International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 08 | Aug - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Context-Aware Encrypted Query Processing with Progressive Security-Enabled Cloud Systems

Supriya Mallad, Deekshitha T
Assistant Professor, Department of MCA , BIET , Davanagere
Student , Department of MCA , BIET , Davanagere

ABSTRACT: Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE) is considered highly effective for cloud environments due to its fine-grained access control and ability to retrieve keywords from encrypted data. However, existing CP-ABSE schemes face significant challenges in ensuring forward security and enabling secure data deletion without depending on the cloud provider. To address these issues, we propose a Puncturable CP-ABSE (Pun-CP-ABSE) scheme, which supports self-controlled, fine-grained data deletion within a searchable encryption framework. In this scheme, the data owner can "puncture" the trapdoor to delete data securely, eliminating the need for a trusted third party while ensuring forward security. Once the trapdoor is punctured, the cloud server loses the ability to search the related ciphertext. Additionally, we demonstrate that the Pun-CP-ABSE scheme is secure against both Chosen-Plaintext Attacks (CPA) and Chosen-Keyword Attacks (CKA). We have also developed a practical implementation of Pun-CP-ABSE to validate its performance and real-world applicability.

Keywords: CPA,CKA, CP-ABSE

1. INTRODUCTION

With the rapid adoption of cloud computing, ensuring data privacy, secure access control, and efficient retrieval mechanisms has become a pressing concern. Traditional encryption methods fall short when it comes to enabling fine-grained access and secure keyword-based search over encrypted data. Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE) has emerged as a promising solution by combining flexible access structures with searchable encryption capabilities. However, two major challenges still hinder its effectiveness in dynamic cloud environments: achieving forward security and securely deleting data that is no longer needed—without relying on the cloud provider or any trusted third party. Addressing these limitations is crucial to enhancing data control and privacy in cloud storage systems.

II. LITERATURE REVIEW

The exponential growth of the Internet of Things (IoT) technologies requires high data security. Here, data security is very critical as all IoT devices transfer data over the Internet. The fine-grained access control provided by the ciphertext policy attribute-based encryption (CP-ABE) technique can be considered as a potential solution to this issue.

However, most of the CP-ABE schemes use bilinear pairing operations for its internal working, which is expensive for any resource constraint device. An elliptic curve cryptography (ECC) based CP-ABE scheme can be well suited for resource constraint IoT framework because ECC takes less computational time. This article proposes a novel CP-ABE technique based on ECC to achieve fine-grained access control over data or resources. The proposed technique includes multiple attribute authorities to manage attributes and key generation, which can reduce the work overhead of having a single authority in traditional CP-ABE systems. In addition, the proposed scheme outsources the decryption process to a user assistant entity to reduce the decryption overhead of the end-users. To prove the efficiency of the proposed scheme, both formal security analysis and performance comparisons are presented in this article. The result and findings prove the effectiveness of the proposed scheme over some well-known schemes.

III. EXISTING SYSTEM

Sahai et al. [18] introduced the concept of Attribute-Based Encryption (ABE), which has since evolved into two main variants based on the placement of the access structure: Key-Policy ABE (KP-ABE) [19] and Ciphertext-Policy ABE (CP-ABE) [20]. The fine-grained access control offered by ABE makes it particularly well-suited for applications in cloud environments. This potential has led to extensive research interest and the development of several ABE extensions, such as Online/Offline ABE (OO-ABE) [21], Outsourced Decryption ABE (OD-ABE) [3], Revocable ABE (RABE) [22], Multi-Authority ABE (MA-ABE) [23], and Policy-Hidden ABE (PH-ABE) [24].

