ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Security Using Ciphertext Policy Attribute Based Access Control: A Literature Survey.

Sneha Sanjay Pardeshi, Bharti Dhote

ME, Dept. of Computer Engineering, Sinhgad Institute of Technology, Lonavala, India

Professor, Dept. of Computer Engineering, Sinhgad Institute of Technology, Lonavala, India

.

ABSTRACT: Attribute based Encryption is a public cryptographic technique.In this technique different attributes are used for the encryption purposes.In most existing CP-ABE schemes, there is only one authority in the system and all the public keys and private keys are issued by this authority, which incurs ciphertext size and computation costs in the encryption and decryption operations that depend at least linearly on the number of attributes involved in the access policy.There are some multi-authority CP-ABE scheme in which the authorities need not interact to generate public information during the system initialization phase. Besides, the multi-authority ABE eliminates the key escrow problem, achieves the length of ciphertext optimization and enhances efficiency of encryption and decryption operation.In this paper we will summarize all the techniques available for ABE.

KEYWORDS: access control,attribute revocation,CP ABE.

I.INTRODUCTION

In recent years,various paperless techniques are evolved for communication.All data is stored in electronic media.This invention of internet leads people to do transaction online.Online transaction is more cost efficient than the previous techniques.But this invention may suffers from the problem of hacking on the central database to steal information.Then this stolen information can be used for the unethical purpose.So there is need of security mechanism[17]. Attribute based access control is one of the good technique available for encryption purpose. Attribute Based Access Control defines an access control paradigm. In this access rights are granted to users through the use of policies which combine attributes together. The policies can use any type of attributes (user attributes, resource attributes, object, environment attributes etc.). This model supports Boolean logic, in which rules contain ”IF, THEN” statements about who is making the request, the resource, and the action. ABAC[1] is further divided into two parts viz. Key policy Based Access control and Ciphertext Policy Based Access Control.

KP-ABE:

In a KP-ABE scheme, the ciphertext encrypting a message is associated with a set of attributes. A decryption key issued by an authority is associated with an access structure. The ciphertext can be decrypted with the decryption key if and only if the attribute set of ciphertext satisfies the access structure of decryption key. Whole Concept of KP ABE is explained in Figure 1.

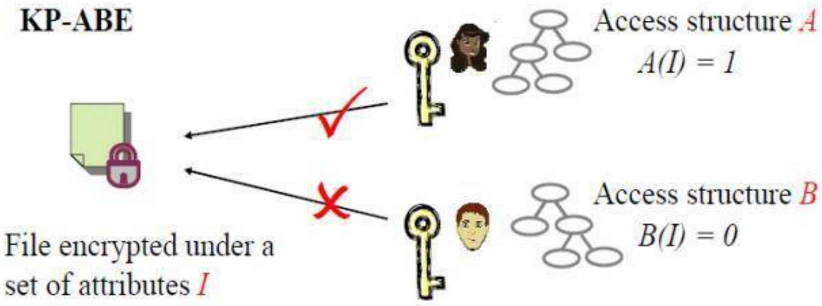

Figure 1: KP-ABE

Drawbacks of the KP-ABE are Encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, and has no choice but to trust the key issuer. KPABE is not naturally suitable to certain applications. For example, sophisticated broadcast encryption, where users are described by various attributes and in this, the one whose attributes match a policy associated with a ciphertext, it can decrypt the ciphertext. KP-ABE scheme supports user secret key accountability. It is providing fine grained access but has no longer with flexibility and scalability.

CP-ABE:

In a CP-ABE scheme, on the contrary, the ciphertext encrypts a message with an access structure while a decryption key is associated with a set of Attribute attributes. The decryption condition is similar: if and only if the attribute set fulfils the access structure. CPABE Scheme can be further described in fig 2.

