Fuzzy Elliptic Curve Cryptography based Cipher Text Policy Attribute based Encryption for Cloud Security

Gurpreet Singh
Research Scholar, Dept. of CSE
IKGPTU, Kapurthala, Punjab
India
cs.thapar.gurpreet@gmail.com

Dr. Sushil Garg
Professor, Dept. of CSE
RIMT, Mandi Gobindgarh, Punjab
India
sushilgarg70@gmail.com

***Abstract*—Cipher Text Policy Attribute Based Encryption which is a form of Public Key Encryption has become a renowned approach as a Data access control scheme for data security and confidentiality. It not only provides the flexibility and scalability in the access control mechanisms but also enhances security by fuzzy fined-grained access control. However, schemes are there which for more security increases the key size which ultimately leads to high encryption and decryption time. Also, there is no provision for handling the middle man attacks during data transfer. In this paper, a light-weight and more scalable encryption mechanism is provided which not only uses fewer re- sources for encoding and decoding but also improves the security along with faster encryption and decryption time. Moreover, this scheme provides an efficient key sharing mechanism for providing secure transfer to avoid any man-in-the-middle attacks. Also, due to fuzzy policies inclusion, chances are there to get approximation of user attributes available which makes the process fast and reliable and improves the performance of legitimate users.**

***Keywords*—Cipher text Policy Attribute based Encryption, Elliptic Curve Cryptography, Diffie Hellman, Fuzzy, Attribute Authority**

I. Introduction

Due to globalization and growth of network, there has been a lot of trend of online data sharing. Everybody wants to celebrate their success and their emotions with their friends. So, people are using various social networking applications like Facebook, Twitter, Instagram and so on . [1] [2]. People every day are generating huge data and cloud is the most promising application platform for solving the problem of huge data storage. These days almost everyone is using cloud for data storage as it provides various features in terms of scalability, on demand provisioning, elasticity and pay as per use. But security is one field which always concerns the users while taking cloud services.

To protect the credential data, various techniques have been used and still research is going on. Encryption has been one technique which is used by almost everyone where the message is transferred into unreadable form using a key so that only the person with key can decrypt it. Similarly, Access Control mechanisms [3] [4] are used in which it prevents the unauthorized access in shared data. Recently, Attribute based Encryption techniques are also being used which provides confidentiality, are one to many and efficient access control schemes[5]- [6].

Cipher text policy attribute based encryption has become the most important encryption mechanism these days where plain text is converted into ciphertext using set of various attributes and unique access policy. [7][8] Cipher text constitutes access policy and users secret keys consist of attributes. When any user has to decrypt the message, they need to satisfy the access policy with their attributes. There are mainly two types of CP-ABE. One is Single Authority where a single authority manages all the attribute set and second is Multi Authority in which multiple authorities handle the user attributes and attributes are from multiple different domains. For example, in an E-learning system, owner may encrypt the data with the access policy “Student and Researcher” where the attribute “student” is issued by Study Organization Authority and the attribute “Researcher” is issued by Research Organization Authority.

II. Related Work

In 2005, first Attribute based Encryption [5] scheme was proposed and after that research has been done for making the technique expressive and flexible[7]. Ist CP-ABE scheme [7] came into existence in 2007 with single authority. Later many researchers proposed multi authority CP-ABE schemes [9] [10] but they raised some questions in terms of high communication costs and stability degradation. Then, various techniques were proposed in multi authority CP-ABE but they used central Global authority[11] but they were lacking in performance. The solution came in Decentralized Multi Authority CP-ABE [12] but in this scheme, user revocation was ignored. Then various centralized and decentralized Multi authority CP-ABE scheme with user revocation came but they were on higher side in computational costs and communication overhead[13]. Phuong et al. [23] in his scheme suggested that security can be enhanced with only ‘AND’ access policy for encrypting the message and after that hide the policy too. But his scheme didn’t mention anything about user revocation as he used Single Authority. Yang et al. proposed in his scheme as ‘LSSS- Linear Secret Sharing Scheme’ matrix based access scheme with Multiple Authority and also added user revocation problem. Ruj et al. [22] also suggested and proposed LSSS matrix based access scheme with added User Revocation and Multiple Authorities for user attributes.

