ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Secure And Privacy Data Sharing Using Attribute Oriented Authentication (AOA) And Attribute Oriented Transmission (AOT)-A Survey

C.Manjula[1], B.Anuradha[2], H.Ananda Kumar[3]

PG Scholar, Department of Information Technology, SNS College of Engineering, Coimbatore[1]

Associate Professor, Department of Information Technology, SNS College of Engineering, Coimbatore[2]

Assistant Professor, Department of Information Technology, SNS College of Engineering, Coimbatore[3]

ABSTRACT: Many technologies are evolved on providing security to the cloud and its not possible to protect the whole cloud. Instead, we are focusing on providing security to data sharing terminology. In data sharing system, two important issues such as enforcement of access policies and support of policy updates is faced. One of the efficient cryptographic solution to solve these issue is XCP-ABE in which the user can define their own access policies and enforce these polices on the data to be distributed. Usually encryption and decryption is done by generating the private keys which is not suitable for data sharing scenarios. In proposed system, the encryption and decryption is done by providing additional secrets i.e..Generation of super keys. On observing the existing system it is found that, there are three major drawbacks such as Key escrow problem, invocation of users and lack of black box traceability which takes the advantages over the proposed one. This additional measure is an optional variant applicable to high sensitivity data subject to frequent access.

Keywords: Data sharing, Extended Cipher text policy-Attribute based encryption, access policies, black box traceability.

1. INTRODUCTION

Using various computing technologies, the user can efficiently share data's with others using online external storage. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and services. The social networks such as face book and MySpace are the main example for data distribution. Although they enjoy the advantages of efficient sharing, the main drawback is that security. Hence many technologies are emerged in providing security to data sharing.

Attribute based encryption(ABE) ,It is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. It is an efficient way for providing defining access policies based on different attributes of the requester, environment, or the data object. ABE is based on log encryption, rather than encrypting each part of log, it just encrypts the log that matches the recipients attribute.

Cipher text policy-Attribute based encryption(CP_ABE)is an technique which is developed for solving key escrow problem and key invocation .It is an cryptographic solution to solve these issues. Here, in this technique the encrypted data can be kept confidential even if the storage is entrusted and also secured against collision attacks. Each user is assigned with an unique identifier ,therefore user can be easily revoked by using unique identifiers; on the other hand encryption and decryption can also done without using the unique identifier. The main drawback of this system is that computational cost is high and computation is very complex, since we are using a Decision bilinear Diffe-Hellman(DBDH).

Extended cipher text policy attribute based encryption (XCP-ABE) is an improvised version of CP-ABE. It provides an efficient algorithm for secured transmission of data. Despite of trusting the cloud owners or providers, it enables the data owners to define their own access policies. It avoids storing the public key certificates of the user, instead an private keys are generated by key generation centre by applying KGC master's key .An identity based encryption is added to KGC to avoid the user's with same attribute. Thus the major of this approach is to find the malicious user from the real user and reduces the storing of public key certificates under the traditional public key infrastructure.

2. EXISTING SYSTEM

The previous work is KP-ABE ,in which the policies are built into the user credentials. So, hence it comes with an main drawback is that ,an fine grained access is adopted. Adoption of fine grained access will lead to an systematic cause that is, using an single attribute of an user the complete details can be revealed.

2.1 RELATED WORK:

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

There are two types of attribute based encryption called Key policy-ABE (KP-ABE) and cipher test policy-ABE(CP-ABE) .In KP-ABE ,attributes are used to describe the encrypted data and the policies are built into the users credentials and the encryptor can decide who can access the data. On the other hand, CP-ABE is more efficient for data sharing system since here the data access are handled by the data owners.

A mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE)[1] scheme is proposed to support revocation of user attributes, which the user cannot use it in the decryption phase. This allows the encryptor to encrypt a message according to an access policy over a set of attributes, and only users who satisfy the access policy and whose attributes are not revoked can decrypt the ciphertext. This scheme is yet to be focused and extended to have a security proof under standard complexity assumptions.

