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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Attribute Based Encryption Techniques and its Applications.

Harshada Deshmukh , Rahul kapse

PG Student, Dept. of Information Technology, Pillai HOC College of Engineering and Technology,

Mumbai University, Maharashtra, India

Assistant Professor, Dept. of Information Technology, Pillai HOC College of Engineer and Technology,

Mumbai University, Maharashtra, India

ABSTRACT: To protect confidentiality of stored data, the data must be encrypted before transfer.To gain fine grained access control and to minimize a computational overhead ABE was introduced.Attributes play vital role in attributes based encryption.To control user's access and to generate public key for encryption of data attributes are widely used.Attribute based encryption can be achieved through different techniques such as Key policy based - ABE, cipher text - ABE,ABE scheme with non-monotonic access structure, Hierarchical ABE scheme.There are various applications of ABE some of them are, Security of Personal Health Record using ABE and Audit Log application.

KEYWORDS: Attribute based encryption, Key-Policy based Attribute based encryption, cipher text Attribute based encryption, Personal Health records.

I. INTRODUCTION

People can store share data by using internet technology as it is growing rapidly .To satisfy various user's requirement, cloud has come forth to put up several application services. In order to protect the sensitive data, it should be encrypted before uploading. Verifiability of attributes of a every users and maintaining the privacy is the main contribution. Traditional public key infrastructure is not recommended as it .The data owner needs to obtain user's public, also computational overhead is increased key for traditional public key infrastructure. To overcome this disadvantage Attribute Based Encryption was introduced.

II. RELATED WORK

[6]In 2005 , A. Sahai and B. Waters, "Fuzzy identity-based encryption," introduced the concept of Fuzzy Identity Based Encryption, which allows for error-tolerancebetween the identity of a private key and the public key used to encrypt a cipher text.Paper described two practical applications of Fuzzy-IBE of encryption using biometrics and attribute-based encryption. It presented the construction of a Fuzzy IBE scheme that uses set overlap as the distance metric between identities. Finally, It proved scheme under the Selective-ID model by reducing it to an assumption that can be viewed as a modified version of the Bilinear Decisional Diffie -Hellman assumption. This work motivates a few interesting open problems. The first is whether it is possible to create a Fuzzy IBE scheme where the attributes come from multiple authorities. While, it is natural for one authority to certify all attributes that compromise a biometric, in attribute-based encryption systems there will often not be one party that can act as an authority for all attributes. Also, a Fuzzy-IBE scheme that hides the public key that was used to encrypt the cipher text isintriguing.scheme uses set-overlap as a similarity measure between identities. (Note a Hamming-distance construction can also be built using techniques.) An open problem is to build other Fuzzy-IBE schemes that use different distance metrics between identities.

[3]In 2007, J. Bethencourt, A. Sahai, and B. Waters, created a system for Cipher text-Policy Attribute Based Encryption. System allows for a new type of encrypted access control where user's private keys are specified bya set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

decrypt. System allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. Finally, provided an implementation of system, which included several optimization techniques.One limitation of system is that it is proved secure under the generic group heuristic. Believe an important endeavor would be to prove a system secure under a more standard and non-interactive assumption. This type of work would be interesting even if it resulted in a moderate loss of efficiency from existing system.

[11]In 2011, B. Waters, "Cipher text-policy attribute-based encryption An expressive,efficient, and provably secure realization,". They created a system for Cipher text-Policy Attribute Based Encryption.System allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. System allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. Finally, They provided an implementation of system, which included several optimization techniques.

Limitation of system is that it is proved secure under the generic group heuristic. They believe an important endeavor would be to prove a system secure under a more standard and non-interactive assumption. This type of work would be interesting even if it resulted in a moderate loss of efficiency from existing system.

A. *Fine-grained Access Control.*

Fine grained access control system grants different access rights to different users and gives flexibility in access rights of individual users. In this paper we introduced that encrypted data which is stored on storage server,can be decrypted in different form of pieces by different users as a security policy.

B. *Secret Sharing scheme.(SSS)*

To divide the secret among the number of parties, Secret sharing scheme is used. The share of the party is the information given to a party. The set of parties construct the secret by using their share, is as defined SSS.
The leaves of tree-access structure are associated with attributes and the user's key is associated with the leaves.
If the key access structure is satisfied by the attributes associated with a cipher text, then user is able to decrypt the cipher text.

