International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

A Cryptographic Framework for Secure Cloud Data Retrieval Using Certificate less Encryption

K Sundara Rao

Lecturer in Computer Applications, Department of Computer Application
Government Degree College, Mandapeta, East Godavari Dist. Andhra Pradesh
INDIA

Abstract

Searchable Public Key Encryption (SPKE) is an important cryptographic technique that enables users to perform keyword searches over encrypted data stored on an untrusted server while preserving the confidentiality of both the data and the search queries. However, many existing SPKE schemes require a secure communication channel and suffer from security vulnerabilities such as keyword guessing attacks. To address these issues, certificate-based cryptography (CBC) has been introduced as an effective public key cryptographic primitive that lies between Identity-Based Cryptography (IBC) and traditional Public Key Cryptography (PKC). In a CBC system, a user first generates a pair of public and private keys independently and then submits identity information along with the public key to a trusted Certificate Authority (CA) to obtain a certificate. Unlike traditional PKI certificates, the certificate in CBC acts as a partial decryption or signing key that is only available to its owner. Consequently, a user must combine the private key and the certificate to perform decryption or signing operations. This mechanism simplifies certificate management, eliminates third-party certificate status verification, and avoids key escrow problems because the CA does not possess the user's full private key.Searchable Public Key Encryption extends traditional public key encryption by allowing a server to test whether encrypted data contains specific keywords without revealing the underlying plain text or the search keywords.n this paper, we propose a new framework called **Certificate-Based Searchable Public Key Encryption (CB-SPKE)**, inspired by certificate-based cryptography and signcryption techniques. The proposed framework enhances security against keyword guessing attacks while providing advantages such as implicit authentication, elimination of key escrow, and removal of the requirement for secure communication channels. Furthermore, a concrete CB-SPKE scheme is developed and analyzed. Security analysis in the random oracle model demonstrates that the scheme satisfies ciphertext indistinguishability and trapdoor privacy under adaptive keyword attacks. Comparative evaluation shows that the proposed scheme is both secure and practical for real-world applications such as encrypted email systems, secure cloud storage, electronic healthcare systems, and Internet of Things (IoT) environments. Below is a rewritten, well-structured "Proposed System" section suitable for a journal or project report, with clear academic language and supporting diagrams placed where they are most appropriate.

Key Words: Cryptographic, Public keyEncription, Decription, Pravate Key,Certificate Based,Searchbale.

1. Proposed System

Overview of the Proposed System

The proposed system extends the concept of **Searchable Public Key Encryption (SPKE)** within the framework of **Certificate-Based Cryptography (CBC)** to develop a new framework called **Certificate-Based Searchable Encryption (CBSE)**. The CBSE framework combines the advantages of searchable encryption and certificate-based cryptography to provide secure and efficient keyword search over encrypted cloud data.

Unlike many traditional SPKE frameworks, the proposed CBSE system eliminates the need for a **secure communication channel** between the sender and receiver. Additionally, the framework avoids the requirement of a **designated storage server** for performing search operations. Instead, any cloud storage server can securely perform the search operation without compromising data privacy.

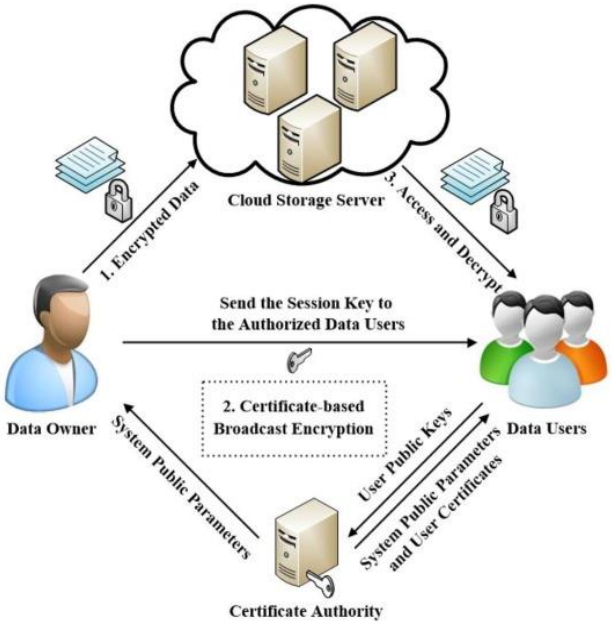
The proposed approach provides several advantages including:

