Public Key Encryption: A Survey

Banazir B

Computer Science, MES College of Engineering, Kuttipuram, Malappuram Dist, Kerala, India

Abstract*: Public key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key are mathematically linked. Public key Cryptography system uses different cryptographic techniques for encryption and decryption. Survey five techniques and analyzed the performance. Technique includes Public Key Infrastructure, Identity Based Cryptography, Certificateless Cryptography, Certificate Based Cryptography, Attribute Based Cryptography.*

Keywords: Public key Infrastructure, Identity Based Cryptography**,** Certificate based cryptography**,** Attribute Based Encryption.

1. Introduction

Security experts around the world have been researched for many years on how to build a safe and reliable network environment, and the studies involved different levels of security technologies and measures. Among them, the public key infrastructure (PKI) [1] has solved the majority of network security issues. The PKI platform provides security services for users to secure communication. PKI based on uniform standards and norms is the key technology of information security. In the process of deploying PKI, there are many problems to be solved. In order to promote the disadvantages of PKI, Israeli scientist's Shamir proposed identity based cryptography (IBC) theory [2] in 1984. In this theory public key can be uniquely identify any strings of the user's identity such as e-mail address, IP address and so on.

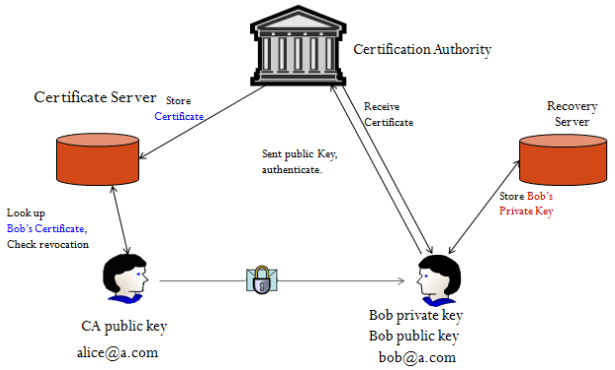
Private Key can be gotten from trusted third party secure access to the private key generator. In IBC key escrow issue exists since PKG is able to find any user's private key, that is compromised PKG. In order to overcome this issue a new paradigm which is certificate less public key cryptography [3] is introduced in which the private key is partially determined by the key generating centre (KGC). A strong security model for certifcate less public key encryption was established Al Riyami and Peterson in 2003. Certificate based encryption (CBE) [4] was introduced by Gentry. The private key selected by the user and the up to date certificate issued by the CA using an IBE. The certificate acts not only one part of the decryption key but also a traditional public key certificate. User's certificate not kept secret. In Cipher text policy attribute based encryption (CP- ABE) [5] the data is encrypted under an access policy defined by a user who encrypts the data and a user secret key is associated with a set of attributes which identify the user. A user can decrypt the cipher text if and only if his attribute satisfy the access policy. In CP- ABE, since the user enforces the access policy moves with the encrypted data. This is important for data storage servers, where data confidentiality must be preserved or untrusted. Attribute based encryption algorithm may suffer from various drawback. In terms of efficiency, cipher text are not length preserving and are in general not efficiently searchable. So proposed a searching method.

2. Related Works

2.1 Public Key Infrastructure (PKI)

In public key infrastructure (PKI) systems [1], a certificate is used to bind an encryption key to a user identity (such as an email address) via a registration process. When this process is tightly controlled and combined with digital signing technologies, the certificate can give a strong assurance that only the indicated user can access messages encrypted with The key contained in the certificate. To communicate securely to a certificate holder, a potential sender (who also must have a certificate) needs to obtain the certificate of the recipient, and then use it to encrypt the message. PKI, particularly in combination with smartcards, can provide robust user authentication and strong digital signatures. When strong controls are enacted around certificate registration, and when user's private keys are well protected from compromise (i.e., stored on a smartcard), certificates enable strong authentication. PKI seems to be an ideal mechanism for enabling encryption as well, but a few significant hurdles present themselves. First, there is the pre-enrollment problem. Here recipients must already have a certificate before they can be sent a message. Second, the sender must obtain the certificate of the recipient, which is generally published via a directory, this introduces problems of trust (does the sender trust the issuer of the recipients certificate) and information leakage (has the directory given spammers and phishes a source of fully qualified email addresses). Finally, while the binding between certificate and identity was true at the time of issuance, there is no guarantee that it remains true after that single point in time. This means that senders must first confirm the validity of recipient's certificates before sending, this is the certificate revocation problem. Even if certificates can be found for all recipients, the validity of these certificates must be determined before a message can be sent. Typical approaches for checking certificate status have been to publish CRLs (certificate revocation lists), which must be frequently updated, or stand up high volume OCSP (online certificate status protocol) servers, which must be accessed by every sender before every send. In either case, senders must be on-line to obtain current information, or to send to recipients with whom they have not previously communicated. Users will always be entering and leaving systems, permissions will change, and private key compromises will occur, anytime any of these events