C. *Identity-Based Encryption and Extensions.*

It represented a particular scheme which is known as Fuzzy Identity-Based Encryption (FIBE).FIBE achieves error tolerance making it matching for biometric identities. Yao et. al. [18] show how an IBE system that encrypts to multiple hierarchical identities in a collusion-resistant manner implies a forward secure Hierarchical IBE scheme. Theyalso note how their techniques for resisting collusion attacksare useful in attribute-based encryption. However, the cost of their scheme in terms of computation, private key size, and ciphertext size increases exponentially with the number of attributes. We also note that there has been other work that applied IBE techniques to access control, but did not address our central concern of resisting attacks from colluding users.

III. ATTRIBUTE BASED ENCRYPTION TECHNIQUES

A. Attribute -based Encryption Scheme

Sahai and Waters proposed an attribute based encryption scheme in 2005.There are authority,sender and receiver in this scheme, and keys are generated by authority 's for sender and receiver to encrypt or decrypt data. Keys are generated according to attributes; and these attributes of public key and master key. If any data user who wants to add to this system, and he owns to attributes don't include pre- defined attributes. The authority will re-define attributes and generate a public key and master key again. The sender encrypts data with a public key and a set of descriptive attributes. A data user's role is to decrypt encrypted data with his private key sent from the authority, and then he can obtain the needed data. For decrypting data, attributes in data user's private key will check by matching with the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

attributes in encrypted data. The data user's private key will be allowed to decrypt the encrypted data if and only if the number of "matching" is at least a threshold value d.

B. Key-Policy Attribute-based Encryption Scheme

To describe the encrypted data and to builds a access policy in user's private key, set of attributes were used. user can obtain the message through decrypt algorithm, if attributes of the encrypted data can satisfy the access structure in user's private key, In addition, the KeyGen() algorithm varies from the attribute-based encryption which is introduced at subsection one in this section. The user's private key is according to the access structure to generate.

C. Cipher text-Policy Attribute-based Encryption Scheme.

It is similar to the key policy attribute-based encryption. In key policy attribute-based encryption, the access policy is in user's private key, the access policy is switched to the encrypted data in ciphertext policy attribute-based encryption. With the user's private key, a set of descriptive attributes are associated. The access structure of the encrypted data is corresponding to the user's private key with a set of descriptive attributes. If a set of attributes in user's private key satisfies the access structure of the encrypted data, the data user can decrypt the encrypted data; if it cannot, the data user cannot obtain the message. For example, the access structure in the encrypted data is{MISV(TeacherWStudent)}. If a set of attributes in user's private key is {MISVTeacher}, the user can recover the data. In the access structure of this scheme, it adopts the same method which was depicted in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data, it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is very close to the traditional access control scheme.

D. Attribute-based Encryption Scheme with Non-Monotonic Access Structures

The access formula of access structure in user's private key can represent any type through attributes such as negative ones. It is different from the previous attribute- based encryption scheme. The previous schemes are like KP-ABE scheme, and the access structure in user's private key has monotonic access formula. No negative attributes exist in it. Apart from this, the access structure of this scheme is the same as the access structure of KP-ABE scheme. There is a Boolean formula such as And, OR, and threshold gates in these access structures, but there is a boolean formula, NOT in access structure of this scheme. However, other schemes do not include it. There is an example for this scheme. If a teacher in department of information management wants to share the data with students, he will set a set of attributes in the encrypted data. And there is an access structure, {MISVStudent} in students' private key. But the teacher doesn't want graduates to access this data, he adds NOTgraduate to the access structure.

E. Hierarchical Attribute-based Encryption Scheme.

This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. Moreover, it used disjunctive normal form (DNF) to express the access control policy, and the same domain authority in this scheme administered all attributes in one conjunctive clause. There are five roles in this scheme: the cloud storage service, data owner, the root authority, the do- main authority, and data users. The role of cloud storage service is that let a data owner can store data and share data with users. The role of data owner is encrypting data and sharing data with users. The role of the root authority is generating system parameters and domain. keys, to distribute them. The role of domain authority is managing the domain authority at next level and all users in its domain, to delegate keys for them. Besides, it can distribute secret keys for users. And users can use their secret keys to decrypt the encrypted data and obtain the message. The key generation in this scheme adopts a hierarchical method. The root authority generates a root master key for domain authority at the first level. The system public key and the master key of the domain authority at first level are used to create the master keys for the domain authorities at the next level by the root authority or the domain authority at the first level. In addition, the do- main authority generates the user identity secret key and the user attribute secret key for the authorized user.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

IV. RESULT

Security Analysis

The criteria contain C1- fine- grained access control, C2- data confidentiality, C3- scalability, C4- user accountability, C5- user revocation, and C6- collusion resistant.The comparison table is listed in Table 1.

