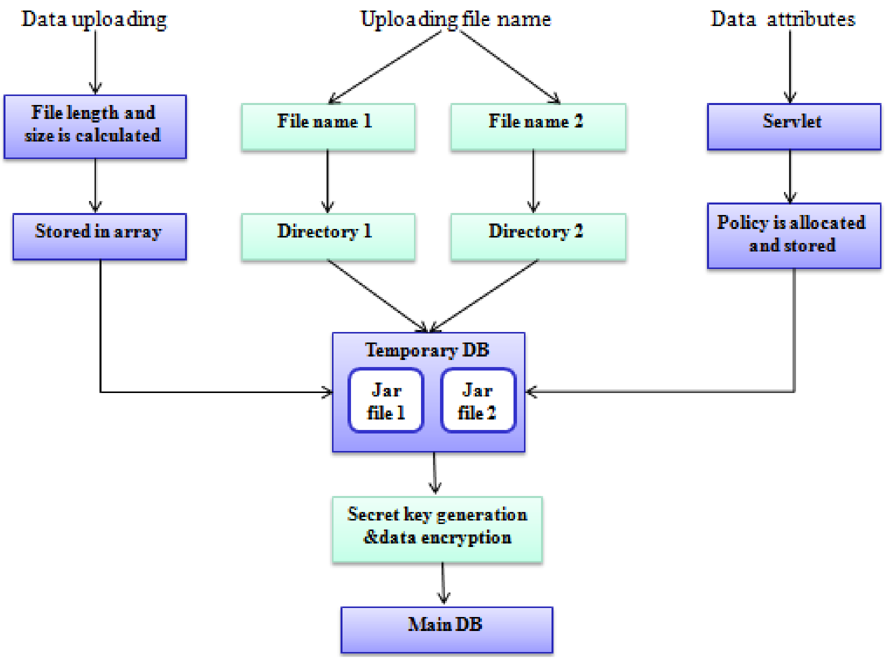

Fig.3. Data Base Access Method in DCP-ABE-M

A. Encryption

The proposed DCP-ABE-M scheme provides more secure system in which the encryption level is increased by using mediators. When the authorized user enters into the system, it will set a decrypted path and create a session for that user. The system first checks the user attribute set for user identification. Then it will provide an array for each user for storing the uploading data size, file type, file name etc. since the proposed system uses both user attributes and data attributes instead of using only user attribute, will increase the efficiency and security level then the existing schemes.

Our system stores the data attributes in servlet. Then the system provides a specific data directory or path for data storage. The given file name is split into two and it is stored in two newly created directories. Based upon attributes, policy is allocated and stored. All these information's are stored in two different jar files and these jar files are stored in Tem DB-E. The encryption process is shown as flow chart in below given figure.

According to user type and attribute, authority and mediator is allocated. Authority generate secret key by using main attribute set.

That is

U_A : { a_1 ,a_2 ,a_3 ....a_n }
D_A : { d_1 ,d_2 ,d_3 ....d_n }
$M_{A:}$ { a_1 ,a_2 ,a_3 ....a_n , d_1 ,d_2 ,d_3 ....d_n }

Which gives $M_A = U_A \cup D_A$. Where U_A indicates user attribute set, D_A indicates data attribute set and M_A indicates main attribute set. By using M_A secret key is generated. This secret key is split into two: mediator key which is made of data attributes and user key which is made of user attributes. The proposed system also calculates the different key generation time, encryption time and stores it in DB. Mediator is allocated according to type of user and based upon the result of user verification. Type of user is identified by one of the secret user attribute. Then mediator identifies the authority accordingly and authority generates encryption key from main attribute set $M_{A.}$

$$E_K = (U_A+D_A)_K$$

$$E_K = (U_{AK}+D_{AK})$$

It is not possible to decrypt the data without E_K. E_K is a combination of (U_{AK}+D_{AK}).

B. Decryption

When a registered user sends a data request access our system will check the user details and it allocated a mediator for that user based upon his attribute. That is if the user is a student then the system will allocate student mediator for that user. Then the mediator will forward the access request to a specific attribute based authority. That is if the user is a student of cse department then our system will allocate a student mediator and a cse department authority. if the user is valid then the mediator will provide the mediator key and will send the request to authority where the authority also provides the authority key. Then proposed system will combine both the keys and generates secret key. Our system will only allow unlocking the file using this secret key. In order to open the file user must satisfy the given policy. We have included two level of encryption. First encryption is performed on the data content and second encryption is performed on the data location. Data location is decrypted if the user satisfies the policy. Authority selection is done on the basis of user request. Selected authority sends its stored authority key A_K which is a user key to the system. Already stored user key is fetched so termed as authority key. Mediator request is initiated after receiving authority key from authority. Mediator sends its M_K to the system. Received user and mediator keys are combined to form decryption key. Now RSA decryption algorithmic approach is applied to form decryption key D_K.

$M_K + A_K = D_K$

E_K is split into two sub keys as it is stated above. Same attributes are used to form encryption key including user and data attributes.

