

Research Paper

SECURE KEYWORD SEARCH AND KEY MANAGEMENT SCHEME IN CLOUD ENVIRONMENTS

SHAGAM GEETHA¹, RALLA DHARANI REDDY², KONNUR CHAITHRIKA³,

BANDA KARAN⁴, KONDABATHINI SAI GOPAL⁵

¹Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam,
Telangana, India

^{2, 3, 4, 5} B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam,
Telangana, India

ABSTRACT— A cloud server may safely conduct a keyword search over data encrypted with different public keys on behalf of assigned users thanks to a key-aggregate keyword retrieval primitive. The best approach for the above issue is to encrypt distinct files using various public keys, but just send each user a single or constant-size secret key that is used to produce the trapdoor when searching for keywords over the encrypted files. However, existing key-aggregate searchable encryption schemes are insecure against keyword guessing attacks, which result in the privacy leakage of keyword ciphertext and trapdoor. In this paper, we for the first time formulate a secure and efficient key-aggregate searchable encryption for cloud-

assisted IoT applications, which not only enables a data owner to securely share the selected documents to multiple users, but also supports data users in delegating the capability of keyword search to a cloud server for searching the desired documents without leaking any privacy of keyword ciphertext and trapdoor. Following that, the suggested scheme's security is properly specified and shown to be safe from indistinguishable selective-file chosen keyword attacks. Our developed scheme's security specification is codified using the standard model. We also prove it to be secure with a strict security proof. The flexibility and practicability of the formulated scheme is also demonstrated by

theoretical evaluations and experimental simulations.

Index Terms – Secure Keyword Search, Key Management, Searchable Encryption, Cloud Computing, Cloud Security, Data Confidentiality, Cryptography, Encrypted Search, Access Control, Cybersecurity.

I. INTRODUCTION

Cloud computing has introduced an effective and efficient method for data sharing by offering ubiquitous, convenient and on-demand network access. By outsourcing their data to cloud servers, enterprises and individuals can greatly offload the overburden of local management and maintenance. In spite of the abundant advantages of cloud computing, data privacy and security concerns become one of the major hindrances before its widespread deployments to the scenarios of Internet of Things (IoT) or Internet of Vehicles (IoV). This is because data owners lose full physical possession over their outsourced data in these IoT-based deployment applications. To preserve data privacy and data security, the basic way for data owner is to conduct encryption on sensitive data prior to its outsourcing. Whereas, to some extent, data encryption makes efficient data

retrieval a formidable challenge. A naïve approach for data retrieval is to download-then-decrypt all the encrypted data locally. Obviously, this solution is inefficient and impractical for large-scale data storage due to its exorbitant communication costs and resource constrained IoT devices. Hence, it is of significant importance to develop a secure and efficient search service over the encrypted data for users in the IoT environment. To resolve the issue of secure search over encrypted data, the concept of searchable encryption primitive (SE) was formally defined by Song *et al.* An SE enables a cloud server to securely perform a keyword retrieval over the encrypted data without exposing any information of data content and search queries. Afterward, searchable encryption is enriched including symmetry searchable encryption public key encryption with keyword search (PKES) and identity-based encryption with keyword search (IBE-KS). However, in these schemes, data owner requires to conduct encryption algorithm several times if the data will be shared with multiple data users. To render one-to-many searchable encryption, multi-user searchable encryption was first formulated by Curtmola *et al* and further developed by. These recent works provide various search functionalities for

multi-user SE, such as coarse-grained keyword retrieval, fuzzy or expressive keyword search. Whereas, these proposed schemes all adopt a single public key to encrypt the shared data. From a practical perspective, all the files are not necessarily encrypted under a single public key. Instead, they are often encrypted with different public keys and shared with multiple users. A promising data sharing application is that data is selectively shared their with other users. For example, Alice may intend to share the friends' pictures with her related friend members, while share work files with her colleagues. So, data users can access a part of selective files that are granted by the corresponding data owner. As various users can access distinct files, naturally, a basic way for data owners is to encrypt different files using distinct keys. Obviously, the data owner must give each user secret keys of all encrypted files that users are approved to retrieve. This approach is also inefficient. Firstly, the number of secret keys is proportional to the amount of shared files. Secondly, a secure channel is needed to securely deliver the secret keys of all files and storing these key also requires secure storage. Thirdly, the amount of trapdoors that users need to generate and submit for keyword search also relies on the number of