Item	ABE	KP-ABE	CP-ABE	ABE with non-monotonic	HABE
C1	N	Y	Y	Y	Y
C2	Y	Y	Y	Y	Y
C3	N	N	N	N	Y
C4	N	N	Y	N	Y
C5	N	Y	Y	Y	Y
C6	Y	Y	Y	Y	Y

Table1. The criteria of an ideal attribute-based encryption scheme

The ABE scheme only satisfies one criteria. Because it uses the attributes in the user's private key to match the attributes in the encrypted data, it only achievethe basic security requirement. But it provides the first concept to develop the attribute-based encryption scheme. After that, these schemes cannot satisfy all the criteria except HABE. Besides, the criteria of user accountability is hard to achieve.It is hard to trace who shares the key,because preventing the problem of illegal key sharing among users is difficult to solve. So almost all ABE schemes that we introduce cannot achieve two criteria.

V. APPLICATION OF ATTRIBUTE BASED ENCRYPTION TECHNIQUES

A. Security of Personal Health Record using Attribute based Encryption

The Patients are efficiently able to create, manage and share their personal health information through PHR. In coming year, Personal Health Record (PHR) has developed as the emerging trend in the health care technology and by which this PHR is now a day's stored in the clouds for the cost reduction purpose and for the easy sharing and access mechanism. The main concern about this PHR is that whether the patient is able to control their data or not. It is very essential to have the fine grained access control over the data with the semi-trusted server. But in this the PHR system, the security, privacy and health data confidentiality are making challenges to the users when the PHR stored in the third party storage area like cloud services.The PHR data should be secured from the external attackers and also it should be protect from the internal attackers such that from the cloud server organization itself.When the PHR owner upload the PHR data to the cloud server, the owner is losing the physical control over the data and thus the cloud server will obtain the access on the plain text data and itwill make lots of security challenges to the PHR privacy and confidentiality. The encryption of data before outsourcing it to the third party is consider as the promising. The normal public key encryption methods and another traditional encryption schemes are making lots key management problem for the sharing of the personal health record and also all those methods provide very less scalability to the system.In recent days the attribute based encryption scheme and its different variations are chosen as the main encryption primitive for the personal health records which made the storage, retrieval and sharing of the medical information more secure and efficient. But in attribute based encryption, the on demand user revocation is a challenging problem. So the cipher text policy –attribute based encryption and key- policy based attribute based encryption are also applied for the security of the personal health record. For reducing the key-management overhead and distribution problems, the multi-authority attribute based encryptions scheme is used. For the emergency access purpose, the break glass access attribute are also introduced with the personal health record scheme.

B. Audit Log Application.

An important application of KP-ABE deals with secure forensic analysis: One of the most important needs for electronic forensic analysis is an "audit log" containing a detailed account of all activity on the system or network to be protected. Such audit logs, however, raise significant security concerns: a comprehensive audit log would become a prized target for enemy capture. Merely encrypting the audit log is not sufficient, since then any party who needs to

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

legitimately access the audit log contents (for instance a forensic analyst) would require the secret key – thereby giving this single analyst access to essentially all secret in- formation on the network. Such problematic security is- sues arise in nearly every secure system, and particularly in large-scale networked systems such as the Global Information Grid, where diverse secret, top secret, and highly classified information will need to appear intermingled in distributed audit logs. Our KP-ABE system provides an attractive solution to the audit log problem. Audit log entries could be annotated with attributes such as, for instance, the name of the user, the date and time of the user action, and the type of data modified or accessed by the user action.