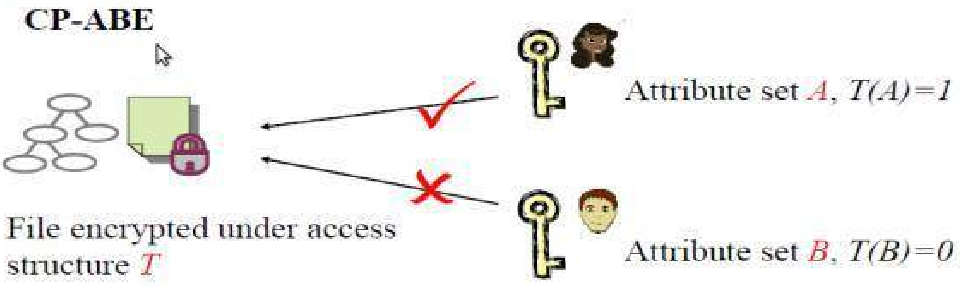

Figure 2: CP-ABE

Limitation of this CP ABE are Negatives of the most existing CP-ABE schemes are still not satisfying the enterprise requirements of access control which require considerable flexibility and efficiency. CPABE has a restriction in terms of specifying policies and management user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so the users can only use all possible combinations of attributes in a single set issued in their keys to fulfill policies. So here we will use better access policy to recover from these limitation.

II. RELATED WORK

In the basic CP-ABE [1-3] schemes, as the number of attributes in the access policy increases size of ciphertext also goes on increasing linearly. For example, the size of ciphertext is n+O(1) in [1] and 2n+O(1) in [2]. In addition, the number of pairing operation is also linearly with the number of attributes in access policy during decryption, which increases the computation overhead on receiver. These limit the usage of ABE in real life applications to a large extent, especially for the scenarios where bandwidth issues and computing resources are of great importance.

Many KP-ABE schemes and CP-ABE schemes have been proposed in the literature. In comparison with KP-ABE, CPABE is more appropriate in access control applications since it enables message encryptor to choose the access structure to decide who can access the message.

The idea about CP-ABE was first proposed by Goyal et al. in [1] but they did not support any modelling.In this system encryptor will encrypt data with the attributes. Attributes may be name, size, city, DOB of user etc. Here access structure used are the AND gate of the attribute .Then they create private key using access structure. For decryption purpose author follow simple recursive algorithm which will take private key and encrypted data to decrypt the data. But this system will not give solution for collision attack .If the two users using same access structure using AND gate the Original file can get without using private key. So this system fails.

Soon after that, Bethencourt, Sahai and Waters [2] proposed the construction of CP-ABE Scheme.This system uses monotononic tree access stucture.In this system users private key can be constructed by attributes instead of access stucture.This system also a collision resistent technique.

Then, Cheung and Newport [8] proposed another CP-ABE which consist of AND gate access structure which is a combination of positive and negative values of AND gate.This scheme is proven as Chosen Plaintext Attack under decisional bilinear Diffie-Hellman (DBDH) assumption.

Herranz et al. [5] proposed CP-ABE towards constantsize ciphertexts.In all the schemes availabe before have size of ciphertext are dependent on the attribute used in the encryprion.So If we are using more attributes then the size of the ciphertext are increased.This is the first scheme where decryption size is constant.Here ciphertext size is independent on the number attributes used.

Chen et al. [7] proposed CP-ABE schemes with constantsize ciphertexts under the threshold access structure. Zhou and Huang proposed a CP-ABE scheme with constant-size ciphertexts under AND gates access structure.

In [8] Cheung and Newport developed CP-ABE schemes in which access structures are AND gates on positive and negative attributes. This scheme is proven to be chosen plaintext (CPA) secure under the decisional bilinear Diffie-Hellman (DBDH) assumption.And the basic scheme can be extended to be CCA secure in the standard model without losing its efficiency.Afterwards Nishant Doshi,Devesh Jinwala[9] proposed a CP-ABE System with constant length which works in a threshold case.But this scheme does not provide recipients anonymity.

Aijun Ge,Rui Zhang,Cheng Chen, Chuangui Ma, and Zhenfeng Zhang[10] developed Threshold Ciphertext Policy Attribute-Based Encryption with Constant Size Ciphertexts which is first CPA secure threshold CP-ABE scheme,which can be further upgraded to the CCA security.

Nuttapong Attrapadung[11] proposed Attribute-Based Encryption Schemes with Constant-Size Ciphertexts schemes allowing for truly expressive access structures and with constant ciphertext size.But encryption required n+t+1 exponentiation, and the decryption required 3 pairing evaluations and O(t2+n) exponentiation, n was the number of attributes in the system and t was the threshold.

All the above approach requires single authority to create public and private keys. Thus, the key escrow problem is inherent such that the trusted authority can decrypt every ciphertext in the system by generating every users private key at any time. One way to solve the key escrow problem is distributing the administration privilege from one authority to many. The encryption system is still secure as long as the required attributes cannot be obtained exclusively from those corrupted authorities and the trusted authority remains honest. In such multi-authority attribute-based encryption schemes, the private keys of the users needed are distributed by different authorities.

