KEY-POLICY ATTRIBUTE BASED ENCRYPTION TO SECURE DATA STORED IN CLOUD

C.Vinoth[1], G.R.Anantha Raman[2]

[1] Computer Science and Engineering,ACE Hosur(India)

[2]Assistant Professor, Computer Science and Engineering, ACE Hosur (India)

ABSTRACT

As more sensitive data is shared and stored by third-party sites on the Internet, the data in these sites will need to encrypt. The main drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We progress a new cryptosystem for fine-grained sharing of re-encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. We explain the applicability of our construction to sharing of audit-log information and broadcast re-encryption with TPA(third Party Auditor). Our analysis supports delegation of private keys which subsumes Hierarchical Identity-Based Re-Encryption (HIBR).

***Key Words*: *Attribute Based Encryption, fine-grained sharing,Key Policy, KDC*.**

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction . There are two main categories of cloud infrastructure: public cloud and private cloud. To take advantage of public clouds, data owners must upload their data to commercial cloud service providers which are usually considered to be semi trusted, that is, honest but curious. That means the cloud service providers will try to find out as much secret information in the users' outsourced data as possible, but they will honestly follow the protocol in general. Traditional access control techniques are based on the assumption that the server is in the trusted domain of the data owner, and therefore an omniscient reference monitor can be used to enforce access policies against authenticated users.

However, in the cloud computing paradigm this assumption usually does not hold, and therefore these solutions are not applicable. There is a need for a decentralized, scalable, and flexible way to control access to cloud data without fully relying on the cloud service providers. Data encryption is the most effective in regard to preventing sensitive data from unauthorized access. In traditional public key encryption or identity-based encryption systems encrypted data is targeted for decryption by a single known user. Unfortunately, this functionality lacks the expressiveness needed for more advanced data sharing. To address these emerging needs, Sahai and Waters [13] introduced the concept of attribute-based encryption (ABE). Instead of encrypting to individual users, in ABE system, one can embed an access policy into the ciphertext or decryption key. Thus, data access is self-enforcing from the cryptography, requiring no trusted mediator. ABE can be viewed as an extension of the notion of identity-based encryption in which user identity is generalized to a set of descriptive attributes instead of a single string specifying the user identity. Compared with identity-based encryption, ABE has significant advantage as it achieves flexible one-to-many encryption instead of one-to-one; it is envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control. There are two types of ABE depending on which of private keys or ciphertexts that access policies are associated with. In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labeled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy (also called the access structure) that specifies which type of ciphertexts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast [5]. For example, in a secure forensic analysis system, audit log entries could be annotated with attributes such as 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. While a forensic analyst charged with some investigation would be issued a private key that associated with a particular access structure. The private key would only open audit log records whose attributes satisfied the access policy associated with the private key.

The first KP-ABE construction was very expressive in that it allowed the access policies to be expressed by any monotonic formula over encrypted data. The system was proved selectively secure under the Bilinear Diffie-Hellman assumption. Later, Wang et al. [6] proposed a KP-ABE scheme where private keys can represent any access formula over attributes, including nonmonotone ones, by integrating revocation schemes into the Goyal et al. KP-ABE scheme. In a ciphertext-policy attribute-based encryption (CPABE) system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the ciphertext, stating what kind of receivers will be able to decrypt the ciphertext. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority. Such a user can decrypt a ciphertext if his/her attributes satisfy the access policy associated with the ciphertext. Thus, CP-ABE mechanism is conceptually closer to traditional role-based access control method.

However, we notice that most of existing identity-based broadcast encryption schemes with constant-size ciphertext do not satisfy the linearity property, and it is not a necessary condition for constructing a KP-ABE schemes with constant-size ciphertext. In this paper, we propose a new KP-ABE construction. In our construction, the access policy can be expressed as any monotone access structure. Meanwhile, the ciphertext size is independent of the number of ciphertext attributes, and the number of bilinear pairing evaluations is reduced to a constant.We prove that our scheme is semantically secure in the selective-set model based on the general Diffie-Hellman exponent assumption. The rest of this paper is organized as follows. Some necessary background knowledge about bilinear pairings, access structure and linear secret sharing scheme.

The rest of this paper is organized as follows. We first summarize the related work in Section II. Then, in Section III, we present system models used in this paper. In Section IV, the implementation part is discussed. The figures are discussed in section V.Finally, we conclude our work in Section VI .