VI. CONCLUSION AND FUTURE WORK

In this paper, we survey five different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, and HABE, and illustrate their schemes and compare them. These schemes can be classified according to their access policy. The access policy in the user's private key is KP-ABE, and the access policy in the encrypted data is CP-ABE. Besides, we can find these schemes that are hard to satisfy user accountability. Moreover, the access structure is pre-defined in these schemes; if a new user wants to access data and his attributes are not in the access structure, these encrypted data will be re-generated. Thus, based on the discussion above, these existing attribute-based encryption schemes have properties: (1) These schemes are encrypted with attributes, so a data owner just needs to predefine these attributes that he would use, he doesn't need to care about the number of users in the system; (2) Each attribute has public key, secret key, and a random polynomial, so different users cannot combine their attributes to recover the data, and different users cannot carry out collusion attacks; (3)Only the user who possesses the authorized attributes can satisfy the access policy to decrypt data; (4) The access pol- icy contains a boolean formula such as AND, OR et al. which can let the access structure be flexible to control users' access. However, almost all schemes exist that the authority is used to generate keys. Since these schemes contain the authority that just suits the private cloud environments, the authority should be removed in the future. Furthermore, ABE schemes (like KP-ABE or CP- ABE scheme) are generally applied in the field of proxy re-encryption.

REFERENCES

[1] J. Anderson, "Computer Security Planning Study," Air Force Electronic System Division, Technical report 73-51, 1972.
[2] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "Me- diatedCiphertext-Policy Attribute-Based Encryption and Its Application," Proc. WISA , LNCS 5932, pp. 309–323, 2009.
[3] A. Sahai, B. Waters, "Fuzzy Identity-Based Encryption," Proc. Eurocrypt, pp. 457–473, 2005.
[4] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-Based En- cryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conference on Computer and Communications Security, pp. 89–98, 2006.
[5] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symposium on Security and Privacy , pp. 321–334, 2007.
[6] R. Ostrovsky, A. Sahai, B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Confer-enceonComputerandCommunicationsSecurity,pp.195– 203, 2007.
[7] A. Lewko, A. Sahai, B. Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symposium on Security and Privacy , pp. 273–285, 2010.
[8] A. Boldyreva, V. Goyal, V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. ACM Conference on Computer and Communications Security , pp. 417–426, 2008.
[9] N. Attrapadung, H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," Proc. Pairing, LNCS 5671, pp. 248–265, 2009.
[10] M. Pirretti, P. Traynor, P. McDaniel, B. Waters, "Secure Attribute-BasedSystems," ProcACMConferenceon Computer and Communications Security , , pp. 234–245,2006.
[11] S. Rafaeli, D. Hutchison, "A Survey of Key Management for Secure Group Communications," ACM Computing Surveys, vol. 35, pp. 309–329, 2003.
[12] P. Golle, J. Staddon, M. Gagne, P. Rasmussen, "A Content- Driven Access Control System," Proc. Symposium on Identity and Trust on the Internet, pp. 26–35, 2008.
[13] S. Yu, C. Wang, K. Ren, W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ASIACCS '10, 2010.
[14] S. D. C. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati, "Over-encryption: Management of Access Control Evolution on Outsourced Data," Proc. VLDB, 2007.
[15] D. Boneh, M. K. Franklin, "Identity-based Encryption from the Weil Pairing," Proc. CRYPTO 2001, LNCS vol. 2139, pp. 213– 229, 2001.
[16] A. Kate, G. Zaverucha, and I. Goldberg, "Pairing-based onion routing," Proc. Privacy Enhancing Technologies Symposium 2007, LNCS vol. 4776, pp. 95–112, 2007.
[17] K. C. Almeroth, M. H. Ammar, "Multicast Group Behavior in the Internet's multicast backbone (MBone)," IEEE Communication Magazine, vol. 35, pp. 124–129, 1997.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

BIOGRAPHY

Harshada Deshmukh is pursuing M.E (IT) from Pillai College of Engineering and Technology, Rasayani ,Mumbai University. She did his graduation B.E (Computer) from Mumbai University, Maharashtra. She is currently working on survey of distributed sharing with verifiable outsourced cryptography using Attribute Based Encryption.

Rahul Kapse is working as assistant professor in Dept. of Information Technology at Pillai College of Engineering ,Rasayani, Mumbai University. He has academic experience of 11 years and industry experience of 3 years.His area of interest are Software Engineering, Genetic Algorithm, Object Oriented Analysis and Design, Advanced Algorithms and Complexity, Decision Making and Adaptive Business Intelligence, ISRM.