Chase [12] proposed a multi-authority ABE.But it does not solve problem of key escrew.Lin[13] provides a threshold multi authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority for the first time. An encrypter can encrypt a message such that a user could only decrypt if he has at least dk of the given attributes about the message for at least t+1; t¡=n/2 honest authorities of all the n attribute authorities in the proposed scheme.But this MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme.

Nishant Doshi and Devesh Jinwala [9] developed system of Constant Ciphertext Length in Single-Authority Ciphertext Policy Attribute Based Encryption.But in this system also central authority is needed.here author worked for collision Resistance problems which is faced by the system.Decryption pairing for key generation is less as compared to the other technique.Here the attributes in the ciphertext must be a subset of users attributes in his secret key.

But this system cant be work for the multiauthority systems. For designing multiauthority system there are to challanges viz. collision and attribute revocation.Multiple users holding attributes from different authorities may collude together to obtain illegal access to the data and Since each attribute is shared by multiple users, any attribute revocation of a user will affect the other users who have the same attribute with him.So here we use key randomization technique to avoid collision problem.Attribute revocation may result in bottleneck during rekeying procedure or security degradation in the system. Existing attribute revocation methods designed for single authority CP-ABE [15-16] could not be applied to multi-authority schemes.

In the ABE each attribute is shared by the multiple users.This revocation may affect to other user who have shared same attribute.May be some authorised users will not get the proper attribute and hence they can't decrypt data.Yu Shucheng et al.[14] provides attribute revocation process to solve this problem.Author gives a proxy reencryption technique by implemention proxy server in the medium.This proxy server can act as a semi-trusted party. On each revocation event, the authority just generates several proxy re-encryption keys and transmits them to proxy servers. Proxy servers will update secret keys for all users but the one to be revoked. Unlike solutions suggested by existing CP-ABE schemes, our construction places minimal load on the authority upon each revocation event, and the authority is able to freely revoke any attribute of users at any time. The only requirement is that proxy servers should stay online and perform honestly.

Bilinear map definition: Let G1 and G2 be a cyclic multiplicative group with the same prime order q, that is, |G1 | =|G2 | = q. Let g be a generator of G1.An efficient bilinear map e: G1 * G2 → G_T , with the following properties:

1. Bilinear: for all g 2 G1 and a; b 2 Zq $e(g^a; g^b) = e(g; g)^{ab}$
2 Non-degeneracy: e(g, g) ≠1.
3 Computability: There is an effcient algorithm to compute e(u,v) for u,v ϵ G:

Access structure : The access structure is combination of AND and OR gates on multi-valued attributes. Without loss of generality, we assume that there are n categories of attributes and every user has at most n attributes with each attribute belonging to a different category. Let U={ att_1...,att_n)}be the set of all attributes in system and s_i={ v_{i1},...,vin)} be the set of possible values for atti , in which ni =| si |;L={L1, ...Lu}(1<=u<=n) be an attribute list for a user, in which Li ∈ Si is an attribute value for atti and W={W_1, ...W_m}(1<=m<=n) be an access structure, in which Wi ∈ Si is an attribute value for att_i

III.CONCLUSION

In this paper,we had summarize all ciphertext policy attribute based encryption scheme.we had deeply studied the all techniques available for Ciphertext Policy Attribute Based Encryption.In this paper we have figured out different advantges and disadvantages of the CP-ABE systems.

ACKNOWLEDGEMENT

Authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. Author is also thankful to the reviewer for their valuable suggestions.Author also thanks the college authorities for providing the required infrastucture and support.Finally, Author would like to extend a heartfelt gratitude to friends and family members.