II. RELATED WORKS

Decentralized Access Control with Anonymous Authentication scheme was proposed by Sushmita Ruj et al.[1]. In this the unknoun user is not allowed to access data. ABE was proposed by Sahai and Waters [13]. In ABE, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs. In key-policy ABE or KP-ABE (Wang et al. [6]), the sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt information if it has matching attributes. In Ciphertext-policy, CP-ABE ([13]), the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates. All the approaches take a centralized approach and allow only one KDC, which is a single point of failure(FIGURE.1). Recently, Lewko and Waters [4] proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. To get over this problem, Green et al. proposed to outsource the decryption task to a proxy server, so that the user can compute with minimum resources (for example, hand held devices). However, the presence of one proxy and one KDC makes it less robust than decentralized approaches. Both these approaches had no way to authenticate users, anonymously. Yang et al. presented a modification of [6], authenticate users, who want to remain anonymous while accessing the cloud. This was also a centralized approach. However, as mentioned earlier in the previous section it is prone to replay attack.

OUR CONTRIBUTIONS

The main contributions of this paper are the following:

1) Key-Policy Attribute Based Encryption of data stored in cloud will allow only the authorized users.
2) Only Valid users are able to access and modify the data stored in cloud.
3) During authentication, the user personality will be protected.
4) Here the KDC is used to distribute the keys.
5) It will help to multiple read and write on data stored in cloud environment.
6) It will be less cost and more secure to data storage in cloud.

III. OUR PROPOSED KEY POLICY ATTRIBUTE BASED ENCRYPTION SCHEME

3.1 Introduction

Our proposed Key-Policy Attribute Based Encryption scheme has described and analyzed in this section.According to KP-ABE scheme a user can able to make a file and store it safely in the cloud environment. This scheme consists of use of the several modules and discussed below .We will first dispute our scheme in details and then gives a concrete example to show how it works.

Here several attributes are used to provide access to the authorized users in the cloud. The MSG is the message and the X is the access policy to store the data. The Secret key Sk is used to retrieve the data from cloud server.

To store the data in Cloud,

C=ABE. Encrypt (MSG,X)

Reading from the cloud,

ABE. Decrypt (C,{Sk,u})

3.2 Cryptographic Key Assumption

Symmetric-Key Encryption (SKE). These techniques, e.g., AES, are usually efficient but introduce complexity in EHR systems as additional mechanisms are required to apply access control. In particular, all healthcare providers use one shared key for encryption and decryption; thus, if the shared key is compromised, all EHRs are compromised the Public-Key Encryption (PKE). These techniques, e.g., RSA, provide a secure solution but are not practical for secure EHR storage due to the requirement for an expensive public-key infrastructure (PKI) to be maintained for distributing and managing public keys and digital certificates for all healthcare providers.

3.2.1 Attribute Key Assumption

The group key distribution schemes has recently received a lot of attention from the researchers, as a method enabling large and dynamic groups of users to establish group keys over unreliable network for secure multicast communication. Every user, belonging to the group, computes the group key using the message and some private information. The main property of the scheme is that, if some broadcast message gets lost, then users are still capable of recovering the group key for that session. The message they received at the beginning of a previous session and the message they will receive at the beginning of a subsequent one, without requesting additional transmission from the Group Manager. This approach decreases the workload on the Group Manager and reduces network traffic as well as the risk of user exposure through traffic analysis.

3.2.2 Key Distribution

Common group key is frequently updated to ensure secure multicast communication. Group lifetime is dived into epochs called sessions; single key instance is valid only throughout one session. Group membership can change between consecutive sessions. At the beginning of session GM distributes a new session key to nodes. Session duration is determined by the GM. It can vary over time, depending on security policy, group membership changes and nodes' behavior. Session key changes have to be performed, with some predefined minimum frequency to protect the system from cryptanalysis attacks. The choice of session length is a tradeoff between key distribution cost in terms of communication and computational overhead, and the required security level.

3.3 Key Issuing Secured Access

Escrow-Free Key Issuing Protocol for CP-ABE The KGC and the data-storing center are involved in the user key issuing protocol. In the protocol, a user is required to contact the two parties before getting a set of keys. The KGC is responsible for authenticating a user and issuing attribute keys to him if the user is entitled to the attributes. The secret key is generated through the secure 2PC protocol between the KGC and the data-storing center. They engage in the arithmetic secure 2PC protocol with master secret keys of their own, and issue independent key components to a user. The secure 2PC protocol deters them from knowing each other's master secrets so that none of them can generate the whole secret keys of a user alone.

