A Survey Paper on Certificate-Less Encryption for Secure Data Sharing

Ankita Gavade[1] Pooja Patil[2] Sangita Patil[3] Prof.Sheetal Thakare[4]
[1,2,3,4]Bharati Vidyapeeth College of Engineering Navi Mumbai, India

Abstract— Internet has widely grown in the recent century and become the necessity. The public is increasingly concerned about the proper use of information, particularly personal data. The threats to information systems from criminals and terrorists are increasing. Many organizations will identify information as an area of their operation that needs to be protected as part of their system of internal control. The certificate-less encryption solves the key escrow problem which is one of the serious in identity based encryption & certificate revocation problem in asymmetric cryptography. Existing certificate-less encryption schemes are inefficient because of the use of expensive pairing operations, so to address the performance & security issues, certificate-less encryption scheme without using paring operation is proposed and also it gives a practical solution to the problem of sharing sensitive information.

Key words: Certificate-less Encryption, Identity based encryption, key escrow problem

I. INTRODUCTION

Data sharing is way to share the same data with multiple machines or users via any communication medium/channel. Data sharing is fundamental feature of database management system .Everyone gets benefits, including funding agencies, investigators, & most mainly the Public. It provides efficient use of limited resources by avoiding unwanted repetition of data collection.

Due to the benefits of secure storage, organizations have been adopting secure services. That is, shared sensitive data must be strongly secured from unauthorized accesses. In order to assure confidentiality of sensitive data stored, a commonly adopted approach is to encrypt the data before uploading it to the system storage. A typical approach used to support encryption based access control is to encrypt different sets of data items to which the same access control policy applies with different symmetric keys and give users either the relevant keys or the ability to derive the keys.[2]

In day to day life security becomes a major issue in IT world. Cryptography is a technique to prevent unauthorized user to access confidential data. It convert original data into unreadable format (Encrypted format). Many organizations focuses on secure storage of their confidential data. Certificate-less public key encryption scheme provide secure sharing of files within protected environment. It can be applicable in Government agencies, banking, Business organizations. The major goals of this system are:

- It is user- friendly and easy to use for users.
- The Users can keep their data on secure storage.
- The users can download or view their data from Storage system[1].

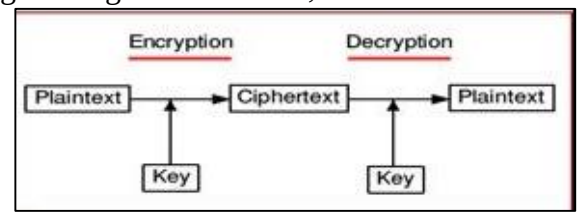

Fig. 1: Cryptography [2]

II. BACKGROUND

The Existing Methodologies that are overcome by using certificateless encryption scheme are listed as follows:

A. Identity-Based Public Key Cryptosystem:

An Identity-based cryptosystem is a novel type of cryptographic scheme proposed by Shamir [2], which enables any pair of users to communicate securely, and to verify each other's signatures without exchanging public or private keys, without keeping any key directories and without using the services of any third party. Problems with the traditional Public key cryptosystems (PKCs) are the high cost of the infrastructure needed to manage and authenticate public keys, and the difficulty in managing multiple communities. Whilst ID-based PKCs will not replace the conventional Public Key infrastructures, it might prove to be a complementary technology[1].

Many attempts have been made to deal with the public key authentication issue. Kohnfelder [5] used the RSA digital signature scheme to provide public key certification. His system involves two kinds of public key cryptography: one is in modulo p, where p is a large prime number; the other is in modulo N, where N = p ⋆ q, and p and q are large primes. Blom [7] proposed a symmetric key generation system (SKGS) based on secret sharing schemes. The problems of SKGS however, are the difficulty of choosing a suitable threshold value and the requirement of large memory space for storing the secret shadow of each user. In 1984, Shamir [1] introduced the concept of an identity. In this system, each user needs to visit a Key authentication center (KAC) and identify him self before joining the network. Once a user's identity is accepted, the KAC will provide him with a secret key. In this way, a user needs only to know the "identity" of his communication partner and the public key of the KAC, together with his secret key, to communicate with others. There is no public file required in this system. However, Shamir did not succeed in constructing an identity-based cryptosystem, but only in constructing an identity-based signature scheme. Since then, much research has been devoted, especially in Japan, to various kinds of identity-based cryptographic schemes. Okamoto et al. [6] proposed an identity-based key distribution system in 1988, and later, Ohta [12] extended their scheme for user identification. These schemes use the RSA public key cryptosystem [13] for operations in modular N, where N is a product of two large primes, and the security of these schemes is based on the computational difficulty of factoring this large composite number N. Tsujii and Itoh [2] have also proposed an identity-based cryptosystem based on the discrete logarithm problem