happens, all other users will need to be informed via one of the indicated mechanisms. And in the real world, both in the public and private sector, communications must often be secured to recipients who do not even have certificates to begin with. PKI is suited for providing strong authenticating mechanism for providing the full range of message security services.



Advantages:

- Strong authentication of users (especially with Smart cards)

Disadvantages:

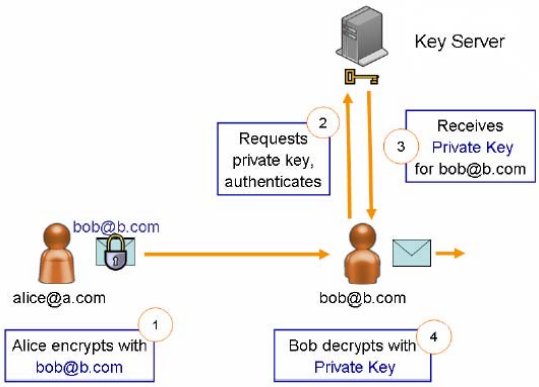
- Users (senders AND recipients) must be pre-enrolled. Certificate directories can leak critical information.

2.2 Identity Based Cryptography (IBC)

With Identity Based Cryptography (IBC) [2], identities (such as email addresses) are used as encryption keys. Any user can communicate with any other user by using the recipients email address as the encryption (or public) key. Decryption (or private) keys are generated by a Public Key Generator from a server master secret. These keys can be re-generated at any time, thus decryption keys need never be archived or stored. These basic properties allow for a secure messaging environment where no users require certificates, and users need know nothing other than their email addresses. This design immediately eliminates both the problems of pre-enrollment, as well as that of certificate revocation checking. Using IBC, when the canonical Alice needs to communicate securely with Bob, all Alice needs to do is encrypt a message using Bobs email address, bob@b. com as the public key. Once Bob receives the message, he needs to obtain the associated private key for decryption. To do so, Bob contacts the Public Key Generator and requests the private key for bob@b. com. The Public Key Generator authenticates Bob as required by policy (perhaps by requiring that he have a smartcard stored certificate, or by prompting for a password). Once Bob is successfully authenticated, the Public Key Generator generates the required decryption key and sends it to Bob. Bob can then decrypt and view his message.

Advantages:

- Provides simple, easy to use encryption.
- Requires no user pre-enrollment for senders or receipts
- Support exible authentication mechanism.



- Extends messaging to all users, not just those with certificates.
- Provides automatic key recovery.
- Integrate easily with boundary messaging services.
- Inexpensive to operate.

Disadvantages:

- Inherent key escrow, PKG requires extremely high levels of assurance.