$M_K + A_K = (U_A+D_A)_K$

$M_K + A_K = (U_{AK}+D_{AK})$

$M_K + A_K = E_K$

$E_K = D_K$

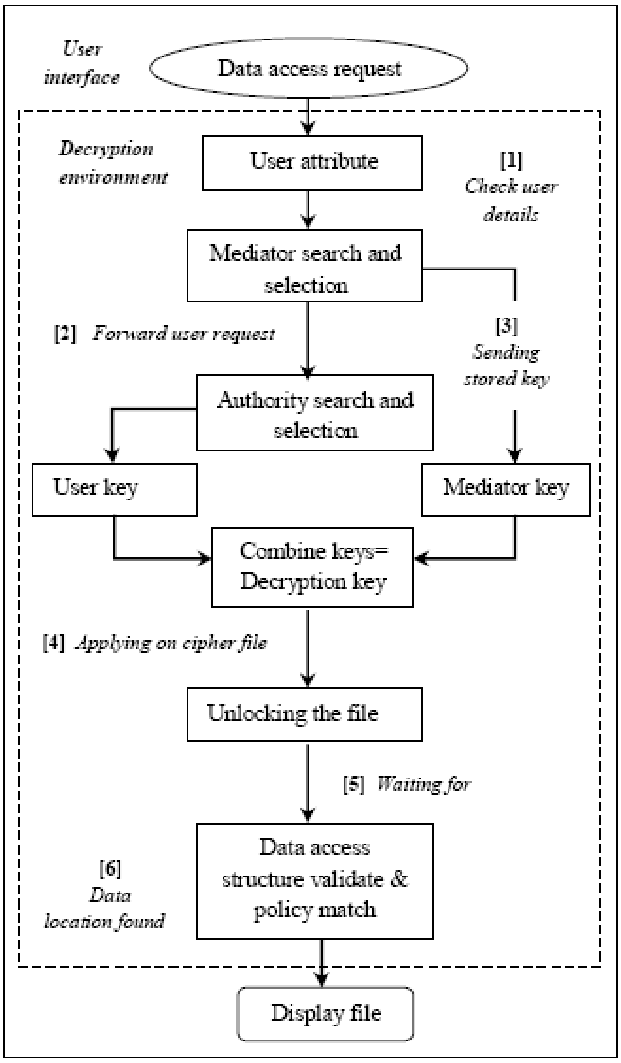

Fig.4. Decryption in DCP-ABE-M System

In decryption, keys are directly fetched after request is generated. This key fetching is done after authority check and user validation. The above given figure shows the flow of decryption process.

IV. CONCLUSION

To overcome with user attribute leak problem, user attribute and data attributes are considered while applying encryption. In the present cryptographic approach, attribute based encryption and cipher text policy are not sufficient cryptographic techniques to enhance the security level. In proposed approach, mediator is added as kind of user which enhances the security by adding the level in encryption. It provides secured management of user rights through authorities. Decryption speed is enhanced to balance the user waiting and response time. Authorities and mediators are managed by trusted authority so that they can be relocated at their failure. In this scheme new approaches are added as usage of user & data attributes, encrypting data and its location, mediator concept, automatic authority and mediator assigning on their failure which shows that the proposed DCP-ABE-M scheme is highly secured and reliable.

REFERENCES

[1] Jinguang han, member, ieee, willy susilo, senior member, ieee, yi mu, senior member, ieee, jianying zhou, and man ho allen au, member, ieee. (march 2015). improving privacy and security in decentralized ciphertext-policy attribute-based encryption. ieee transactions on information forensics and security. vol. 10, no. 3 (1), 665-678.

[2] H. Qian, J. Li, and Y. Zhang, “Privacy-preserving decentralized cipher text-policy attribute-based encryption with fully hidden access structure,” in Information and Communications Security (Lecture Notes in Computer Science), vol. 8233. Heidelberg, Germany: Springer-Verlag, 2013, pp. 363–372.

[3] J. Han, W. Susilo, Y. Mu, and J. Yan, “Privacy-preserving decentralized key-policy attribute based encryption,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2162, Nov. 2012.

[4] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 6632. Heid.elberg, Germany: Springer-Verlag, 2011, pp. 568–588.

[5] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,” in Progress in Cryptology (Lecture Notes in Computer Science), vol. 5365. Heidelberg, Germany: Springer-Verlag, 2008, pp. 426–436. 678 ieee transactions on information forensics and security, vol. 10, no. 3, march 2015.

[6] Kan Yang, student member, ieee, and xiaohua jia, fellow, ieee. (july 2014). expressive, efficient, and revocable data access control for multi-authority

cloud storage. ieee transactions on parallel and distributed systems. vol. 25, no. 7 (1), 1735-1744.

[7] M. Chase and S. S. Chow, “Improving privacy and security in multiauthority attribute-based encryption,” in Proc. 16th ACM Conf. CCS, 2009, pp. 121–130.

[8] M. Chase, “Multi-authority attribute based encryption,” in Theory of Cryptography 2007, (Lecture Notes in Computer Science), vol. 4392. Heidelberg, Germany: Springer-Verlag, pp. 515–534..

[9] J. Herranz, F. Laguillaumie, and C. Ràfols, “Constant size cipher texts in threshold attribute-based encryption,” in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6056. Heidelberg, Germany: Springer-Verlag, 2010, pp. 19–34.

[10] J.Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in Proc. IEEE Symp. SP, May 2007, pp. 321–334.

[11] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in Proc. 14th ACM Conf. CCS, 2007, pp. 456–465.

[12] R.Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proc. 14th ACM Conf. CCS, 2007, pp. 195–203.

[13] 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. CCS, 2006, pp. 89–98.

[14] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494. Heidelberg, Germany: Springer-Verlag, 2005, pp. 457–473.

[15] D. Boneh and X. Boyen. “Secure identity based encryption without random oracles”. In CRYPTO, pages 443-459, 2004.

[16] D. Boneh and X. Boyen. “Efficient selective-id secure identity based encryption without random oracles”. In EUROCRYPT, pages 223 - 238, 2004.

[17] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In CRYPTO, pages213–229, 2001

[18] Boldyreva,Vipul Goyal, ―Identity- based Encryption with Efficient Revocation‖,2008.

[19] Adi Shamir,‖Identity Based Cryptosystems and Signature schemes‖ Departments of applied mathematics, 1998.