with single discrete exponent which uses the ElGamal NEW IDENTITY-BASED CRYPTOGRAPHIC SCHEME... 67 public key cryptosystem.

B. Attribute Based Encryption:

An attribute based encryption scheme introduced by Sahai and Waters in 2005 and the goal is to provide security and access control. Attribute-based encryption (ABE) is a public-key based one to many encryption that allows users to encrypt and decrypt data based on user attributes. In which the secret key of a user and the cipher-text are dependent upon attributes (e.g. the country she lives, or the kind of subscription she 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. Decryption is only possible when the number of matching is at least a threshold value d. Collusion-resistance is crucial security feature of Attribute-Based Encryption .An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it use the access of monotonic attributes to control user's access in the system.[5]

Method Name	ID-Based PKC	Attribute based Encryption
Advantages	1.Key revocation lose. 2.The authenticity of the public keys is guaranteed implicitly as long as the transport of the private keys to the corresponding user is kept secure (Authenticity, Integrity, Confidentiality)	1.To reduce the communication overhead of the Internet. 2.To provide a fine-grained access control.
Disadvantags	1.It suffers from the key escrow problem as the key generation server learns the private keys of all users. 2.The Private Key Generator (PKG) generates private keys for users, it may decrypt and/or sign any message without authorization. 3.It introduces a key-management problem where all users must have the most recent public key for the server.	1.ABE has the revocation problem as the private keys given to existing users should be updated whenever a user is revoked. 2.It suffers from the key escrow problem as the key generation server learns the private keys of all users.

Table 1: Advantages and disadvantages of existing methods

III. CERTIFICATE-LESS ENCRYPTION

The main difficulty today in developing secure systems based on public key cryptography is not the problem of choosing appropriately secure algorithms or implementing those algorithms. Rather, it is the deployment and management of infrastructures to support the authenticity of cryptographic keys: there is a need to provide an assurance to the user about the relationship between a public key and the identity (or authority) of the holder of the corresponding private key. In a traditional Public Key Infrastructure (PKI), this assurance is delivered in the form of certificate, essentially a signature by a Certification Authority (CA) on a public key [5]. Encryption is the solution for the security . There are many encryption techniques. Each one has its own merits and demerits. In the case of identity based encryption it is free from security mediator, predefined keys are there, and have the problem of key escrow and certificate revocation. Then the arrival of mediated certificate-less scheme eliminates the key escrow problem, and certificate revocation problem. In certificate-less encryption scheme, key generation process is divided in between the user and the storage system. In this system data owner encrypt the data using its secret key. Then the data owner encrypt the secret key twice. Hence formed intermediate keys. Then send this encrypted data and intermediate keys to storage system. The storage system partially decrypt the intermediate key and send partially decrypted data and encrypted data to required user. The user decrypt the partialy decrypted data. Then the user will get the required key for decryption. so the user can decrypt it completly.The main advantage of system is, the data owner can send same data to multiple clients with minimum cost.[2].

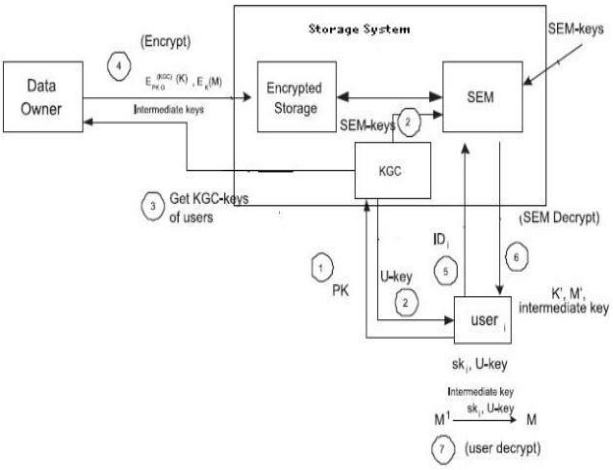

Fig. 2: System Architecture[1]

The system architecture consists of three major parts namely Data Owner, Storage system & User. The architecture displays the basic process flow.

