Capability of Certificateless Cryptography for Secure Data Sharing Over the Network

Pushpalata Gondake\textsuperscript{1}, Pallavi Khandagale\textsuperscript{2}, Vidya Tanpure\textsuperscript{3}, Prof. S. K. Said\textsuperscript{4}
\textsuperscript{1,2,3}Student, JCOE, Department Of Computer Engineering, Kuran
\textsuperscript{4}Professor, JCOE, Department Of Computer Engineering, Kuran

Abstract: The network is act as a medium for cloud computing provides the facility of data storage and access for cloud users. Network is widely used service model for storage. Outsourcing the data to a third party causes safety issue of sensitive data. The mediated certificateless encryption (mCL-PKE) scheme solves the key escrow problem and certificate revocation problem. mCL-PKE scheme does not utilize paring operations. Since most CL-PKC schemes are based on bilinear pairing and are computationally expensive. The security mediator acts as a policy enforcement point as well and supports instantaneous revocation of compromised or malicious users. It is more efficient than the pairing based scheme. By applying mCL-PKE scheme can construct a practical solution to the problem of sharing sensitive information in the public network. According to the access control, the data owner was encrypt a semantic encryption algorithm and uploads the encrypted data items and encrypted data encryption key in to the network. Upon successful authorization, the network partially decrypts the encrypted data for the users. The confidentiality of the content and the keys is preserved with respect to the network, because the network cannot fully decrypt the information.

1. Introduction

Recently Cloud computing is most widely used service model for storage i.e. Storage as a service that enables user to share their data in public cloud. Public cloud storage model should solve the critical issue of data confidentiality that data only accessed by authorized users. Shared sensitive data must be strongly secured from unauthorized access over the clouds. But security issue is most significant concern to protect data in the cloud. In order to assure confidentiality of sensitive data stored in public clouds, a commonly used approach is to encrypt the data before uploading it to the cloud.

In our public network/database the practical solution to the problem is applied using our scheme. We study and implemented an efficient certificateless encryption for secure data sharing over the network. The network is employed as a secure storage as well as a key generation centre.

Since network does not know the keys that we are used to encrypt the data, the confidentiality of data from network storage is assured. There are many security methods already existing to provide the security. Security mechanisms are used to provide authentication, confidentiality and integration services in the cloud environment. Main security mechanism comes under any of these two categories: Symmetric key mechanism and Asymmetric key mechanism. Fine grained encryption access control of the data is processed with the symmetric key based method. Symmetric key based mechanisms have various problems as handling uniqueness of keys, which in turn incurs high key management cost. A traditional public key cryptosystem requires a trusted Certificate Authority to issue digital certificates that bind users to their public keys. But this certificate management is very costly and complex [8]. To address certificate management issue new system as Identity Based Public Key cryptosystem (IB-PKC) was introduced but it had a key escrow problem which means the key generation
server knows the private keys of a user. So this scheme not safe to assure users privacy. Attribute Based Encryption provide the flexibility for the user to encrypt every data item based upon their access control policy. But it also had the revocation problem because the private key provided to the existing users has to be updated whenever a user dynamic changes. Al-Riyami and Paterson developed a new mechanism called Certificateless Public Key Cryptography (CL-PKC). Next the Certificate less Proxy Re-Encryption mechanism was introduced for secure data sharing in public cloud. This mechanism is based on CL-PKC to remove the key escrow problem and certificate management issue although uses pairing operation. To address above problem the concept of mediated cryptography has been used which support immediate revocation. Mechanism of mediated cryptography makes a practical and effective use of security mediator (SEM). Security mediator can control security capabilities for every transaction. The user's participation in a transaction will stopped immediately, once the SEM is been notified that a user's public key should be revoked. A notation of security mediated certificateless cryptography is introduced to present a mCL-PKE which depends upon the pairing operations, the computational costs required for pairing are still considerably high. If user applies the basic mCL-PKE scheme to the cloud computing environment or many users access the same data, the cost of encryption becomes high for data owner.

In this situation data owner should encrypt the data content with the same encryption key for multiple times. To remove this difficulty, the basic mCL-PKE scheme with an extension had been introduced. The extended scheme makes the data owner to apply the data encryption key process only once not multiple times like previous scheme which in turns provides some added information to the network. So with use of this additional information the authorized users can decrypt their content using the private keys. This scheme is similar to that of the Proxy ReEncryption (PRE) in which the encryption key is encrypted using the data owner’s public key and continue later to decrypt using different private keys. In this extension scheme, network does not perform any transformation it simply acts as the storage model. The security models of the existing schemes are insecure against partial decryption attack. So secure mediated CL-PKE without pairings is needed. The idea behind this scheme is that data owner encrypts the data and after encryption process sends the encrypted data over the network. Then the network partial decrypts the encrypted document and it to the requested users. The user, then fully decrypt the data content using their private keys. The extremely important thing is that, if more than one user are accepted and they want to get the access to same document then encryption rate will be enormously high for data owner since owner has to encrypt the same document several times for different users using the user’s public key in previous mediated Certificateless public key encryption scheme. To overcome this difficulty the extended mCL-PKE system is, data owner encrypts the data only one time and sends the extra information to the network for certified users to decrypt the data. But in this proposed system there is no need of extra information for the user to decrypt the encrypted data.