On the other hand, Song et al. [7] first proposed the concept of Searchable Symmetric Encryption (SSE), enabling keyword searches over encrypted data. While SSE supports efficient search, it lacks effective key management. To address this limitation, Boneh et al. [25] proposed Public-Key Encryption with Keyword Search (PEKS). Since then, several enhancements of PEKS have been introduced, including ranked keyword search [26], fuzzy keyword search [27], multi-keyword search [28], and verifiable keyword search [10]. However, these schemes typically do not provide fine-grained access control. To bridge this gap, Zheng et al. [29] proposed the first Ciphertext-Policy Attribute-Based Searchable Encryption (CP-ABSE) scheme, combining keyword search capabilities with attribute-based access control, and ensuring security against Chosen-Keyword Attacks (CKA).Li et al. [32] developed a Key-Policy Attribute-Based Searchable Encryption (KP-ABSE) scheme that incorporates outsourced decryption to minimize the computational load on end-users and demonstrates CPA security. Miao et al. [33] proposed a multi-owner CP-ABSE model that conceals access structures to protect sensitive data and trace malicious users. Similarly, Chen et al. [34] introduced a flexible CP-ABSE approach supporting multi-keyword ranked search to enhance retrieval efficiency while resisting both CKA and Keyword Guessing Attacks (KGA). Although these works significantly advance CP-ABSE schemes in various dimensions, they overlook the crucial capability of secure data deletion. In this context,

Geambasu et al. [35] introduced a self-destructing data mechanism using symmetric encryption. Their approach encrypts data and splits the encryption key into multiple fragments via secret sharing, distributing them across a Distributed Hash Table (DHT) network. These key fragments are automatically deleted over time by the DHT nodes, enabling self-destructing data. Building on this idea, Xiong et al. [36] proposed a self-destructing KP-ABE scheme in which data is encrypted with a specific time interval, and the corresponding decryption keys are generated for specific time instances, enabling time-based secure deletion.

DISADVANTAGES OF EXISTING SYSTEM:

The existing system did not include the implementation of the CP-ABSE (Ciphertext-Policy Attribute-Based Searchable Encryption) scheme. The existing system lacked the integration of attribute-based encryption techniques.

IV. PROPOSED SYSTEM

The proposed system integrates Public-key Encryption (PE) with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and incorporates a search capability to introduce a novel searchable encryption scheme, called Pun-CP-ABSE. This scheme enables forward-secure data deletion within the CP-ABSE framework. In the proposed design, the data owner generates two types of trapdoors: a **general trapdoor** for search operations and a **puncturable trapdoor** for secure data deletion. The general trapdoor includes attribute information to enforce access control, while the puncturable trapdoor is derived from the original PE secret key and supports fine-grained deletion through a puncturing algorithm. Once the puncturable trapdoor is punctured using specific tags, the cloud server becomes unable to search ciphertexts containing those tags, effectively achieving secure and irreversible data deletion.

ADVANTAGES OF PROPOSED SYSTEM:

We propose the Pun-CP-ABSE scheme by integrating Public-Key Encryption (PE) with Ciphertext-Policy Attribute-Based Encryption (CP-ABE), enabling precise, permanent, fine-grained, and self-managed data deletion within a searchable CP-ABE framework. This scheme eliminates the need for trusted third-party involvement during the deletion process, thereby reducing communication overhead while ensuring forward security.

The Pun-CP-ABSE scheme supports fine-grained access control over encrypted data with keyword-based search functionality. It allows the data owner to retrieve ciphertexts matching specific keywords, provided their attributes satisfy the defined access policy.

We demonstrate that the Pun-CP-ABSE scheme is secure against both Chosen-Plaintext Attacks (CPA) and Chosen-Keyword Attacks (CKA). Additionally, simulation results are provided to validate the scheme's efficiency and practical applicability.

