Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.689 – 694

RESEARCH ARTICLE

Secure System Implementation using Attribute Based Encryption

Apurva Gomase[1], Prof. Vikrant Chole[2]

[1]Department of Computer Science and Engineering, GHRAET, Nagpur, India

[2]Department of Computer Science and Engineering, GHRAET, Nagpur, India

[1] apurva.a.gomase@gmail.com; [2] Vikrantchole@gmail.com

Abstract: ***Today there is an demand of distributed data security in data sharing system such as social network or cloud computing challenging issue in data sharing system is access policy and support of policy update. The cryptographic solution to this issue is Cipher text policy Attribute based encryption. In Which data owner defines their access policy over user attribute and applies this policy on data. The problem introduce the Scheme is called as key escrow problem, in which key generation center decrypt any message which addressed to the User by generating there private key. these approach is not suitable for data sharing scenario, also it introduce the another challenge called revocation. Data accessible to only authorized user. The proposed CP-ABE scheme is used to solve the key escrow problem by 2pc protocol between generation center and data storing center. Proposed work consists of also immediate user Revocation.***

Keywords: Attribute based encryption, Key Escrow, Access Structure, Revocation

I. INTRODUCTION

There is recent development of the network and computing technology enables many people to easily share their data with others using online external storages. People can share their Private data as well as personal data by using online social networks such as Facebook and MySpace; or upload highly sensitive personal health records (PHRs) into online data servers. As people enjoy the advantages of these new technologies and services, What about data security and access control, concern is arises about those things. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. Data only accessible to the authorized user whether it is private or personal data.

Most promising cryptographic approach is Attribute-based encryption (ABE) is a achieves a fine-grained data access control. It provides away of defining access policies based on different attributes of the requester, environment, or the data

object. The(CP-ABE) scheme i.e cipher text policy attribute-based encryption enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the cipher text, and enforce it on the contents.

II. RELATED WORK

Apurva gomase etal[1]In these paper we studies the different ABE schemes also studies there problem we give the comparison between them**.** Shamir[3] proposed IBE schemes in 1998 and practical implementation is done in 2001 These schemes replace public key infrastructure Amit sahai etal[4] Fuzzy Identity-Based Encryption in which identity of a user is viewed as a set of attributes. In these schemes with the help of set of attributes private key is associated. if the decryptor want to decrypt the data if the certain no of attributes are overlap with the set which is define by encryptor. Vipul goyal,etal [5] (Key policy –attribute based encryption in these policy encryptor has no control who can access the data .encryptor defines the set of attributes. Most of the scheme [4][6] based on single trusted authority or KGC has power to generate user private key by using their master key.ie KGC has power to generate hole secret key of specific user These create escrow problem. M. Chase etal [7]These paper focused on Distributed KP-ABE schemes to solve the escrow problem in Multiauthotity System. Disadvantage of these approach is Performance degradation. There is result of O(N^2) communication overhead.

III. PROPOSED WORK

In Proposed work basically consists First process will Registration process after that there will Authentication process. then user(act as data owner) want to upload the data for that user will specify first credential (attributes) after that it will get the key from Kgc and data storing center and Re-encrypt the data with these key and store the data to the data storing center. after when the user want to access the data. will authenticates by KGC (basically satisfy the Credential) after that the 2pc protocol will perform between KGC and data storing center after that user get two key component with help that user get the decrypted file.

- Registration and Authentication: These process Perform for Registering the user in the System and to check whether the user is Valid user or not.
- Credential: if the user want to upload the data user will specify the credential of those user, for who user will share the data. and when the user want to access the data firstly its authenticate by Kgc(user will satisfy the attribute)
- Data storing Center: After performing the encryption store the data to the data storing center.

A. Escrow Problem:

In proposed work we work on Escrow problem[2] the escrow problem. The problem basically is that most of the ABE schemes base upon single trusted authority or KGC has power to generate private(secrete)key of user with master secret information these problem is solve by 2pc protocol perform between the Kgc and data storing center.kgc will generates the key and data storing center also generates the key by using both key will re-encrypt the data.frist is encrypted by the key will generated by data storing center again the data encrypted by the key generated by kgc. With the help of that these problem will solve.

*B. Grid Based authentication***:**

proposed work also consist of grid based authentication these technique is used for strong authentication. These grid card is consists of series gird character along with numeric number. Randomly three character will set which is present on that card.

C. Double Authentication layer:

In proposed work consists of double authentication system .Kgc perform the authentication. Also we will add the datastoring center also perform the authentication process.

D. Revocation:

Proposed work also consists User Revocation. with immediate user revocation enhances forward and backward secrecy also revoke the user manually if user found. revocation by setting expiration time. If user last access time is more than set time of the system then user revoked automatically from the system. In our proposed work we also revoke the user Manually if the user done any unauthorized activity in system then user revoke from the system by admin panel.