1) The Data Owner Module :The data owner possesses sensitive content that wants to share with authorized users.
2) The User Module :If a user is revoked, the data owner updates the access control list at the SEM so that future access requests by the user are denied.
3) Storage System : It consist of Security Mediator (SEM) and Key Generation Center (KGC) that generates public/private key pairs for each user.

AES: The AES algorithm defined by the National Institute of Standards and Technology (NIST) of the United States has been widely accepted to replace DES as the new symmetric encryption algorithm [8]. The AES algorithm is a symmetric block cipher. It processes data blocks of 128 bits using a cipher key of length 128, 192, or 256 bits. Each data block consists of a 4 × 4 array of bytes called the state, on which the basic operations of the AES algorithm are performed [8].The proposed algorithm differs from conventional AES as it has 200 bits block size and key size both. Number of rounds is constant and equal to ten in this algorithm. The key expansion and substitution box generation are done in the same way as in conventional AES block cipher. AES has 10 rounds for 128-bit keys, and 12 rounds for 192-bit keys, and 14 rounds for 256- bit keys [9]. The AES algorithm is not only use for security purpose but it also improves the performance of the system as well as hardware resources.

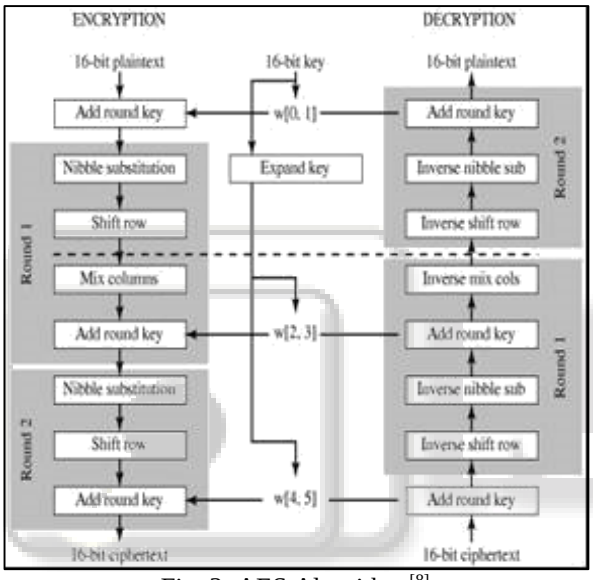

Fig. 3: AES Algorithm [8]

A. RSA:

The algorithm RSA, at present is the most successful use for ciphering keys and passwords or counts. The key long varies from 64 to 1024 bits [15]. It has the advantage to be strong in the break if the key is rather long and on the other hand, it does not need to pass on the key deprived via the network to the receiver. The principle of encoding is based on an acquisition of the image followed by a compression then a segmentation in blocks of L pixels (in normal mode L = 8 pixels or 64 bits).

It is encrypted into cipher text with a cryptographic algorithm, which will in turn be decrypted into usable plaintext. In symmetric cryptography single key is used for encryption and decryption e.g. Data Encryption Standard (DES) and Advanced Encryption Standards (AES).In asymmetric algorithm different keys are used to encrypt and decrypt the data.RSA is widely used in electronic ecommerce protocols. With sufficiently long keys and the use of up-to-date implementations; RSA is believed to be totally secure. There are two ways in which we can achieve security 1.encrypted file transfer 2.Strong secure protocol for transmission of files. RSA (Rivest, Shamir & Adleman) is asymmetric cryptographic algorithm developed in 1977. It generates two keys: public key for encryption and private key to decrypt message [2].