The Fuzzy Identity Based Encryption, [2]which allows for error-tolerance between the identity of a private key and the public key used to encrypt a cipher text. It creates a Fuzzy IBE scheme first, 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 ciphertext is intriguing. Our scheme uses set-overlap as a similarity measure between identities. Difficulty is to build other Fuzzy-IBE schemes that use different distance metrics between identities.

A new cryptosystem for fine-grained sharing of encrypted data[3], called as Key-Policy Attribute-Based Encryption (KP-ABE) in which the ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. It solves drawback of encrypting data, and it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). However, this scheme do not hide set of attributes under which the data is encrypted and even if it possible, then viewing attributes as keywords in such a system would lead to the first general keyword-based search on encrypted data. It leaves the problem of hiding the set of attributes as open.

Attribute-Based Encryption with Non-Monotonic Access Structures,[4] provides a proof of security for our scheme based on the Decisional Bilinear Diffe Hellman (BDH) assumption and with a less expensive ABE systems that allows a user's private key to be expressed in terms of any access formula over attributes. Access formula used in this system show some problems during decryption process, and also more processing time is required to complete encryption and decryption process.

'Revocation Systems with Very Small Private Keys'[5]and 'Ciphertext-Policy Attribute Based Encryption'[6], is a method for creating public key broadcast encryption systems which is mainly for revoking users. It revokes users from the storage and uses simple private keys for processing but, more size required for the ciphertext storage[5]. Whereas, system[6],[7] 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. One limitation of the system is that it is proved secure under the generic group heuristic but, an important endeavor would be a system secure under a more standard and non-interactive assumption. The credentials are given to the users instead of attributes, but the main drawback is that the intruders can easily hack the data and steal the information from the data base.[8],[9],.

3. PROPOSED WORK

In this paper, we propose an Extended CP-ABE scheme for secure data sharing, which achieves the following features

First, the key escrow problem is the arrangement of cryptographic keys so that the intruders can easily hack these keys and this problem can be solved by key issuing protocols. Using master secret keys, the key issuing protocol is used to generate and issue user the secret keys by performing a 2party computation between the key generation center and Data storage center using their master keys. Despite, the user cannot completely relay on KGC and data storing center in order to protect the data to be shared. Thus this is overcome by enforcing the data confidentiality and privacy cryptographically.

Second, the User Invocation which is done via the proxy encryption algorithm with XCP-ABE. In each attribute group, the attribute key are distributed to the valid users and which then are used to re-encrypt the decrypted data from the XCP-ABE algorithm. On any membership changes it enhances the backward and forward secrecy of the data. The additional functionality is that , providing invocation which can be done at both levels system level as well as the each attribute level. If suppose the user is revoked from the other attribute groups, then the user can still decrypt the shared data until he holding the attributes that satisfy the access policy of the cipher text.

Third, the Black Box Traceability which is used to find the original user from the malicious user. It is used to trace the user having the same attributes and find out the malicious one. If the attribute is from the unknown user, the KGC prevents it entering to the data center.

In this process, the data owner does not define their access policy over users but they define their access policy over the attributes in the previous ABE schemes. The proposed scheme manages the membership management and user invocation, the KGC is responsible for attribute key management and CP-ABE scheme provides confidentiality. Therefore, the proposed scheme is most suitable for data sharing scenarios where the user encrypt the data only once and upload it into data centre ,then encryption and decryption is done.

3.1. SYSTEM ARCHITECTURE:

The Data owner shares the file with receiver attributes and data owner public key. The KGC verifies , validates and authenticate the data owner with the private

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

keys. The same Process is repeated at the receiver side. Both the owner and receiver encrypt and decrypt the data using their super keys, during User retrieval process.The KGC is added with an identity based encryption which also identifes the malcious user from the original user.It also prevents the malicious user entering into the system.Thus the KGC efficently authenticates the user and owner with their private and public key inorder to generate the super keys.