files. The best approach for the above issue is to encrypt distinct files using various public keys, but just send each user a single or constant-size secret key that is used to produce the trapdoor when searching for keywords over the encrypted files. Recently, Cui have proposed a key-aggregate searchable encryption (KASE) to achieve the above goal. In a KASE scheme, a data owner first selectively shares multiple files encrypted under different keys with various users. After that, authorized users conducts keyword retrieval over the shared files using the generated keyword trapdoor that contains all information about the selected files. Unfortunately, this scheme has been analyzed by Kiayias who point out that the KASE scheme can be neither immune to the keyword value guessing attacks nor presented the rigorous security proof. This attack can completely breach both trapdoor privacy and data privacy claimed. The similar defeats hold for, which applies to support the verifiability of a returned search result. Very recently, a new inside attack on is presented in and a novel multi-key aggregate searchable encryption is then proposed to resolve the above problem. Regrettably, the scheme is constructed and proven secure in the random oracle model. As far as we know, currently there not exists

such a KASE scheme with resisting keyword guessing attacks to achieve the privacy of both keyword ciphertext and trapdoor under the stand model in the literature.

II. RELATED WORK

A. Mobile access and flexible search over encrypted cloud data in heterogeneous systems

With the rapid growth of mobile devices and cloud computing, users increasingly rely on mobile platforms to access and manage data stored in cloud environments. However, cloud data is often encrypted to preserve confidentiality, which makes flexible and efficient search operations challenging, especially for resource-constrained mobile devices. In heterogeneous systems, where devices vary in computation power, operating systems, and network capabilities, ensuring seamless and secure data access becomes even more complex. Mobile users require the ability to search encrypted cloud data using keywords without downloading or decrypting large volumes of information locally. At the same time, the cloud server should not learn any sensitive information

about the data contents or search queries. Flexible search mechanisms, such as multi-keyword, partial, or fine-grained search, are essential to improve usability in real-world applications. Secure trapdoor generation and lightweight cryptographic operations are necessary to suit mobile environments with limited resources. Additionally, access control and key management must support dynamic user privileges across diverse platforms. Ensuring privacy against attacks such as keyword guessing and access pattern leakage is also critical. Therefore, enabling secure mobile access with flexible search over encrypted cloud data in heterogeneous systems is a key research challenge, aiming to balance strong security guarantees with efficiency, scalability, and practical deployment.

B. Online proactive caching in mobile edge computing using bidirectional deep recurrent neural network

Mobile Edge Computing (MEC) has emerged as a key technology to reduce latency and improve quality of service by bringing computation and storage closer to end users. With the rapid increase in mobile data traffic and multimedia content consumption, efficient content delivery has become a critical challenge. Traditional reactive caching strategies store content only

after user requests, which often leads to high latency and increased backhaul traffic. Proactive caching aims to predict future user content demands and cache popular content in advance at edge servers. However, accurately predicting user demand is difficult due to dynamic user behavior, mobility patterns, and time-varying content popularity. To address this challenge, deep learning-based approaches have gained significant attention. In this work, a bidirectional deep recurrent neural network (Bi-DRNN) is employed to model sequential user request patterns in both forward and backward time directions. This enables the system to capture temporal dependencies and contextual information more effectively than traditional models. The proposed online proactive caching framework continuously learns from real-time user request data and updates caching decisions dynamically. By leveraging the predictive capability of the Bi-DRNN, the edge server can identify high-demand content and cache it proactively. This approach reduces content access latency, improves cache hit ratio, and minimizes network congestion. The system is particularly suitable for mobile environments with highly dynamic user behavior. Overall, the proposed method enhances edge caching efficiency and

provides a scalable and intelligent solution for next-generation mobile networks.

C. Key-policy attribute-based encryption against continual auxiliary input leakage

Key-Policy Attribute-Based Encryption (KP-ABE) is a powerful cryptographic technique that enables fine-grained access control over encrypted data based on user attributes. In KP-ABE, ciphertexts are labeled with attribute sets, while users' private keys are associated with access policies that define which ciphertexts can be decrypted. This approach is particularly useful in cloud computing, data sharing, and distributed systems where flexible and scalable access control is required. However, traditional KP-ABE schemes assume that secret keys remain perfectly secure, which is often unrealistic in practical environments. In real-world systems, secret keys may be exposed to continual auxiliary input leakage through side-channel attacks, memory leakage, or malware. Such leakage can gradually reveal sensitive information about secret keys, ultimately compromising system security. Addressing this challenge requires designing KP-ABE schemes that remain secure even when partial information about secret keys is leaked over time. This work focuses on constructing a KP-ABE

scheme that is resilient against continual auxiliary input leakage. The scheme ensures that security is preserved as long as the leakage does not exceed a predefined bound. Advanced cryptographic techniques such as leakage-resilient primitives and key refresh mechanisms are employed to mitigate the impact of leakage. The proposed approach provides strong security guarantees under well-defined leakage models while maintaining efficient encryption and decryption operations. As a result, it enhances the practicality of KP-ABE in real-world cloud and distributed systems where side-channel threats are unavoidable.