III. Proposed model

Here, in this paper, the detailed Fuzzy Elliptic Curve Cryptography based Diffy Hellman Cipher text Policy Attribute based Encryption(F-ECCDH-CP-ABE) scheme

978-1-7281-4097-1/20/$31.00 ©2020 IEEE

has been proposed to improve the data confidentiality and computational complexity. In addition, some brief details about the scheme are provided. In this model, basic four entities are there which are used for data confidentiality and secure transmission. These are Cloud Storage Server, N Attribute authorities, data owner and users.

1. **Data owner**: data owner is responsible for encrypting the data using the access policy and transfer it on the cloud.

2. **Attribute Authorities**: Each attribute authority manages their set of attributes and generate the secret key for each user.

3. **Cloud Storage Server(CSS):** Here the message after encryption is stored and it provides access to various users on the basis of access policy.

4. **Data Users**: Those who will satisfy the access policy with their private keys can decrypt the message and other users can't.

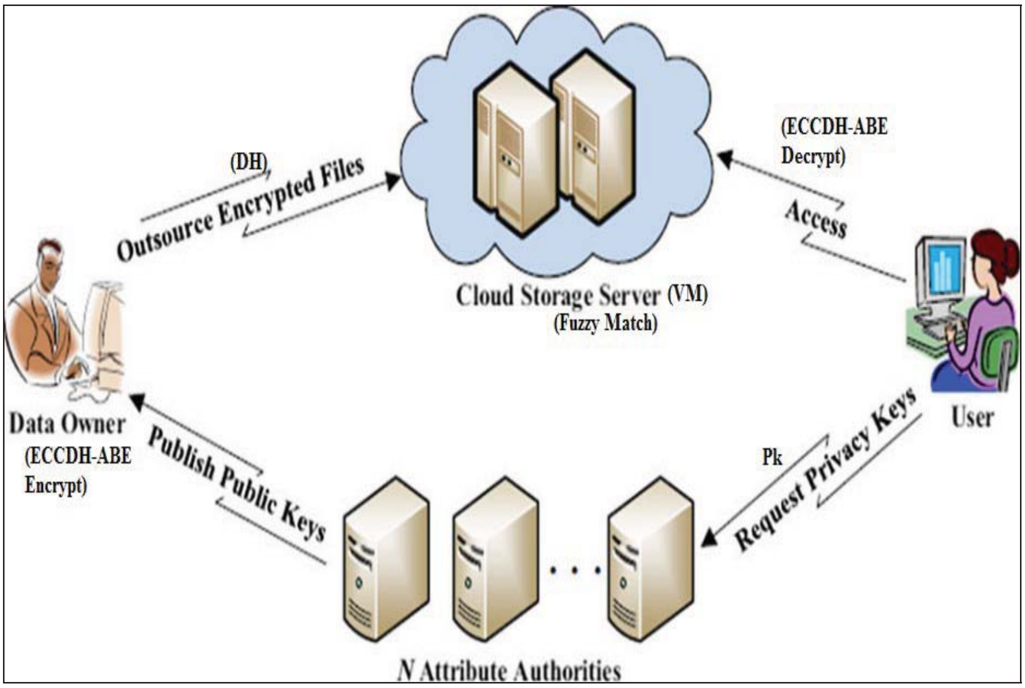

Figure1: Proposed model for secure data transfer using Fuzzy ECC-DH CP-ABE

Along with, these basic entities, some unique techniques are added which makes this model a novel approach.

Elliptic Curve Cryptography(ECC) : For cloud users, when the data is shared over the cloud, the Elliptic Curve Cryptography(ECC) is much more scalable as ECC can work with fewer resources with faster encryption and de cryption time without sacrificing security using fewer bits to encode and decode the data. For example, ECC at 56-64 bits has comparable security of 128 bit SHA-1 at lower computational complexity. Also, in ECC, we can design our own encryption mechanism which makes it even harder to interpret, for example, standard algorithms such as MD5, AES, DES, SHA etc have predefined set of set used by everyone so if there is a breach or collision attack is available, then every data encrypted using such algorithms is rendered unsafe. Thus, a new encryption method based on custom Elliptic Curves has been proposed, away from standard to add security layer. Also, the ECC will use lesser bits for lower computational complexity without sacrificing any security. Various Attributes of client will be used to generate a key using custom Fuzzy membership mechanism.

Advantages of ECC when compared with other cryptography techniques.