**Objectives:**
1. To obtain the efficient performance and higher level of security.
2. To avoid expensive pairing operation.
3. To avoid the vulnerable against partial decryption attacks.
4. Use the mCL-PKE scheme without any certificate authority.

**Existing System:**
The widespread adoption of cloud storage services the public cloud storage module should solve the critical issue of the data confidentiality. In order to secure confidentiality of sensitive data stored in public clouds, the commonly adopted approach is to encrypt the data before uploading is to the cloud. Since the cloud does not encrypt the keys send to encrypt the data, the confidentiality of the data from is arrived. In existing system, certificateless encryption is for secure data sharing is perform in a public cloud.

**Drawback Of Existing System:**
1. Even though the key decryption based approaches reduce the number of keys to be manage symmetric key based mechanisms is generated here the problem of high costs for key management.
2. In addition to the key escrow problem, ABE has the revocation problem as the private keys given to existing users should be updated whenever a user is revoked.
3. Moreover, their scheme only achieves Chosen Plaintext Attack (CPA) security. As pointed out, CPA security is often not sufficient to guarantee security in general protocol settings. For example, CPA is not sufficient for many applications such as encrypted email forwarding and secure data sharing that require security against Chosen Cipher text Attack.

**2. Literature Review**

Literature survey is the most important step in software development process. The existing Attribute-Based Encryption (ABE), which is one effective and promising technique. The technique is used to provide fine-grained access control to data in...
the Cloud environment. Attribute-Based Encryption is an access control mechanism where a User to encrypt each data item based upon their access control policy. Access to data in the Cloud was provided through Access Control Lists (ACLs), so this was not scalable and only provided coarse-grained access to data.

Tu S, Niu S, Li H, Xiao-ming Y, Li M [4] proposed a CP-ABE in the context of enterprise applications and also developed a revocation mechanism that allows high adaptability, fine-grained access control and revocation. The assigns users a set of attributes within their secret key and also distributes the secret key to the respective users. If user satisfies the access control policy defined by the data collaborator than he can access the data. The scheme is proven to be semantically secure against chosen cipher text attacks against the CP-ABE model. The scheme is not good in the case of user revocation because the updating of cipher texts after user revocation places heavy computation overhead even if the burden is transferred to the Cloud.

Dan Boneh [5], proposed an identity based cryptography scheme with the use of pairing. This scheme removes the need of certificate authority to manage the certificate. To encrypt a message intended for the entity described with the identity string. Identity based cryptography doesn't solve the revocation difficulty. To manage this problem in identity-based cryptography, short validity periods could be encoded into the identity string. However, this doesn't fit an environment where immediate revocation could be required.

D. Boneh, X. Ding, and G. Tsudik [7], presented the concept of mediated cryptography to support immediate revocation. Mediated cryptography removes the revocation problem. The basic idea of the mediated cryptography is to utilize a security mediator which can control security capabilities for every transaction. If the security mediator is notified that a user’s public key should be revoked, it can stop the user’s participation in a transaction.

3. Problem Statement

The confidentiality of the content and the keys is preserved with respect to the network, because the network cannot fully decrypt the information. To improve the efficiency of the encryption we propose an extension to our approach.

In order to assure confidentiality of sensitive data stored in public networks, we propose Certificateless mCL-PKE for secure data sharing without pairing operations and vulnerable against partial decryption attack and confidentiality of information, security, performance.

CL-PRE (Certificateless Proxy Re-Encryption) scheme for secure data sharing in public network environments. Although their scheme implement me is based on CL-PKC to solve the key escrow problem and certificate management, it relies on pairing operations. We have proposed the aes-128-256 scheme without pairing operations and provided its formal security. Our aes-128-256 solves the key escrow problem and revocation problem. Using the AES-128-256 scheme as a key building block, we proposed an improved approach to securely share sensitive data in our database. Our approach supports immediate revocation and assures the confidentiality of the data stored in an untrusted database while enforcing the access control policies of the data owner.

4. Proposed Work

In order to reduce the overhead of key management, an alternative is to use a public key cryptosystem. However a traditional public key cryptosystem require a trusted Certificate Authority to initiate digital certificates like that bind to share public keys. Because the CA has to generate its own signature on each users public key and manage each users certificate, the overall certificate management is very expensive and complex. To address such shortcoming, the Based public key cryptosystem (mCL-PKC) was introduced, but it arrives from the key encrypt problems on that key generation server learns the private keys of all users.