- Resistance against **Keyword Guessing (KG) attacks**
- **Implicit authentication**
- **No key escrow problem**
- **No secure key distribution channel required**
- **Flexible cloud storage environment**

2. Architecture of the Proposed System

The proposed system architecture consists of five major entities:

1. **Certificate Authority (CA)**
2. **Sender (Data Owner)**
3. **Receiver (Data User)**
4. **Storage Server (Cloud Server)**
5. **Users**



The architecture shows how encrypted data and encrypted keywords are stored in the cloud server while allowing authorized users to perform secure searches without revealing sensitive information.

In this system, the **Certificate Authority (CA)** generates system parameters and certificates for users. The **Sender** encrypts data and associated keywords before uploading them to the cloud server. The **Receiver** generates a trapdoor (search token) to retrieve encrypted files containing the desired keywords. The **Cloud Server** performs the search operation and returns the matching encrypted results without learning the actual data or keywords.

Searchable encryption allows encrypted data stored in cloud servers to be queried securely using search tokens generated from secret keys. This approach prevents unauthorized access while enabling efficient data retrieval.

3. Functional Modules of the Proposed System

T1 User Registration Module

The user must first register in the system through a registration interface. After successful registration, the user receives login credentials. If the user has already registered, they can directly log in to the system using their username and password.

The registration information is stored securely in the system database.

2 Sender Module (Data Owner)

The sender is responsible for uploading sensitive data files into the cloud storage server.

Before uploading the data, the sender performs the following operations:

1. Generate encrypted data using public key encryption.

2. Generate encrypted keywords associated with the data.
3. Upload both the encrypted data and encrypted keyword index to the cloud server.

This ensures that the cloud server stores only **encrypted data**, preventing unauthorized access.

3 Storage Server Module

The storage server acts as the cloud infrastructure that stores encrypted data and keyword indexes uploaded by senders.

The storage server performs the following tasks:

- Stores encrypted files securely.
- Receives search trapdoors from receivers.
- Executes the keyword matching algorithm.
- Returns the matching encrypted files.

The server performs search operations **without decrypting the data**, thereby preserving privacy.

4 Receiver Module

The receiver is the authorized user who wants to retrieve encrypted files from the cloud server.

The receiver performs the following operations:

1. Generate a **trapdoor (search token)** using a secret key.
2. Send the trapdoor to the cloud server.
3. Receive encrypted search results.
4. Decrypt the retrieved files using the private key.

Only authorized receivers possessing the correct secret key can decrypt the returned data.

5 Certificate Authority (CA) Module

The Certificate Authority plays an important role in maintaining system security.

The CA performs the following operations:

- Generates system parameters
- Generates master secret keys
- Issues certificates to users
- Manages public and private key generation
- Monitors malicious activities and attackers

The CA ensures secure communication and trust among all entities in the system.

In certificate-based cryptography, certificates serve as partial cryptographic keys that must be combined with user private keys to perform encryption or decryption operations.

4. Security Mechanism Against Keyword Guessing Attacks

Many traditional SPKE frameworks suffer from **Keyword Guessing (KG) attacks** because attackers can generate possible keywords and test them against encrypted keyword ciphertexts.

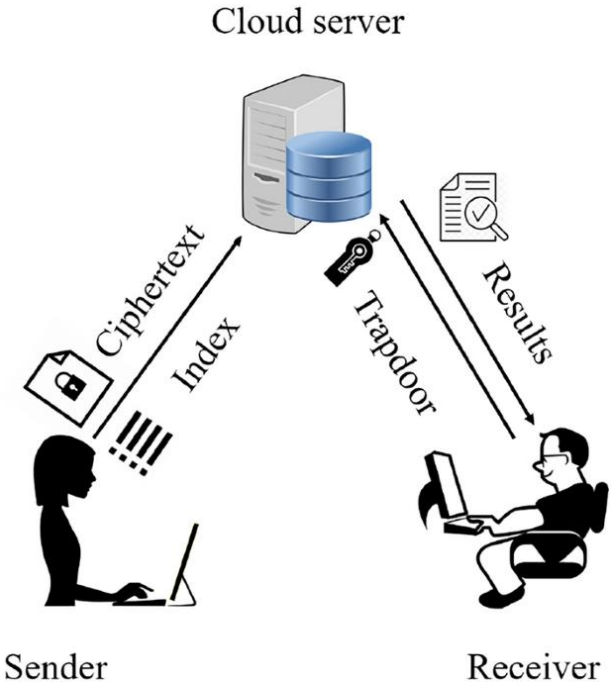
To overcome this problem, the proposed CBSE framework introduces **signcryption techniques**. In this approach, the sender's private key is used along with the receiver's public key to generate the encrypted keyword.