3.4 Security Analysis

Security architecture satisfies the security requirements for authentication, data integrity, and confidentiality, which follows directly from the employment of the standard cryptographic primitives, namely digital signature, message authentication code, and encryption, in our system. The fraud can be repudiated only if the client can provide a different representation he knows of from the trusted authority (TA).

IV. IMPLEMENTATION

Its key generation procedure is modified for our purpose of removing escrow. The proposed scheme is then built on this new CP-ABE variation by further integrating it into the proxy reencryption protocol for the user revocation. To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group which is related to TPA permission generated code, since otherwise revocation cannot take effect after all. This setting where the data-storing center knows the revocation list does not violate the security requirements. It is only allowed to re encrypt the cipher texts with authentication and can by no means obtain any information about the attribute keys of users only accessed by valid users.

This section gives the details and specification of the hardware on which the system is expected to work. The CloudSim is an advanced tool to simulate the integration of Java coding. The processor will be Dual core 2 GHz with 2 GB RAM and 120 GB hard disk. The operating system is Windows XP. Java coding are easy to implement and CloudSim is freeware.

V.FIGURES

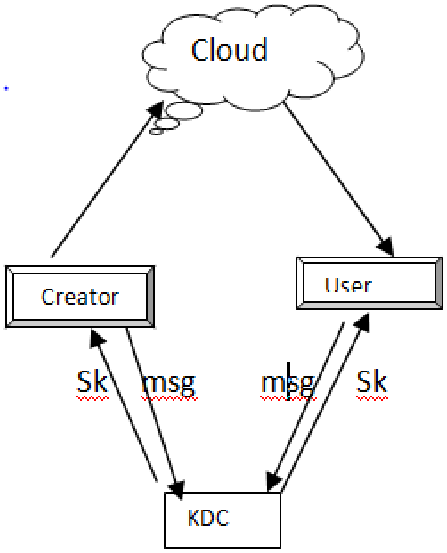

FIGURE .1 Data Storage in Cloud

VI. CONCLUSION

We have presented the Key Policy Attribute Based Encryption scheme, which provides more secure and fine-grained data access control in the system. It will be efficient and scalable to securely manage user data in the system. For key distribution the KDC is used. It is also helpful to secure data from the unauthorized users and auditors. The challenging problem is the construction of KP-ABE scheme with constant ciphertext size and constant private key size

REFERENCES

[1]. S. Ruj, M. Stojmenovic, and A. Nayak,” Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds”, IEEE transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.

[2] S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” Proc.IEEE/ACM Int’l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[3]. Mohamed Nabeel, Member, IEEE, Ning Shang, and Elisa Bertino, Fellow, IEEE,” Privacy Preserving Policy-Based Content Sharing in Public Clouds” IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 11, November 2013.

[4]. A.B. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,” Proc. Ann. Int’l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.

[5]. S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc.14th Int’l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[6]. Changji Wang and Jianfa Luo,” An Efficient Key-Policy Attribute-Based Encryption Scheme withConstant Ciphertext Length”, Hindawi Publishing Corporation Mathematical Problems in Engineering, Volume 2013, Article ID 810969, 7 pages.

[7]. Junbeom Hur and Dong Kun Noh,” Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems”, IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 7, July 2011.

[8]. Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng,” Attribute-Based Encryption With Verifiable Outsourced Decryption”, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 8, August 2013.

[9]. Fuchun Guo, Yi Mu,Willy Susilo,Duncan S. Wong, and Vijay Varadharajan,"CP-ABE With Constant-Size Keys for Lightweight Devices”, IEEE Transactions on Information Forensics and Security, Vol. 9, No. 5, May 2014.

[10].Piotr K. Tysowski and M. Anwarul Hasan,” Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds,” IEEE Transactions on Cloud Computing, Vol. 1, No. 2, July-December 2013.

[11]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou,” Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption”, IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 1, January 2013.

[12]. Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang,” Securely Outsourcing Attribute-Based Encryption with Checkability”, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 8, August 2014.

[13]. John Bethencourt , Amit Sahai and Brent Waters,” Ciphertext-Policy Attribute-Based Encryption”.