ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Survey on Attributes Based Encryption

Dhanshri A. Nevase [1], Prachi P. Rayate [2]

Assistant Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, Warje, Pune, India[1]

Assistant Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, Warje, Pune, India[2]

ABSTRACT: Encryption protects the data from unauthorized access or from unauthorized attacker. Different techniques are used for securing the data. Attribute based encryption (ABE) is one of the most powerful technique used for encryption of data. Attribute based encryption is expanded version of encryption. The data is accessed only when it satisfy some policy that are defined in mathematically. In this scheme data is not encrypted only for single user. But multiple users can decrypt that data that satisfy given attribute based policy. Attribute is used as public key to encrypt the data and also used to control the access of data. The key policy and cipher text policy are the types of access policy. In this paper, we survey on different techniques used for attribute based encryption scheme and its disadvantages.
.

KEYWORDS: Encryption, Attribute based encryption, Key policy, cipher text policy.

I. INTRODUCTION

In today's life user data is private and user wants to secure its data from unwanted access. Encryption techniques are used to protect user data. The simple technique used to protect the data is public key encryption. In this scheme plaintext is encrypted using key. This key is shared between users. The receiver of that plaintext use same key to decrypt the data. But this scheme has some disadvantage as require more preparation time. It is difficult to use traditional public key encryption for complex access control because access control policy defined using attributes such as size, place etc. Most existing public key encryption methods permit a particular user to encrypt data, but unable to access control of encrypted data.

Now a day, the complexity and need of access control is rapidly growing to obtained data. Encryption is as long as use to privilege the secure data with the help of security policies. In attribute based encryption, collection of attributes relationship known as descriptive attribute. These attributes are used to indentify generate secret key and access control gives structure of control as well as how to interact user and system with other. This technique is used to encrypt file in respect of access policy to calculate set of attributes. By using attribute based encryption it can put data privacy, aware of involving great attention and non requiring access control. An attribute-based Encryption (ABE) scheme has two techniques for encryption to access controls as Key Policy Attribute based encryption (KP-ABE) and Cipher-text Policy Attribute Based Encryption (CP-ABE).

In Key Policy Attribute based encryption (KP-ABE), a cipher text is related with attributes set and a secrete key of user is related with an access structure. If the attributes related to the cipher text desires of access structure connected with secrete key can decrypt the cipher text by secrete key holder.

The Cipher-text Policy Attribute Based Encryption (CP-ABE) is opposite to KP-ABE, a cipher text is related with the access structure and the secrete key of user is related with a set of attributes. If the attributes related to secrete key desires of access structure connected with secrete key can decrypt the cipher text by secrete key holder.
The Cipher-text Attribute based encryption is used to control the access issues which is bring into use cryptographic solution. This technique is suitable for data encryption which comprise set of attributes that decryption needs to take control of cipher text in decrypt form. According to the security policy many people may enable different part for decryption.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

II. RELATED WORK

Attribute Based Encryption

Sanai and waters [1] first develop the technique for attribute based encryption in 2005. In this paper the data is encrypted and decrypted using user attributes. Attributes are described and creates a set of that attributes. The cipher text and secret key depends on the set of user attributes. The message can be decryption only when set of attributes are matched. The set of matches must be up to threshold value.

Disadvantage:-

Computation overhead is increases because every authorized user's public key used by data owner for encryption.

Identity Based Encryption

Shamir introduce identify based encryption in 1984 [2] . In this paper, sender and receiver communicate with each other securely. Signature are verified of each other without have knowledge of public or private key. The attributes and secret key depends on identity of user, for example biometric is unique identity of user.

Disadvantage:-

Some security issues are generated if trusted third party gets compromised. At that time security cannot be maintain using this technique.

Key Policy attribute based encryption (KP-ABE)

Goyal,et at [3] first introduce encryption technique which is based on key factor. Paper introduce encrypted data can be shared using fine grained method instead of coarse grained encrypted data. Set of attributes are used to generate the cipher text. The cipher text can be decrypted using access structure associated with private key.