1) ECC employs a relatively short encryption key
2) One another advantages of ECC is that it has significantly lower size of the encrypted message (overhead).
3) Furthermore, ECC algorithm is more complex and needs custom elliptic curves implement than standard algorithms, which reduces the likelihood of collision attacks, thus increasing the security of the algorithm.

ECC-DH (diffie hellman key exchange): As most security breaches are orchestrated using middle man attacks, it seem viable to use some sort of efficient key sharing mechanism over a secure channel. The diffie hellman key exchange provides the state of the art solution for same.

Fuzzy: To get approximation of Attribute available at the client (as client may or may not have sufficient Attributes for validation).

IV. Proposed Methodology

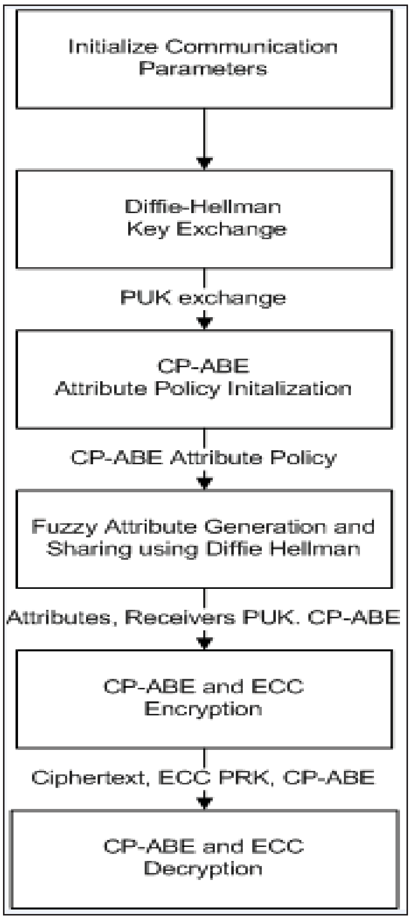
Initialize Communication Parameters
Diffie-Hellman Key Exchange
PUK exchange
CP-ABE Attribute Policy Initalization
CP-ABE Attribute Policy
Fuzzy Attribute Generation and Sharing using Diffie Hellman
Attributes, Receivers PUK. CP-ABE
CP-ABE and ECC Encryption
Ciphertext, ECC PRK, CP-ABE
CP-ABE and ECC Decryption

Figure2: Proposed Flowchart

In the proposed system, following entities are involved:

1) Cloud Service Provider: CSP as Authority multiple authorities can be presented at any given time.
2) Sender: The Sender of the secure message requested by the receiver
3) Receiver: Recipient/requestor of the secure message.

Step 1: **Generation of the public key, master key and agreement of CP-ABE policy**

First, before communication we need to setup CP-ABE policy. The CP-ABE policy dictates who can access the encrypted information. CP-ABE can be in the form of a matrix or as a logical function. For CSP to generate a key it needs the attributes of the users or the parties evolved in communication. At any given time a user may have some of its attributes present. However in existing ABE schemes according to policy all validating attributes must be present at the time of decryption. This condition, however, cannot be fulfilled by all participants every single time. Unavailability of some attributes reduces ABE performance for legitimate entities. To solve this problem the proposed scheme will be using Fuzzy-ABE policy. So, using available attributes of the entities the CSP constructs a policy dictating, who can access the messages sent by the sender.

Step 2: The CSP generates a secret key based on the users attributes using Fuzzy Policy

For the given attributes of entity's identity, the key generation algorithm generates a private key which is derived using the fuzzy logic function utilizing entity's attributes. If the receiving entity is able to "have" at least some attributes alongside it's private key, then the receiver can perform decryption of the encrypted message.

Step 3: Encryption

The Sender encrypts the message according to the agreed upon access policy and sends over the secure communication channel (deffie-hellman).

Step 4: Communication

Upon receiving the encrypted message the receiver validates its available attributes with CSP.

Step 5: Policy Validation

The CSP Checks if the receiver has sufficient access rights using Fuzzy-ABE policy constructed from cipher text and calculating fuzzy memberships using receivers attributes, if the receiver matches the policy requirements, the CSP sends decryption key to receiver using previously established secure channel.

Step 6: Decryption

Receiver can decrypt the ciphertext successfully only if its attributes satisfy the corresponding access policy.

