International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | March – 2026 DOI: 10.55041/ISJEM.ACME011
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Trusted Data Retrieval: A Verifiable Search Model for Multi-Tenant Applications

Yaddala Pavan Kalyan[1], Dr. Y. Ravi Kumar[2],

[1]P.G Scholar, Department of CSE, Sree Rama Engineering College, Tirupati, Andhra Pradesh, India, pavankalyanyaddala@gmail.com

[2]Professor, Department of CSE, Sree Rama Engineering College, Tirupati, Andhra Pradesh, India, Y.ravi@sreerama.ac.in

---

Abstract - This research proposes a Verifiable Search Model to address the critical security and privacy challenges of cross-tenant data retrieval in multi-tenant cloud environments. Traditional searchable encryption targets single-tenant architectures, lacking essential mechanisms for result verifiability and user accountability. To overcome these limitations, our objective is to facilitate secure, collaborative data sharing without compromising data confidentiality. The methodology integrates Elliptic Curve Cryptography (ECC) for lightweight data encryption and secure search token generation, alongside SHA-256 hashing for effective data deduplication and keyword index integrity. Furthermore, a partitioned inverted index is employed to process large-scale queries via fast parallel processing. Performance evaluations against standard RSA-based and sequential search techniques demonstrate that the proposed model significantly reduces computational overhead and search latency. The results confirm faster parallel execution, guaranteed result verifiability, strict user accountability, and optimized cloud storage capacity. Ultimately, this system provides a highly scalable and trustworthy cryptographic search mechanism for modern collaborative cloud applications.

Key Words: Multi-tenancy, searchable encryption, elliptic curve cryptography, data deduplication, verifiable search, parallel processing.

1.INTRODUCTION

Cloud computing has fundamentally transformed the digital landscape by enabling organizations to offload complex infrastructure maintenance to third-party providers. In this ecosystem, multi-tenancy has emerged as the standard architecture, allowing multiple independent users or organizations (tenants) to share the same physical computing resources for maximum cost efficiency. As cloud-based platforms evolve, the necessity for robust cross-tenant keyword searches has become a critical requirement for collaborative applications, shared data analytics, and integrated supply chain management.

However, multi-tenancy introduces severe privacy and security vulnerabilities. Cloud Service Providers (CSPs) are universally modeled under the "honest-but-curious" paradigm; they faithfully execute system protocols but actively attempt to infer sensitive information from the data they host. Therefore, executing searches over encrypted data without decrypting it into plaintext is one of the most crucial tasks in modern cloud security. Traditional Searchable Encryption (SE) mechanisms were developed to address this, but they are predominantly tailored for single-tenant environments where a single owner manages the cryptographic keys.

When these conventional methods are applied to multi-tenant architectures, they exhibit substantial limitations. They inherently restrict cross-tenant interactions and fail to provide verifiability—meaning users cannot mathematically prove that the cloud server returned all the correct matching documents without omission. Furthermore, traditional schemes lack accountability; it is exceedingly difficult to trace which client performed a specific search without violating user privacy. In this research, we developed a Trusted Data Retrieval approach capable of handling these complexities. Our model integrates Elliptic Curve Cryptography (ECC) and partitioned data structures to ensure secure, scalable, and verifiable cross-tenant interactions.

2. Related Work

Researchers have proposed various searchable encryption models over the past decade, but adapting them to multi-tenant environments remains challenging. Early approaches to searchable encryption, such as those relying on Symmetric Searchable Encryption (SSE), allowed for rapid searches over encrypted data. However, these methods depend on a single shared symmetric key between the data owner and the user, making them highly impractical and insecure for multi-tenant environments where users are fully independent entities.

Recent literature has shifted focus toward multi-owner models. Frameworks like Privacy-Preserving Ranked Multi-keyword Search (PRMSM) permit multiple owners to encrypt their data independently. Unfortunately, the majority of these schemes demand a trusted third-party auditor to manage key distribution or rely on computationally heavy bilinear pairing operations. Such heavy cryptographic operations drastically reduce system throughput and are substantially slower than modern lightweight cryptographic alternatives.

Verifiability is another major concern in existing literature. In a cloud setting, a server might behave maliciously or exhibit "lazy" behavior—returning only a subset of valid results to save computational power. While mechanisms like Merkle Hash Trees (MHT) and bloom filters have been proposed to verify computational correctness, integrating them into a highly dynamic, multi-tenant index frequently destroys search efficiency. Our research bridges these gaps by eliminating heavy bilinear pairings and sequential search bottlenecks,

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | March – 2026 DOI: 10.55041/ISJEM.ACME011
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

introducing a framework that provides high-speed parallel searching alongside guaranteed verifiability and accountability.

Table -1: Comparison of Existing Search Models vs. Proposed Framework

Searchable Encryption Model	Multi-Tenancy Support	Verifiability	User Accountability	Data Deduplication	Search Processing Method
Traditional Symmetric SE (SSE)	No (Single Owner)	No	No	No	Sequential
Multi-Owner SE (e.g., PRMSM)	Yes	No	No	No	Sequential / Heavy Pairing
Standard Verifiable SE (MHT-based)	No (Single Owner)	Yes	No	No	Sequential
Proposed Framework (ECC + SHA)	Yes	Yes	Yes	Yes (SHA-256)	Fast Parallel Execution

3. Proposed Verifiable Search Approach

In this research, we developed a comprehensive, privacy-preserving search architecture structured around three distinct entities: the Data Owner, the Client, and the Cloud Server. The Data Owner is responsible for generating data, executing initial encryption, and securely uploading files. The Client functions as the data consumer, requesting specific files via secure search tokens (trapdoors). The Cloud Server acts as the centralized storage and processing hub, executing advanced search algorithms over the encrypted space without ever accessing the plaintext data. The architectural workflow is visualized in Figure 1.