Because the sender's private key is known only to the sender, attackers cannot generate valid keyword ciphertexts. As a result, both malicious storage servers and external attackers cannot perform keyword guessing attacks.

Thus, the proposed framework provides stronger protection against both:

- **Outside attackers**
- **Malicious cloud servers**

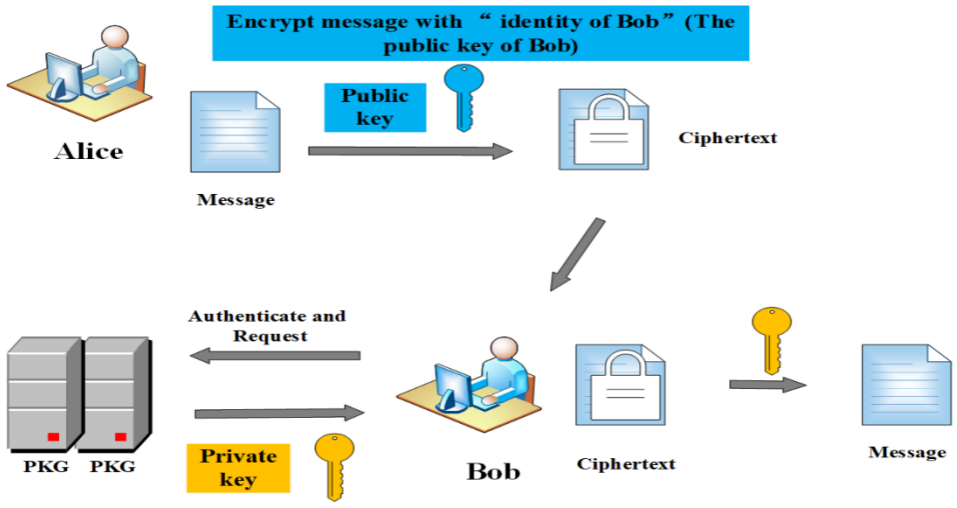
5. Working Process of the Proposed System



The process includes the following steps:

1. The sender encrypts the data and keywords.
2. The encrypted data and keyword index are uploaded to the cloud server.
3. The receiver generates a search trapdoor using a secret key.
4. The trapdoor is sent to the cloud server.
5. The cloud server performs a search over encrypted data.
6. The server returns matching encrypted files to the receiver.
7. The receiver decrypts the retrieved files.

This approach ensures that **data privacy and keyword privacy are preserved throughout the search process**.



References

1. A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. CRYPTO 1984, pp. 47-53, 1984.
2. S.S. Al-Riyami, K.G. Paterson, "Certificateless public key cryptography," Proc. ASIACRYPT 2003, pp. 452-473, 2003.
3. C. Gentry, "Certificate-based encryption and the certificate revocation problem," Proc. EUROCRYPT 2003, pp. 272-293, 2003.
4. W. Wu, Y. Mu, W. Susilo, X. Huang, L.Xu, "A provably secure construction of certificate-based encryption from certificateless encryption," The Computer Journal, vol. 55, no. 10, pp. 1157-1168, 2012.
5. Y. Lu and J. Li, "A provably secure certificate-based encryption scheme secure against malicious CA attacks in the standard model," Information Sciences, vol. 372, pp. 745-757, 2016.
6. Y. Lu and J. Li, "A pairing-free certificate- based proxy reencryption scheme for secure data sharing in public clouds," Future Generation Computer Systems, vol. 62, pp. 140-147, 2016.