Disadvantage:-

Not used for broadcasting application because the data owner has to trust the key issuer. Owner of data cannot decide who can decrypt the data.

Expressive Key Policy ABE (EKP-ABE)

In this technique even if storage server is not trusted the data which is encrypted is confidential [4]. In this method data owner determine who can decrypt that data. User credentials are described using attributes.

Disadvantage:-

Negative attributes are used which is not related to encrypted data so increase overhead.

Ciphertext Policy ABE (CP-ABE)

It is opposite of KP-ABR technique [5] . In this technique user's private key is depends on set of attributes and the encrypted text is associated with an access structure. If set of attributes of private key satisfies the access structure associated with encrypted text then user can decrypt the cipher text. Even if trusted third party is compromised this technique is more secure.

Disadvantage:-

It is not use for enterprise purposes. Attributes are logically a single set.

Multiple Authority ABE (MAABE)

K.Yang, X.Jia, K.Ren and B.Zhang [6] was proposed encryption techniques useful to access data using cipher text and secrete key for multi-authority and users for cloud storage system. They developed multiple number of attribute authorities and one central authority to decrypt the users attributed set. It required independent authorities to access the data so that data may corrupt or loss while distributing the secrete key.

Disadvantage:-

Multi-authority users can access the same set of attributes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

File Hierarchy Attribute Based Encryption (FH-ABE)

File Hierarchy Attribute Based Encryption uses file hierarchy based encryption methodology. Based on the layered access structure the files are encrypted. Both text content storage and time costs of encryption are saved[7]. It requires standard assumptions to proved this scheme.

Disadvantages:-

It is secure under standard assumption.

Ciphertext policy Weighted ABE (CPWABE)

Cipher text policy Weighted ABE (CPWABE) assigns weight to the attributes based on the preference defined in the access control structure. Clients will have allocate the load to their attributes. Based on the attributes the data owner will encrypt the data. The private key is based on weighted access structure and the decryption [8] is possible only when the cipher text and the weighted attribute matches with the weighted access structure.

Disadvantages:-

More computation is required.

III. CONCLUSION

Various attribute based encryption techniques (ABR) are summarized in this paper. Major concern of this paper is security. Time required for encryption and decryption to be reduced. Also cost of storing the cipher text to be reduced. FH-WABE performs better than the other attribute encryption techniques related to scalability, flexibility and fine grained access control.

REFERENCES

[1] A.Sahai and B.Waters, Fuzzy identity based encryption, in Proc. Advances in Cryptology – Eurocrypt, 2005, pp.457-473.
[2] Adi Shamir. Identity-based cryptosystems and signature schemes, in Proc. of CRYPTO 84 on Advances in cryptology, pages 47–53. SpringerVerlag New York, Inc., 1985..
[3] V.Goyal, O.Pandey, A.Sahai and B.Waters, Attribute based encryption for fine grained access control of encrypted data, in proc. ACM conf. computer and communications, 2006
[4] J.Bethencourt, A.Sahai, and B.Waters, Ciphertext policy attribute based encryption, in proc. IEEE symposium security and privacy, 2007.
[5] S.Rifki, Y.Park, and S.Moon, A fully secure ciphertext policy attribute based encryption with a tree-based access structure, Journal of Information Science and Engineering, Vo.31,pp.247-265,2015.
[6] G.Wang, Q.Liu and J.Wu, Hierarchical attribute based encryption for fine grained access control in cloud storage services, in Proc. ACM conf. computer and communication security, 2010.
[7] K.Yang, X.Jia, K.Ren and B.Zhang, Dac-Macs: Effective data access control for multiauthority cloud storage systems, in Proc. Of IEEE Infocom, 2013.
[8] Ximeng Liu, Jiafeng Ma, Jinbo Xiong, Qi Li, Jun Ma, Ciphertext – policy weighted attribute based encryption for fine grained access control, International conference on Intelligent networking and collaborative systems, 2013.