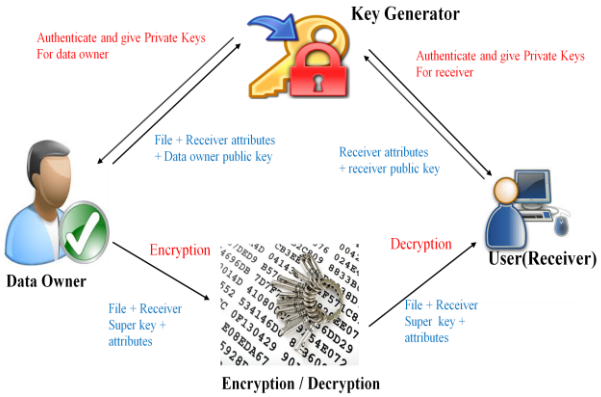

Fig 1:Overall System Architecture

3.2. EXPERIMENTAL RESULT:

3.2.1 DATA OWNER FILE SHARING:

In this process the data owner shares files to the another user, using his public key and the receivers attribute. Then the Key Generation Center checks the public key of the user and authenticates the private keys for data owner. Thus the data owner only decides who can access the files. While sharing the file, the data owner gives the attribute of the user who want to receive the file .Then the encryption file uses these attribute to encrypt the file. Here the input parameters will be the users detail for registration, the KGC checks for any duplicate entry and then it gets the log in details of the user. Once the login details are entered, then the KGC again checks and authenticate the user and allow to access. Then the file gets uploaded and receiver can browse the file.

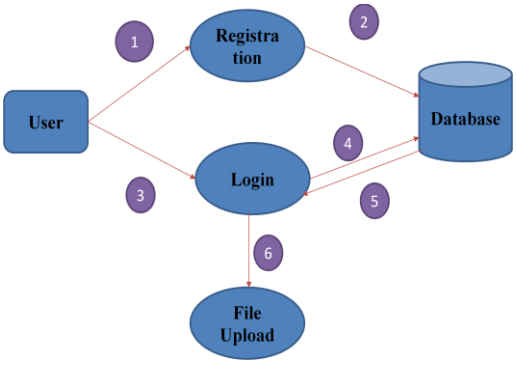

Fig 2:Data owner File Sharing system Architecture

4. CONCLUSION

The enforcement of access policy and support for policy updates are the two important issues in data sharing system. The proposed Scheme XCP-ABE is used to solve these issues through removing escrow problem, user revocation and provides black box traceability. Thus the proposed scheme enhances the data privacy and confidentiality in data sharing system against the system administrators and any outsiders without enough credentials

REFERENCES:

[1] J. Anderson, “Computer Security Planning Study,” Technical Report 73-51, Air Force Electronic System Division, 1972.

[2] L. Ibrahim, M. Petkovic, S. Nikola, P. Hartel, and W. Jonker, “Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application,” Proc. Int’l Workshop Information Security Applications (WISA ’09), pp. 309-323, 2009.

[3] A.Sahai and B.Waters,“Fuzzy Identity-Based Encryption,” Proc. Int’l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt ’05), pp. 457-473, 2005.

[4] V. Goyal, O.Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[5] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[6]R.Ostrovsky,A.Sahai,andB.Waters,“Attribute-Based Encryption with Non-Monotonic Access Structures,” Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007.

[7] A. Lewko, A. Sahai, and B. Waters, “Revocation Systems with Very Small Private Keys,” Proc. IEEE Sym p. Security and Privacy, pp. 273-285, 2010.

[8]A.Boldyreva, V.Goyal and V.Kumar, “Identity-Based Encryption with Efficient Revocation,” Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

[9] N. Attrapadung and H. Imai, “Conjunctive Broadcast and Attribute-Based Encryption,” Proc. Int’l Conf. Palo Alto on Pairing-Based Cryptography (Pairing), pp. 248-265, 2009.