2.3 Ciphertext policy attribute based encryption (CP-ABE)

Attribute-based encryption (ABE), as introduced by Sahai and Waters, allows for fine grained access control on encrypted data. In its key-policy (the dual cipher text-policy scenario proceeds the other way around), the primitive enables senders to encrypt messages under a set of attributes and private keys are associated with access structures that specify which cipher texts the key holder will be allowed to decrypt. These results were extended by Goyal et al. [6] into richer kinds of attribute-based encryption, where decryption is permitted when the attribute set satisfies a more complex Boolean formula specified by an access structure. Since ABE is the generalization of IBE, every arbitrary string is utilized as a valid public key for an attribute. The trusted authority, called the key generation center (KGC), is responsible for the generation of private keys for every user after user authentications. The KGC generates private keys for users by applying the KGCs master secret keys to their associated set of attributes. Thus, the major benefit of this approach is to largely reduce the need for processing and storage of public key certificates under traditional public key infrastructure (PKI). CP-ABE scheme consist of four fundamental algorithms. Setup, KeyGen, Encrypt, and Decrypt. In setup phase, setup the public parameter PK and a master key MK. In the key generation phase generate the secret key based on set of attributes and master key. In the encryption phase message is encrypted with access policies and public key. And produce a cipher text. In decryption phase decrypted by using private key and access structure, and returns a message.

2.4 Certificateless Public Key Encryption (CLE):

In 2003, Al-Riyami and Paterson proposed a new type of encryption scheme that avoids the draw backs of both traditional public key encryption and identity-based encryption. They termed this new type of encryption

certificate less public-key encryption (CL-PKE) [3] because their encryption scheme did not require a public key infrastructure. Roughly speaking, their idea was to combine the functionality of a public key scheme with that of an identity based scheme. Hence, to encrypt a message, a sender requires both the receiver's identity and a public key value produced by the receiver. Similarly, to decrypt a cipher text, a receiver requires the partial private key corresponding to their identity (which is given to them by a key generation centre) and the private key corresponding to the distributed public key. It has seven fundamental algorithms. Such as Setup, secret value generation, public key generation, Partial private key, set private key, encryption, and decryption. In setup phase it returns the master key and system parameters. Secret value is set by based on input parameter corresponding secret value is obtained. Partial private key is extracted by master key and id. Private key is set by partial secret key and private value. In encrypted phase, message is encrypted by master public key and user's id. And decrypted by Private key and public key parameters.

Advantages:
- Reduce the processing time, Support flexible authentication mechanism, Support automatic key recovery.

Disadvantages:
- Denial of decryption attack.

2.5 Certificate Based Encryption (CBE)

Certificate less public key encryption (CLE) and certificate based encryption (CBE) [4] are two novel public key cryptographic primitives requiring no authenticity verification of the recipient's public key. Both of them are motivated to simultaneously solve the heavy certificate management problem inherent in the traditional public key encryption (PKE) and the key escrow problem inherent in the identity-based encryption (IBE). It is an attractive cryptographic task to formally explore the relation between CBE and CLE. In 2005, Al-Riyami and Paterson proposed one general conversion from CLE to CBE. Shortly later, Kang and Park pointed out a law in the security proof of Al-Riyami-Paterson conversion. In 2012, Wu et al. proposed another generic conversion from CLE to CBE. Compared with Al-Riyami-Paterson conversion [5], Wu et al.s method can be proved secure, but it has to additionally involve collision resistant hash functions. It remains an open problem whether the generic conversion due to Al-Riyami and Paterson, which is very neat, is provably secure. We aim to solve this open problem. First, we formalize CLEs new security model, featured by introducing a new security property overlooked by previous security models. With this new security model as the basic technique, we succeed in proving that the Al-Riyami-Paterson generic conversion from CLE to CBE is secure .Certificate-based encryption (CBE) is a new public key encryption mechanism introduced by Gentry. As in the traditional PKI, each client in CBE generates its own public/private key pair and the Certificate Authority (CA) then generates a certificate which can guarantee the authenticity of the client's public key. In CBE, the certificate has an additional feature, namely it also acts a partial private key. A (IBC) successful decryption requires both the private key and the up-to-date certificate. This provides an implicit verification of one's certificate and eliminates third-party queries for certificate status required in traditional PKI. Since CA does not know the clients private key, there is no key escrow problem in CBE. It has six fundamental algorithms. Such as setup, setup key pair, certification, Consolidate, Encrypt and decrypt. In set up phase set the security parameter returns the master key and system parameters. Key pair is generated from input parameter and output the public key and secret key. Certify by using master key, security parameters and producing the client identifying information and public key.

Advantages:
- Certificate management. Certification revocation list is not needed. No key escrow.

Disadvantages:
- Certificate can leak the critical information.

