Secure Data Sharing

Shubhangi Bhalerao[1] Parth Joshi[2] Mahipal Singh[3] Husain Garbadawala[4] Neha Parmar[5]
[1,2,3,4]B. Tech Student [5]Assistant Professor
[1,2,3,4,5]Department of Computer Science & Engineering
[1,2,3,4,5]Parul University, Waghodia Road, Limda, India

Abstract— In various distributed systems a user should only be able to access information if a user possess a certain set of credentials or attributes. Recently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the information is compromised, then the confidentiality of the data will be compromised. In the paper we present a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption (CP-ABE). The user key of encrypted data and make policies were used to describe previous Attribute Based Encryption systems; while in our system these characteristics are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt the data. In addition, we provide an implementation of our system and give better performance measurements.
Keywords: Secure Data Sharing, CP-ABE, ABE

I. INTRODUCTION

Attribute-based encryption (ABE) was proposed by Amit Sahai and Brent Waters. It is a relatively recent approach that reconsiders the concept of public-key cryptography. The ABE was proposed to solve the complex access control mechanism over encrypted data. Basically, ABE is public key based on one to many encryption that decrypt the cipher-text only if private key associated with the user matches with public key and master secret key. The decryption of data takes place directly by the server itself. Thus the performance is increased. In the ABE the cipher-text and key both are dependent on the attributes. The key issue is that someone should only be able to decrypt a cipher-text if the person holds a key for "matching attributes" where user keys are always issued by some trusted party.

II. LITERATURE REVIEW

To get the greater understanding and knowledge about image recognition and augmented reality we have read several papers. We list some of the papers below with briefly.

In [1], we studied about attribute based encryption. Attribute-based encryption (ABE) is proposed by Amit Sahai and Brent Waters. It is a relatively recent approach that reconsiders the concept of public-key cryptography. The ABE is proposed to solve the complex access control mechanism over encrypted data. Basically, ABE is public key based on one to many encryption that decrypt the cipher-text only if private key associated with the user matches with public key and master secret key. The decryption of data takes place directly by the server itself. Thus the performance is increased.[1] In the ABE the cipher-text and key both are dependent on the attributes. The key issue is that someone should only be able to decrypt a cipher-text if the person holds a key for "matching attributes" where user keys are always issued by some trusted party.

In [2], The key policy ABE was proposed by goyal et al.[2] In Key-policy attribute based encryption private key is assigned to access policy and cipher-text is associated with set of attributes. Decryption of data is possible only when an attribute satisfies the policy.
Key policy attribute based encryption has four algorithms Setup, Encryption, Key Generation and Decryption. The major limitation of KP-ABE is the Access structure granted full access to the users.[5]

In [3], The CP-ABE was proposed by Brent waters. In cipher-text-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a cipher-text specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a cipher-text, if and only if his attributes satisfy the policy of the respective cipher-text. Policies may be defined over attributes using conjunctions, disjunctions and (k,)-threshold gates, i.e., k out of n attributes have to be present.

In [4], Fuzzy Identity Based Encryption was proposed by Adi Shamir and Brent Waters in 2005. In Fuzzy IBE, identity view as set of descriptive attributes, provide authentication using biometric techniques and encryption based on biometric identity.The error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently Will have some noise each time they are sampled.Users with an assigned a set of attributes which combines their "identity", w, may decrypt a given cipher-text encrypted with the public key w' only if w and w' are within a certain distance from each other in a set threshold.

In [5], Melissa Chase has proposed the ABE scheme for multiple authorities. In this scheme allow any polynomial number of independent authorities to monitor attributes and distribute secret keys. The encryptor the owner can choose, for each authority a number dk and a set of attributes. Then encrypt a message such that a user can only decrypt if at least dk of the given attributes from each authority k. The Author has also provide the idea about the single authority and multi authority.

Sr No.	Title	Journals	Approaches & Algorithms	Summary
1	A Survey on Attribute Based Encryption	International Journal of Advanced Research in Computer and Communication Engineering.	Various attribute based encryption techniques	The paper contains various attribute based encryption techniques to be used in cloud computing such as ABE, CP-ABE, and KP-ABE.

		[7]		
2	Key Policy Attribute Based Encryption (KP-ABE): A Review	Research Scholar, Department of C.E. School of Engineering R.K University, Rajkot .[2]	Key Policy Attribute Based Encryption (KP-ABE	Key policy attribute based encryption has four algorithms Setup, Encryption, Key Generation and Decryption. The major limitation of KP-ABE is the Access structure granted full access to the users
3	Cipher-text-Policy Attribute-Based Encryption	UCLA John Bethencourt, Carnegie Mellon University.[3]	CP-ABE	In cipher-text-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a cipher-text specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a cipher-text, if and only if his attributes satisfy the policy of the respective cipher-text.
4	fuzzy identity based encryption	International association of cryptologic research.[4]	fuzzy ibe	In Fuzzy IBE, identity view as set of descriptive attributes, provide authentication using biometric techniques and encryption based on biometric identity.[3]
5	Multi-authority Attribute Based Encryption.	Chase Melissa. "Multi-authority attribute based encryption." Springer Berlin Heidelberg, 2007.[6]	Multi-authority Attribute Based Encryption.	In [6] Melissa Chase has proposed the ABE scheme for multiple authorities. In this scheme allow any polynomial number of independent authorities to monitor attributes and distribute secret keys.

Table 1:

III. CONCLUSION

In this paper, we tried to report various techniques for data security. We get to know various methods for encryption. We get to know how to use multi authority for better results. How to resist single point of failure and work on collusion attacks. These techniques will be very useful.

REFERENCES

[1] Kumar N. Saravana, GV Rajya Lakshmi and B. Balamurugan. "Enhanced Attribute Based Encryption for Cloud Computing." Procedia Computer Science 46 (2015).
[2] Bethencourt John, Amit Sahai and Brent Waters. "Cipher-text-policy attribute-based Encryption." IEEE Symposium on Security and Privacy (SP'07), IEEE, 2007.
[3] Attribute Based Encryption, Available from: http://crypto.stackexchange.com/questions/17893/what-is-attribute-based-encryption
[4] Sahai Amit and Brent Waters. "Fuzzy identity-based encryption." Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005.
[5] Lai Junzuo et al. "Fully secure key-policy attribute-based encryption with constant-size cipher-texts and fast decryption." Proceedings of the 9th ACM symposium on Information, computer and communications security. ACM, 2014.
[6] Chase Melissa. "Multi-authority attribute based encryption." Theory of cryptography. Springer Berlin Heidelberg, 2007. 515-534.
[7] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 9, September 2014)

