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. 3, Issue. 11, November 2014, pg.465 – 468

REVIEW ARTICLE

A Review on 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-In Data sharing such as social network or cloud computing there is an demand for data security. Challenging issue in data sharing system is access policy and support of policy update. The policy attribute based encryption (CP-ABE) is cryptographic solution to this issue. The data owner defines their own access policy over user attribute and applies this policy on data. These scheme introduce the problem is called as key escrow problem, in which key generation center decrypt any message which addressed to the User by generating there private key. Data accessible to only authorized user. Also it introduces another challenge regard to user revocation. In this research work the proposed novel CP-ABE scheme is used to solve the key escrow problem by escrow free key issuing protocol generated by using two party computations. Fine-grained user revocation per each attribute could be done by proxy encryption.

Keywords: Attribute based encryption, cipher text policy, Revocation

I. Introduction

The development of the network and computing technology enables many people to easily share their data with others uses online external storage. using online social networks such as Facebook and MySpace People can share their lives with friends by uploading their private photos or messages or upload highly sensitive personal health records (PHRs) into online data servers. Thus the people enjoy the advantages of these new technologies and services, concerns about data security and access control also arise. Use of the data should be improper by the storage server or unauthorized access by outside users could be threats to their data.

People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Attribute-based encryption (ABE) is a promising cryptographic approach that 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 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 cipher text, enforce it on the contents. it allowed to decrypt different pieces of data per the security policy to each user with a different set of attributes. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access, which is the traditional access control approach of such as the reference monitor**.**

II. Existing Work

Junbeom Hur [1] these paper focused on Novel CP-ABE policy(cipher text policy attribute based encryption)In which the escrow problem solves by using escrow key free issuing protocol .It generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data-storing center with their own master secrets. none of them could generate the whole set of user keys alone.

Thus they cannot fully trusted on key generation center and data storing center so provide protection the data to be shared. Data confidentiality and privacy can be cryptographically enforced against any curious KGC or data- storing center in the proposed scheme. Immediate user revocation can be resolved by using proxy Re-encryption.it enhances forward and backward secrecy of data.

III. Related Work

A. Identity-Based Encryption

Shamir[3] proposed IBE schemes in 1998 and practical implementation is done in 2001 These schemes replace public key infrastructure .The data owner (sender) does not lookup for the public key certificate of receiver.

B. Fuzzy Identity-Based Encryption

In fuzzy IBE [4] identity of a user is viewed as a set of attributes. In these schemes private key associated with set of attributes. If the decryptor want to decrypt the data if the certain no of attributes are overlap with the set which is define by encryptor. There are two main application of FIBE 1) it uses the biometric identities 2) error-tolerance property. It also provides the Security against the collision .which is useful in attribute-based encryption.

C. Richer type of Attribute based encryption

In these schemes i.e KP-ABE Vipul goyal,etal [2] (Key policy –attribute based encryption)in these policy encryptor has no control who can access the data .encryptor defines the set of attributes. In John Bethencourt, etal[10] CP-ABE in which private key is associated by set of attributes. Data owner which encrypt the message they specify the access structure so only authorized user Able to decrypt the cipher text.

D. Access structure

R. Ostrovsky[6] Attribute based encryption with non monotonic access structure in which they define that access structure are present with any access formula(non-monotonic).previous ABE schemes limited to monotonic ones.

E. Escrow Problem

Most of the scheme [4][10] based on single trusted authority or KGC has power to generate user private key by using there master key.ie KGC has power to generate hole secret key of specific user These create escrow problem.

F. Improving Privacy and Security in Multi-Authority Attribute based Encryption

These paper[5] focused on Distributed KP-ABE schemes to solve the escrow problem in Multi authority System. Disadvantage of these approach is Performance degradation. There is result of O(N^2) communication overhead.

G. Improving security and efficiency in attribute based data sharing

junbeom Hur[1] proposed novel-CPABE in which instead of building new schemes from scratch the makes some changes the key issuing protocol to solve these escrow problem in which when the user private key is generated by using 2PC protocol. means user key generated when there Is communication take place between data storing center and key generation center. after that the use key is generated.

IV. Methodology

In these section we describing different components of architecture

- Key Generation center: In key generation center can generate the public and secret parameter for CP-ABE
- Data storing Center: Data storing center another authority to generate the private key of user and its also providing data sharing services.
- Data owner: client who wishes to upload the data in external storage. it is also responsible for defining attribute based access policy over the data to be distributed.
- User: if the user possess valid set of attribute and satisfy the policy of encrypted data then user is allowed to access the data

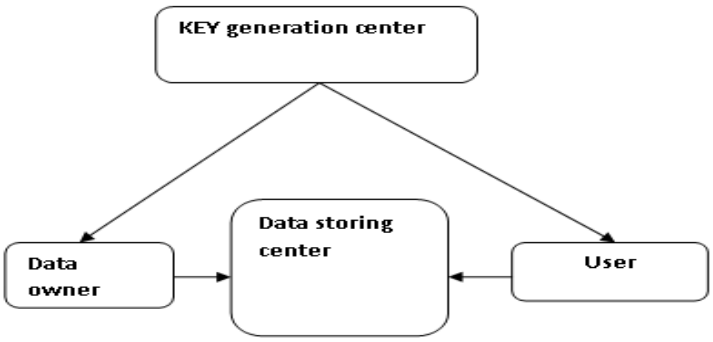

Fig1: Architecture of data sharing system

Evaluation and Discussion

TABLE I

Sr No	Studies	Approach	Limitation
1	Shamir	IBE	These scheme ideal for closed group of user
2	shahani	FIBE	Escrow problem
3	Vipul goyal	KP-ABE	Encrypt or has no control who can access the data

I. 4	John Bethencourt	CP-ABE	Escrow problem
II. 5	Chase and chow	Multi authority ABE	Performance degradation

V. Conclusion

Literature survey is done based on existing Attribute based encryption schemes and their implementation which gives an idea that there are still limitations in existing system also these approaches gives idea about more scope in encryption techniques.

References

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

[2] 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

[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] 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.

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

[7] D. Boneh and M.K Franklin, ―*Identity-based encryption from the weil pairing*‖. CRYPTO, pages 213–229, 2001.

[8] Shucheng, Yu, Cong Wang, Kui, R., and Wenjing, Lou: ―*Attribute based data Sharing with attribute revocation*‖. ASIACCS10. (2010).

[9] J. Bethencourt, Amit Sahai, and Brent Waters, "*Ciphertext-PolicyAttribute-Based Encryption*," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007

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

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