V. Conclusion

In this paper, Fuzzy Attribute based Encryption policy has been proposed by which performance can be improved of ABE scheme by using available attributes for decryption and thus further improves the reliability. Secondly, after encryption using agreed access policy, the cipher text will be sent through secure channel using Diffie Hellman Key Exchange algorithm. Thirdly, using Elliptic Curve Cryptography, computational complexity can be lowered without sacrificing the security. Also ECC algorithm is more complex and hard to interpret, thus increasing the security of the system.

Future works can be done in this direction by the introduction of new light weight encryption and decryption schemes for reducing the computational complexity over the Cloud and IoT-based applications.

References

[1] C. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," *IEEE Pervasive Computing*, vol. 12, no. 4, pp. 50–57, October-December 2013.

[2] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. K. Liu, "TIMER: secure and reliable cloud storage against data re-outsourcing," *Proceedings of the 10th International Conference on Information Security Practice and Experience*, vol. 8434, pp. 346–358, May 2014.

[3] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "ktimes attribute-based anonymous access control for cloud computing," *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2595–2608, September 2015.

[4] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for web-based cloud computing services," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, pp. 484–497, March 2016.

[5] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” *Advances in Cryptology–EUROCRYPT*, pp. 457–473, May 2005.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98, October 2006.

[7] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, “Efficient attribute-based encryption from R-LWE,” *Chinese Journal of Electronics*, vol. 23, no. 4, pp. 778–782, October 2014.

[8] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” *IEEE Symposium on Security and Privacy*, pp. 321– 334, May 2007.

[9] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 456–465, October 2007.

[10] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Mediated ciphertext-policy attribute-based encryption and its application,” *Information Security Applications*, pp. 309–323, August 2009.

[11] X. Xie, H. Ma, J. Li, and X. Chen, “An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing,” *Journal of Universal Computer Science*, vol. 19, no. 16, pp. 2349–2367, October 2013.

[12] F. Guo, Y. Mu, W. Susilo, D. S. Wong, and V. Varadharajan, “CP-ABE with constant-size keys for lightweight devices,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 763–771, May 2014.

[13] A. Balu and K. Kuppusamy, “An expressive and provably secure ciphertext-policy attribute-based encryption,” *Information Sciences*, vol. 276, pp. 354–362, August 2014.

[14] X. Liu, J. Ma, J. Xiong, and G. Liu, “Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data,” *International Journal of Network Security*, vol. 16, no. 6, pp. 437–443, July 2014.

[15] Y. Chen, Z. L. Jiang, S. Yiu, J. K. Liu, M. H. Au, and X. Wang, “Fully secure ciphertext-policy attribute based encryption with security mediator,” *Proceedings of the 16th International Conference on Information and Communications Security*, vol. 8958, pp. 274–289, December 2014.

[16] Y. Yang, J. K. Liu, K. Liang, K. R. Choo, and J. Zhou, “Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data,” *Computer Security in ESORICS 2015*, vol. 9327, pp. 146–166, September 2015.

[17] J. Liu, X. Huang, and J. K. Liu, “Secure sharing of personal health records in cloud computing,” *Future Generation Computer Systems*, vol. 52, no. C, pp. 67–76, November 2015.

[18] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, “A secure and efficient ciphertext-policy attributebased proxy re-encryption for cloud data sharing,” *Future Generation Computer Systems*, vol. 52, no. C, pp. 95–108, November 2015.

[19] Jung T, Li XY, Wan Z, Wan M (2013) Privacy preserving cloud dataaccess with multi-authorities. In: Proceedings of the IEEE INFOCOM 2013, IEEE, pp 2625–2633.

[20] Müller S, Katzenbeisser S, Eckert C (2008) Distributed attribute-based encryption. In: Information security and cryptology–ICISC 2008, Springer, NewYork, pp 20–36.

[21] Lewko A, Waters B (2011) Decentralizing attribute-based encryption. In: Advances in cryptology–EUROCRYPT 2011, Springer, NewYork, pp 568–588.

[22] Ruj S, Stojmenovic M, Nayak A (2014) Decentralized access control with anonymous authentication of data stored in clouds. IEEE Trans Parallel Distrib Syst 25(2):384–394.

[23] Phuong TVX, Yang G, Susilo W (2016) Hidden ciphertext policy attribute-based encryption under standard assumptions. IEEE Trans Inf Forensics Secur 11(1):35–45.

[24] Yang K, Jia X (2014b) Expressive, efficient, and revocable data access control for multi-authority cloud storage. IEEE Trans Parallel Distrib Syst 25(7):1735–1744.