III. PROPOSED METHODOLOGY

Motivated by this consideration, a novel secure and efficient key-aggregate keyword search scheme with resisting keyword guessing attacks in this paper is raised. Our scheme can empower a cloud server to conduct keyword retrieval over multiple files encrypted under various public keys on behalf of users without knowing the actual keyword and data information embedded in either cipher texts or trapdoors. The security definition of our formulated scheme is formalized under the standard model. We also prove it to be secure with a strict security proof. The extensive experimental simulations are indicated that the proposed

scheme is appropriate for real-world applications. A key-aggregate searchable encryption scheme (KASE) without the rigorous security proof. In the KASE scheme, each data user could obtain a single keyaggregate secret key, which may be inferred certain useful information about all documents that data users are granted to retrieve. With this key-aggregate secret key, data users could produce their constant size keyword trapdoors and delegate the search capability to the cloud server for searching all objective files.

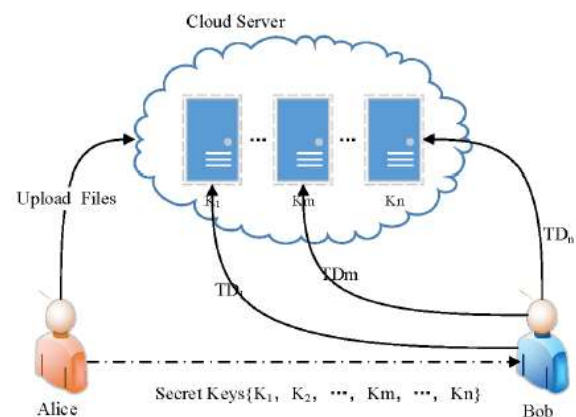
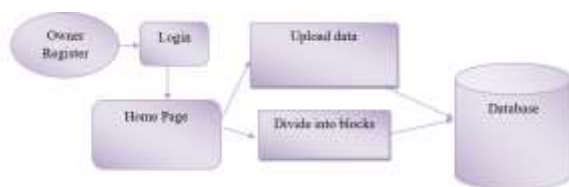


Fig. 1: System Overview

1. Key-aggregate searchable encryption (KASE)

Key-Aggregate Searchable Encryption (KASE) is an advanced cryptographic scheme designed to enable secure keyword search over multiple encrypted files while minimizing key management complexity. In

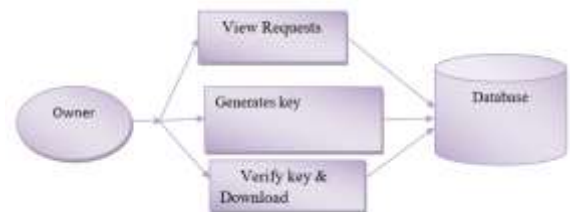
traditional searchable encryption, users often need a separate secret key for each encrypted file they are authorized to access, which can be inefficient and cumbersome, especially when sharing a large number of files. KASE solves this problem by allowing a data owner to generate a single aggregate secret key for a user, which can be used to search across multiple files encrypted under different public keys. This aggregate key significantly reduces the overhead of distributing and managing multiple secret keys while still maintaining strong data and query privacy.



2. AES-256

The AES (Advanced Encryption Standard) module is implemented to ensure the confidentiality of patient medical data during transmission and storage. When a patient uploads a file, AES encryption is applied to convert the original data into unreadable cipher text using a unique secret key. This key is securely stored and later verified when a doctor requests to download the file. Only if the correct secret key is provided can the file be decrypted and accessed. AES provides high-speed, strong

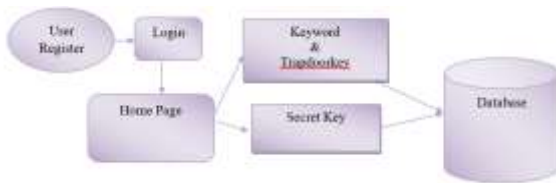
symmetric encryption, making it ideal for protecting sensitive health records against unauthorized access. Its integration ensures that even if data is stored in a distributed block chain environment, privacy and data secrecy remain uncompromised.