REFERENCES

[1] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data, Proc. Thirteenth ACM Conference on Computer and Communications Security, pp. 89-98, 2006.
[2] Bethencourt J, Sahai A, and Waters B, Ciphertextpolicy attribute-based encryption, Proc. IEEE Symp. Security and Privacy (SP07), pp. 321-334, May. 2007, doi:10.1109/SP.2007.11.
[3] Waters B, Ciphertext-policy attribute-based encryption: An expressive, effcient, and provably secure realization, Public Key Cryptography Fourteenth International Conference on Practice and Theory in Public Key Cryptography, D. Catalano, N. Fazio, R. Gennaro and A. Nicolosi, eds., Lecture Notes in Computer Science F6571, International Association for Cryptologic Research, pp. 53-70 2011.
[4] Emura K, Miyaji A, and Nomura A, A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length, Information Security Practice and ExperienceFifth International Conference, F. Bao, H. Li and G. Wang, eds., Lecture Notes in Computer Science F5451, Berlin: Springer-Heidelberg, pp. 13-23, 2009.
[5] Herranz J, Laguillaumie F, and Rfols C, Constant size ciphertexts in threshold attributebased encryption, Public Key Cryptography Thirteenth International Conference on Practice and Theory in Public Key Cryptography, P.Q. Nguyen and D. Pointcheval, eds., Lecture Notes in Computer Science F6056, International Association for Cryptologic Research, pp. 19-34 2010.
[6] Attrapadung N, Libert B, and Panafieu E.D, Expressive key-policy attribute-based encryption with constant-size ciphertexts, Public Key Cr yptographyFourteenth International Conference on Practice and Theory in Public Key Cryptography, D. Catalano, N. Fazio, R. Gennaro and A. Nicolosi, eds., Lecture Notes in Computer Science F6571, International Association for Cryptologic Research, pp. 90-108 201
[7] Chen Cheng, Zhang Zhenfeng, and Feng Dengguo, Efficient ciphertext policy attributebased encryption with constant-size ciphertext and constant computation-cost, Provable SecurityFifth International Conference, X. Boyen, and X. Chen, eds., Lecture Notes in Computer Science F6980, GmbH Berlin: Springer-Verlag, pp. 84-101 2011.
[8] Cheung Land Newport C, Provably secure ciphertext policy ABE, Proc. Fourteenth ACM Conference on Computer and Communications Security(CCS007),pp-465,2007 doi:10.1145/1315245.1315302.
[9] Doshi N and Jinwala D, Constant Ciphertext Length in CP-ABE, IACR Cryptology ePrint Archive, 2012, 2012: 500.
[10] Ge Aijun, Zhang Rui, and Chen Cheng, Threshold ciphertext policy attribute-based encryption with constant size ciphertexts,Information Security and PrivacySeventeenth Australasian Conference, pp. 336-349, 2012, doi:10.1007/978- 3-642-31448-3 25.
[11] Attrapadung N, Herranz J, and Laguillaumie F, Attribute-based encryption schemes with constant-size ciphertexts, Theoretical computer science, vol. 422, pp. 15-38, Mar. 2012.
[12] Chase M, Multi-authority attribute based encryption, Theory of CryptographyFourth Theory of Cryptography Conference, S.P. Vadhan, eds., Lecture Notes in Computer Science F4392, Berlin: Springer-Verlag, pp. 515-534 2007.
[13] Lin Huang, Cao Zhenfu, Liang Xiaohui, and et al. Secure threshold multi authority attribute based encryption without a central authority, Information Sciences, vol. 180, no. 13, pp. 2618- 2632, July. 2010.
[14] Yu Shucheng, Wang Cong, Ren Kui and et al. Attribute based data sharing with attribute revocation, Proc. Fifth Symposium on Information, Computer and Communications Security (ASIACCS 10), pp. 261-270, 2009, doi:10.1145/1755688.1755720.
[15] Jahid S, Mittal P, and Borisov N, Easier : Encryption-based access control in social networks with efficient revocation Proc. Sixth ACM Symposium on Information, Computer and Communications Security (ASIACCS 11), pp. 411- 415, 2011, doi:10.1145/1966913.1966970.
[16] Hur J and Noh D.K, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214- 1221, July 2011, doi:10.1109/TPDS.2010.203.
[17] Bharti Dhote and A.M. Kanthe,”Secure Approach for Data in Cloud Computing”, International Journal of Computer Applications (0975 8887)

BIOGRAPHY

Sneha Sanjay Pardeshi is a student in the Computer Engineering Department, Sinhgad Institute Of Technology Lonavala, Savitribai Phule University Of Pune . She is pursuing Master of Computer Engineering (ME) degree from SIT, Lonavala, MS, India. Her research interests are Computer Security (wireless Networks).

Bharti Dhote is a professor in a Computer Engineering, Sinhgad Institute Of Technology Lonavala, Savitribai Phule University Of Pune.