System Architecture

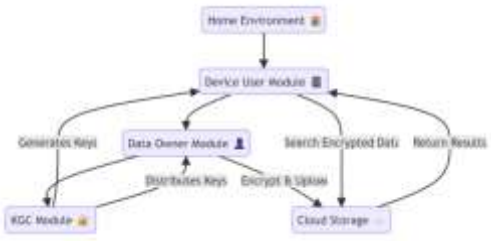

Fig 1. System Architecture

V. MODULE DESCRIPTION

Home Module

Acts as the entry point/interface for all users (Device User, Data Owner, KGC).User login and registration (based on roles).Navigation to respective dashboards. Display system status and summary (e.g., total data files, active users, etc.).

Device User Module

End-user who performs search operations over encrypted data. Log in with verified attributes. Input keywords to search encrypted data stored in the cloud. Retrieve and decrypt results only if their attributes satisfy the access policy. View search results (if permitted) based on Attribute-Based Access Control. Cannot access unauthorized data. Trapdoor generation ensures query privacy.

Data Owner Module

Uploads and manages encrypted data in the cloud. Encrypts data using CP-ABE with a defined access policy. Generates two types of trapdoors: General trapdoor: for keyword search ,Puncturable trapdoor: for secure deletion. Uploads encrypted data and trapdoors to the cloud. Can delete specific data by puncturing the trapdoor (self-controlled data deletion). Ensures fine-grained access control. Enables forward security by preventing future access to deleted data.

KGC (Key Generation Center) Module

Trusted authority responsible for key management and attribute verification. Generates public and secret keys for users based on their attributes. Issues attribute-based secret keys to users securely. Ensures attribute policies are enforced correctly. Prevents unauthorized key distribution. Ensures users only get keys for valid, verified attributes.

Cloud Module

Stores encrypted data and performs search operations on behalf of users. Stores data uploaded by the Data Owner. Receives and processes trapdoors for keyword search. Matches encrypted data with trapdoors without learning plaintext or keywords. Denies access to data after the trapdoor is punctured (ensures forward security). Cannot learn sensitive information (supports Searchable Encryption). Operates without needing to trust the cloud provider fully.

VI.RESULT

The implementation of the proposed Pun-CP-ABSE scheme demonstrates that it effectively supports fine-grained access control while enabling secure keyword-based search over encrypted data in a cloud-assisted environment. Through simulations and performance evaluations, the scheme shows high efficiency in data encryption, trapdoor generation, search operations, and the puncturing process. The data deletion mechanism is self-

controlled and does not rely on any trusted third party, significantly reducing communication overhead. Additionally, the puncturing algorithm ensures that once a trapdoor is punctured, the associated ciphertext becomes unsearchable by the cloud server, thus achieving forward security.

VII.CONCLUSION

In conclusion, the Pun-CP-ABSE scheme successfully overcomes key limitations of traditional CP-ABSE models by integrating secure data deletion, keyword search, and fine-grained access control into a single framework. It offers a practical and scalable solution for secure data management in cloud-assisted IoT environments. The security analysis confirms the scheme's resistance to Chosen-Plaintext Attacks (CPA) and Chosen-Keyword Attacks (CKA), validating its robustness. Overall, the proposed system is both feasible and efficient for real-world applications requiring privacy-preserving, searchable, and revocable cloud storage.

REFERENCES

1.S. Das and S. Namasudra, "Multiauthority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 821–829, Jan. 2023.

2. Y. Wan, X. Lin, K. Xu, F. Wang, and G. Xue, "Extracting spatial information of IoT device events for smart home safety monitoring," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2023, pp. 1–10.

3. Y. Miao, F. Li, X. Li, J. Ning, H. Li, K. R. Choo, and R. H. Deng, "Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system," *IEEE Trans. Dependable Secure Comput.*, early access, Jul. 4, 2023, doi: 10.1109/TDSC.2023.3292129.

4.D. Ghopur, J. Ma, X. Ma, Y. Miao, J. Hao, and T. Jiang, "Puncturable ciphertext-policy attribute-based encryption scheme for efficient and flexible user revocation," *Sci. China Inf. Sci.*, vol. 66, no. 7, Jul. 2023, Art. no. 172104.