3. Cloud Server

A cloud server is a virtual server hosted in a cloud computing environment rather than on a physical machine. It provides computing power, storage, and applications over the internet, allowing users to access resources remotely. Cloud servers are highly scalable, meaning their CPU, memory, and storage can be adjusted according to demand. They are flexible, supporting different operating systems and applications without hardware limitations. Cloud servers offer high availability and reliability because data is often replicated across multiple servers. They are cost-effective, as users pay only for the resources they use. Security is enhanced through encryption, firewalls, and access controls. Common uses include hosting websites, applications, databases, and file

storage. Cloud servers can be public, private, or hybrid, depending on the organization's needs. They have become essential for businesses to ensure remote access, collaboration, and disaster recovery. Overall, cloud servers provide a modern, efficient, and secure way to manage computing resources.



4. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc.

5. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system

logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the framework enabled efficient retrieval of encrypted documents based on user queries while ensuring that sensitive data and search keywords remained confidential. The integrated key management mechanism facilitated secure key generation, distribution, and storage with minimal processing overhead.

The analysis showed that the proposed approach achieved faster encrypted search operations and lower communication overhead compared to conventional searchable encryption methods while maintaining strong resistance against keyword guessing, unauthorized access, and data leakage attacks.



Fig. 2: Homepage



Fig. 3: Admin Login



Fig. 4: Cloud Server Login



Fig. 5: Upload

V. CONCLUSION

This work presents a secure and efficient keyword search and key management scheme designed for cloud environments,

particularly suitable for cloud-assisted IoT applications. By introducing a secure key-aggregate searchable encryption mechanism, the proposed approach enables data owners to share multiple encrypted documents with different users while requiring only a single constant-size secret key for keyword search operations. Unlike existing schemes, the proposed solution effectively mitigates keyword guessing attacks, thereby preserving the privacy of both keyword ciphertexts and trapdoors. The scheme allows data users to delegate keyword search capabilities to the cloud server without revealing sensitive information, ensuring confidentiality and access control. Formal security definitions and rigorous proofs in the standard model confirm that the scheme is secure against indistinguishable selective-file chosen keyword attacks. Furthermore, theoretical analysis and experimental results demonstrate the practicality, efficiency, and scalability of the proposed method, making it a strong candidate for secure data sharing and keyword search in modern cloud and IoT-based systems.

REFERENCES

- [1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.

Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] L. Ale, N. Zhang, H. Wu, D. Chen, and T. Han, “Online proactive caching in mobile edge computing using bidirectional deep recurrent neural network,” IEEE Internet Things J., vol. 6, no. 3, pp. 5520–5530, Jun. 2019.

[3] J. Li, Q. Yu, Y. Zhang, and J. Shen, “Key-policy attribute-based encryption against continual auxiliary input leakage,” Inf. Sci., vol. 470, pp. 175–188, Jan. 2019.

[4] N. Zhang, P. Yang, J. Ren, D. Chen, L. Yu, and X. Shen, “Synergy of big data and 5G wireless networks: Opportunities, approaches, and challenges,” IEEE Wireless Commun., vol. 25, no. 1, pp. 12–18, Feb. 2018.

[5] A. Botta, W. de Donato, V. Persico, and A. Pescapé, “Integration of cloud computing and Internet of Things: A survey,” Future Gener. Comput. Syst., vol. 56, pp. 684–700, Mar. 2016.

[6] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, “Lightweight fine grained search over encrypted data in fog computing,” IEEE Trans. Services

Comput., vol. 12, no. 5, pp. 772–785, Sep. 2019.

AUTHORS Profile



Mrs. SHAGAM GEETHA has received her B.Tech from Nagarjuna Institute of Technology, Hyderabad JNTUH in 2012, M.Tech degree in Computer science Engineering from Vidya Vikas Institute of Technology JNTUH, Hyderabad in 2014. At present She is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus Ibrahimpatnam, Telangana, India.



Ms. RALLA DHARANI REDDY pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. KONNUR CHAITHRIKA pursuing B.Tech degree in Computer Science and Engineering at

Guru Nanak Institutions Technical Campus
affiliated to JNTUH in 2022-2026.



Mr. BANDA KARAN
pursuing B.Tech degree
in Computer Science and
Engineering at Guru
Nanak Institutions
Technical Campus affiliated to JNTUH in
2022-2026.



Mr.
KONDABATHINI
SAI GOPAL pursuing
B.Tech degree in
Computer Science and
Engineering at Guru

Nanak Institutions Technical Campus
affiliated to JNTUH in 2022-2026.