3. Observation and Analysis

Comparison of various schemes for public key encryption can be shown the tables. There compare the different Cryptographic techniques based on different parameters. In these observations we can conclude that attribute based encryption techniques are better than others. By implementing these techniques with the fuzzy key word search techniques [8]. It will increase the efficiency of Encryption schemes.

Scheme	*Key Escrow*	*Complexity*	*Key Recovery*	*Cost*	*Security*
PKI	No	High	Yes	High	High
IBC	Yes	Low	No	Low	Medium
CLE	No	Medium	No	Medium	Medium
CBE	No	Medium	No	High	High
CP-ABE	No	Medium	No	Medium	High

Scheme	*Trusted Authority*	*Public Key*	*Brute Force Attack*	*Denial of Decryption Attack*	*Collision Attack*
PKI	CA	Key	No	No	No
IBC	PKG	Identity	No	No	Yes
CLE	PPK	Arbitrary	No	Yes	Yes
CBE	CA	Key	No	No	No
CP-ABE	KGC	Attribute	Yes	No	No

4. Conclusion And Future Work

Analyzed about the public key cryptography system[1]-[6] which is based on Public key infrastructure, identity encryption, Certificate less public key encryption, Certificate based encryption and Cipher text policy attribute-based encryption. Based on security Cipher text Policy Attribute based Encryption is better than others. Attribute based encryption schemes suffer from various drawbacks. In terms of efficiency, cipher text are not length preserving. So difficult for searching. These properties severely limit the deployment of public key encryption schemes in [9] application involving massive data sets where the cipher text expansion ratio is crucial. It is solved by public key

encryption with oblivious keyword search and committed blind anonymous identity based encryption. Another problem based on security. In CP- ABE scheme present Certification Authority (CA), Who is responsible for issuing unique key. If CA is compromised, it can affect security. It can be avoided by Decentralizing [7] the CP- ABE scheme.

References

[4] David C. Yen Sean Lancaster and Shi-Ming Huang, "Public Key Infrastructure: a micro and macro analysis. "Computer standard Interfaces,25(5):437-446, jun2003.

[5] Taiping Mo, Jianhua Wang, and Wei Mo., "Design of secure communication network system based on data encryption and digital signature," in High performance computing and stimulation,2011 International conference on, pages 626-630,july.

[6] Sattam S. Alriyami and Kenneth G. Peterson, "Certificate less public key cryptography," Advances in Cryptology-ASI-ACRYPT, Springer Berlin Heidelberg, 2894(10):452{473, 2003.

[7] Meixue Hong Jiguo Li, Xinyi Huang and Yichen Zhang, "Certificate based signcryption with enhanced security features."computer mathematics with application, 58(1): 1587-1601, Jan 2012.

[8] David Galindo, Paz Morillo, and Carla Rfols," Improved certificate based encryption in the standard model," Journals of system and software, 81(7): 1218-1226, 2008.

[9] Nuttapong Attrapadung, Javier Herranz, Fabien, Laguillaumie, Benot Libert, Elie de Panafleu and carla R fols," Attribute-based encryption schemes with constant-size ciphertexts," Theoretical computer science, 422(0): 15-38, 2012.

[10] Jinguang Han, W. Susilo, Yi Mu, and Jun Yan, "Privacy-preserving decentralized key policy attribute based encryption, "Parallel and distributed system, IEEE Transactions on, 23(11):2150, Nov.

[11] Xu, P. and Jin, H. and Wu, Q. and Wang, W, "Public key encryption with fuzzy keyword search : a provably secure scheme under keyword guessing attacks, "computer IEEE transactions ,2012,doi : 10.11

[12] 09/TC.2012.215.

[13] Jan Camenisch, Markulf Kohlweiss, Alfredo Rial, and Caroline Sheedy, "Blind and anonymous identity-based encryption and Authorized private searches on public key encrypted data," Public key cryptography PKC 2009, volume 5443 of lecture note in computer science, pages 196-214, Springer Berlin HeidelbErg, 2009.

Author Profile

Banazir B has received his B-Tech degree in Information Technology from Amrita Institute of Technology and Science, Kollam. Presently she is M-Tech student of MES College of Engineering, Kuttipuram. Her research interest in cryptography.