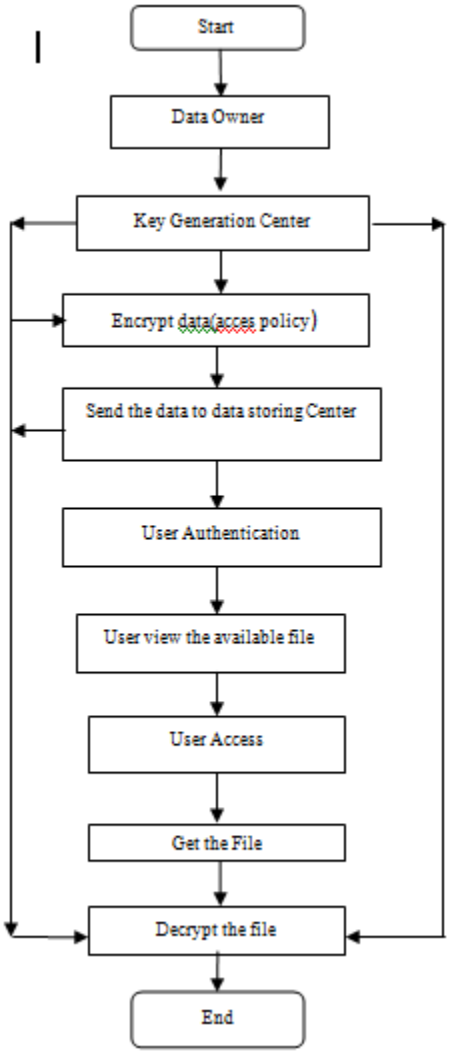
IV. ALGORITHM

A. Ciphertext policy attribute-based encryption(CP-ABE) :

Attribute-based encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control It provides a way of defining access policies based on different attributes of the requester, environment, or the data object. cipher text policy attribute-based encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the ciphertext, and enforce it on the contents [5].
Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access.

B. Encryption algorithm:

AES: The Advanced Encryption Standard (AES),also referenced as Rijndael and is also called as symmetric key algorithm. Its Block cipher and block length is 128 bit.
AES consists of different key sizes 128 bit,192bit and 256 bit in Symmetric algorithm depend upon key length larger key sizes encryption also stronger. Encryption consists of 10 round of processing for 128bit key size 12 round for 192 bit key size 14 round for 256 key size.

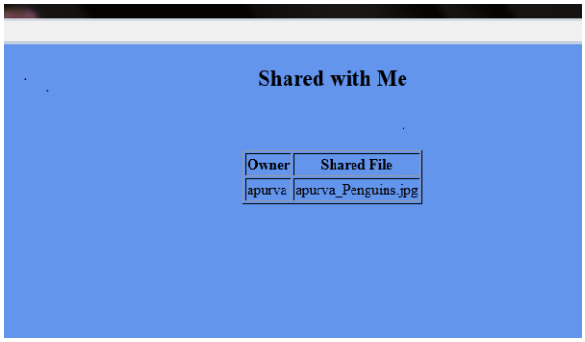


Fig(1): System Flow diagram

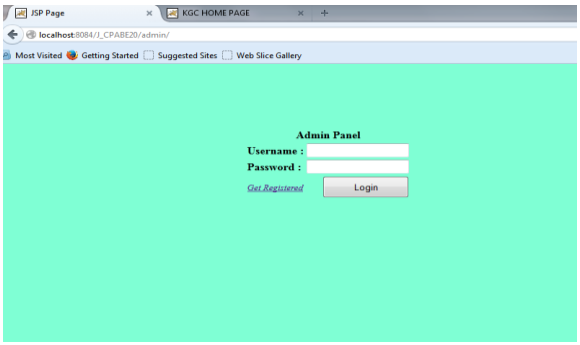
V. RESULTS AND DISCUSSION

Given fig show the some output window fig(2) show the output window of credential fig(3) output window of file sharing fig(4) output window of Revocation.

Fig(2):Result Show Credential



Fig(3): Result show which file is share



Fig(4): Result Revocation window

VI. COMPARATIVE ANALYSIS

We are providing some information on the performance evaluation of proposed work, and compare it with CP-ABE. The graph represent encryption and decryption time of proposed system and existing system and the time given in seconds

CONCLUSION

To achieves more secure and fine-grained data access control in the data sharing system. In proposed work we perform re-encryption in which the data is encrypt twice. so scheme is efficient and scalable to securely manage user data in the data sharing system user ensures about the data storage in external data storing center. Data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials. immediate user revocation Result to manage the system efficiently from unauthorized user.

REFERENCES

[1] Apurva Gomase, Vikrant Chole "Review On Secure System Implementation Using Attribute Based Encryption"in International journal of Computer Science and Mobile Computing ISSN 2320-088X,Volume 3,Issue.11,November 2014,Page No 465-468

[2] Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL:25 NO:10 2013

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

[4] Amit Sahai and Brent Waters, "Fuzzy Identity-Based Encryption," Proc.Int'l Conf. Theory and Applications of Cryptographic Techniques(Eurocrypt '05), pp. 457-473, 2005.

[5] vipul goyal,omkant pandey amit sahai and brent Waters, "Attribute Based encryption for fine grained acess control of encrypted data" Proc. ACM Conf. Computer and Comm. Security,2006

[6]John bethencourt , Amit sahai, brent Waters, "Cipher textpolicy attribute based encryption" Proc. IEEE Symp. Security and Privacy,pp321-334,2007

[7]M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.

[8] Nayani Sateesh "An Approach For Grid Based Authentication Mechanism To Counter Cyber Frauds With Reference To Credit Card Payments, " Global Journal of Computer Science and Technology, Volume 11 Issue 1 Version 1.0 February 2011.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

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

[11] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryptionwith Non-Monotonic Access Structures," Proc. ACM Conf.Computer and Comm. Security, pp. 195-203, 2007.

[12] Vaibhav Satane, Arindam Dasgupta, " Advancement in Security and Efficiency For attribute based data sharing ", International Journal of Science and Research (IJSR),year 2012

[13] Ritika Chehal, Kuldeep Singh "Efficiency and Security of Data with Symmetric Encryption Algorithms " International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 8, August 2012.

[14] M. Pratheepa, R. Bharathi "Improving Security and Efficiency in Attribute Based Data Sharing," International Journal of Science and Research Volume 3 Issue 1, January 2014