In order to address the key encrypt problem in IB-PKC, Al-Riyami and Paterson introduces a new cryptosystem called Certificateless Public Key Cryptography (CL-PKC). The Certificate less Proxy Re-Encryption mechanism was introduced for secure data sharing in public network. This mechanism is based on CL-PKC to remove the key escrow problem and certificate management issue although uses pairing operation. To address above problem the concept of mediated cryptography has been used which support immediate revocation. Mechanism of mediated cryptography makes a practical and effective use of security mediator (SEM).
Each user first generates its own private and public key pair, called PK and PubK, using the SetPrivateKey and SetPublicKey operations respectively using our mCLPKE scheme. The user then sends its public keys and its identity (ID) to the KGC in the network. The KGC generates two keys for the user. One key, referred to as SEM-key, is stored at the SEM in the network. The other key, referred to as User-key, is given to the user. The data owner obtains the KGC-keys of users from the KGC in the network. The data owner then encrypts each data item for which the same access control policy applies using a key K and then the data owner encrypts K using the KGC-keys of users. The encrypted data is uploaded to the network. When a user wants to read some data, it sends a request to the SEM to obtain the partially decrypted data. The SEM first checks if the user is in the access control list and if yes then user’s KGC-key encrypted content is available in the network storage. If the verification is successful, the SEM retrieves the encrypted content from the network and partially decrypts the content using the SEM-key for the user. The partial decryption at the SEM reduces the load on users. The user uses its SK and U-key to fully decrypt the data.

**Figure 2. Data flow structure of proposed scheme**

**Advantages Of Proposed System:**
1. Our system that is mCL-PKE scheme does not depend on the pairing-based operation, it provide security proof.
2. It reduces the computational overhead.
3. Key Generation Center only needs to be semi-trusted and can reside in the public network, because our mCL-PKE scheme does not suffer from the key escrow problem.

**System Entities:**
There are five entities in our system: the data owner, users, the Security Mediator (SEM), the Key Generation Center (KGC), and the storage service. The SEM, KGC, and the storage service are semi-trusted and reside in a public network.

1. Data Owner-Data owner encrypt the sensitive data using public key and upload it on network.
2. User-User encrypt and decrypt the data over a network. After successful authorization, network partially decrypt the encrypted data and user can get the fully decrypted using their private keys.
3. Encrypted storage-Upload the data at encrypted storage that is on a network.
4. Key generation centre-Generated the key for getting the data.
5. Security Mediator

**Algorithm:**
AES encryption algorithm is used to provide security in public network because AES is considered secure. Encryption and decryption time taken by AES is minimum as compared to others. So it is fastest block cipher algorithm amongst all analyzed cipher algorithms such as blowfish, DES, triple DES.

Advanced Encryption Standard i.e. AES 128 bit block consist of following steps:
1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (ciphertext).

**Working Of AES:**

Following steps gives detail working of AES algorithm over a network.

1. **Key Expansion**  
   Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. **Initial Round**  
   Add Round Key- each byte of the state is combined with a block of the round key using bitwise XOR.

3. **Rounds**  
   - **A. SubBytes** - non-linear substitution step where each byte is replaced with another.
   - **B. ShiftRows** - A transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   - **C. MixColumns** - A mixing operation which operates on the columns of the state, combining the four bytes in each column.
   - **D. AddRoundKey**

4. **Final Round (no Mix Columns)**  
   - A. SubBytes
   - B. ShiftRows
   - C. AddRoundKey.

5. **Conclusion**

   A traditional public key cryptosystem requires a trusted Certificate Authority (CA) to issue digital certificates that bind users to their public keys. Because the CA has to generate its own signature on each user’s public key and manage each user’s certificate, the overall certificate management is very expensive & complex. To address such shortcomings, and to obtain high security to the cloud data over a network, and to improve the efficiency of the encryption. We propose an extension to our approach. We propose our mCL-PKE scheme, the overall network based system, evaluates its security and performance. It will be much less costlier, less complex and strictly secure security mechanism to deal with network security issues. We proposed an improved approach to securely share sensitive data in our database. Our approach supports immediate revocation and assures the confidentiality of the data stored in an untrusted database while enforcing the access control policies of the data owner.

6. **Acknowledgement**

   We express our sincere thanks to our project guide Prof. S. K. Said who always being with presence & constant, constructive criticism to made this paper. We would also like to thank all the staff of COMPUTER DEPARTMENT for their valuable guidance, suggestion and support through the project work, who has given co-operation for the project with personal attention. Above all we express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during project work. At the last we thankfull to our friends, colleagues for the inspirational help provided to us through a project work.

7. **References**


   [9] Sushmita Ruj, CSE, Indian Institute of Technology, Indore, India, Milos Stojmenovic, Singidunum University, Belgrade, Serbia, Amiya