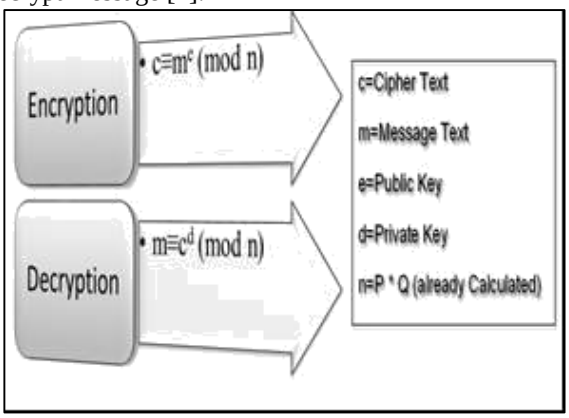

Fig. 4: RSA Algorithm [15]

RSA algorithm consist of three phases, phase one is key generation which is to be used as key to encrypt and decrypt data, second phase is encryption, where actual process of conversion of plaintext to cipher text is being carried out and third phase is decryption, where encrypted text is converted in to plain text at other side. As a public key is used for encryption and is well known to everyone and with the help of public key, hacker can use brute force method to find private key which is used to decrypt message. Secure RSA prevents files from hackers and help safe transmission of files from one end to other [14].

Method Name	Certificate-less Encryption
Advantages	1.Hybrid encryption is considered a highly secure type of encryption. 2. Key escrow problem and Certificate revocation problem is solved 3.Partial decryption attacks is not possible. 4.The system can share the data with high security. 5.This methodology does not depend on the pairing-based operation, it reduces the computational overhead .
Disadvantages	1.To decrypt the data user needs to use only their private key.

Table 2: Advantages of certificate-less encryption

IV. CONCLUSION

Using the Certificate-less encryption scheme as a key building block, this is an improved approach to securely share sensitive data. Approach assures the confidentiality of the data stored in an untrusted public storage system while enforcing the access control policies of the data owner. The improved approach performs only a single encryption of each data item and reduces the overall overhead at the data owner.

REFERENCES

[1] Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE,"An Efficient Certificate-less Encryption for Secure Data Sharing" Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 9, SEPTEMBER 2014
[2] S. Tsujii, and T. Itoh, An ID-Based Cryptosystem based on the Discrete Logarithm Problem, IEEE Jounral on selected areas in communications, 7 (1989), 467-473
– Shamir, Identity based cryptosystems and signature schemes. Advances in Cryptology – Proceedings of Crypto'84.
[3] V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89{98, 2006}
[4] X. W. Lei Xu and X. Zhang, "CL-PKE: A certificate-less proxy re-encryption scheme for secure data sharing with public cloud," in ACM Symp. Inform. Comput. Commun. Security, 2012.
[5] J. Dankers et al. Public key infrastructure in mobile systems. IEE Electronics and Commucation Engineering Journal, 14(5):180–190, 2002.
[6] C. Adams and S. Lloyd. Understanding Public-Key Infrastructure – Concepts, Standards, and Deployment Considerations. Macmillan, Indianapolis, USA, 1999.
[7] P. Gutmann. PKI: It's not dead, just resting. IEEE Computer, 35(8):41–49, 2002.
[8] Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang, and Cheng-Wen Wu, National Tsing Hua University,"A high throughput low cost AES processor" IEEE Communications Magazine 0163-6804/03 © 2003 IEEE.
[9] Navraj Khatri, Rajeev Dhanda , Jagtar Singh ,"Comparison of power consumption and strict avalanche criteria at encryption/Decryption side of Different AES standards''International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 4, August 2012.
[10] J.C.Borie, W.Puech, M.Dumas, " Encrypted Medical Images for Secure Tranfer". International Conference on Diagnostic Imaging and Analysis ICDIA 2002, Shanghai,August 2002, pages 250-255.
[11] K. Ohta, Efficient identification and signature schemes, Electron. Lett., 24(2) (1988), 115-116.
[12] J. Gordon, Strong RSA keys, Electron. Letter, 20, No. 12 (14984), 51-516.
[13] Xin Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", IEEE, 6th International Forum on Strategic Technology, pp- 1118 – 1121
[14] Eun- Jun Yoon, Kee –Young Yoo, "An Efficient Diffie – Hellman – MAC Key Exchange Scheme" IEEE, Fourth International Conference on Innovative Computing , Information and Control , pp 398 – 400, 2009.