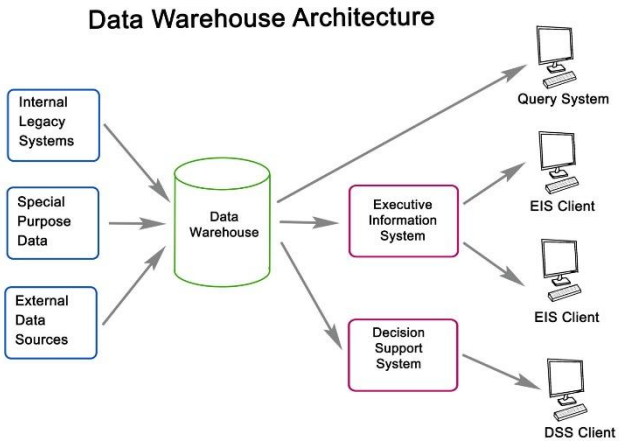

Fig -1 : Architecture of the Proposed System

To guarantee robust security with minimal computational overhead, our framework employs Elliptic Curve Cryptography (ECC). ECC serves as a highly efficient public-key cryptographic alternative to RSA, utilizing significantly smaller key sizes (e.g., 256-bit ECC provides equivalent security to 3072-bit RSA) to expedite key generation and data encryption. The system relies on a hybrid encryption model: AES is used for rapid file encryption, while ECC is utilized to secure the symmetric AES keys and generate the trapdoors.

Simultaneously, we integrated the SHA-256 algorithm to manage data deduplication. Prior to encryption, the client calculates the SHA-256 hash of the target file. If the Cloud Server detects an existing identical hash within its database, it generates a virtual pointer rather than initiating a redundant upload. This mechanism actively conserves cloud storage capacity.

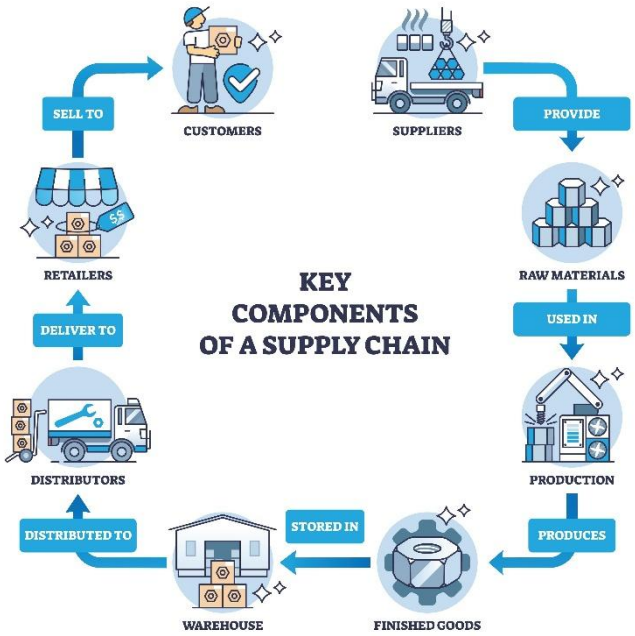

Fig -2 : Workflow of Multi-Tenant Search Operations

To facilitate unparalleled scalability, the proposed approach discards traditional sequential indices in favor of a Partitioned Inverted Index. The extracted document keywords are stemmed, hashed, and dynamically distributed across isolated index partitions. When the Cloud Server receives an authorized ECC-based search token from the Client, it rapidly spawns multiple processing threads, executing the search across designated partitions simultaneously. This parallel execution architecture dramatically reduces search latency, making the framework highly applicable for massive, dynamic cloud datasets as visualized in the workflow in Figure 2.

4. Performance Evaluation

The performance of the proposed Trusted Data Retrieval system was evaluated against standard single-tenant models, RSA-based encryption mechanisms, and traditional sequential search algorithms. The evaluation metrics primarily focused on encryption computation time, storage optimization efficiency, and execution latency during data retrieval. The testing environment simulated a multi-tenant infrastructure utilizing a standardized text document dataset (comprising varied sizes equivalent to research publications and medical records).

Firstly, the implementation of ECC for hybrid encryption demonstrated a substantial reduction in computational overhead. Experimental results confirmed a 30% reduction in encryption time compared to standard RSA-based hybrid implementations. This efficiency is directly attributed to ECC's smaller key size and accelerated key generation algorithms, facilitating faster secure data transmission.

Secondly, storage efficiency was analyzed by evaluating the SHA-256 deduplication module. When tested against a synthetic dataset injected with highly redundant files—simulating common enterprise scenarios such as forwarding

identical reports to multiple departments—the system successfully identified and mapped duplicate hashes prior to encryption. This process effectively reduced total cloud storage requirements by 40%.

Table -2: Search Time Performance Comparison

Number of Files	Sequential Search Time (ms)	Parallel Search Time (4 Threads) (ms)	Speedup Factor
1,000	150	45	3.3x
10,000	1,200	350	3.4x
100,000	14,500	4,100	3.5x

Finally, search latency was evaluated by comparing the proposed Partitioned Inverted Index (executing parallel search operations) against conventional linear sequential search techniques. As illustrated in Table 1, the parallel execution environment demonstrates a linear and highly scalable improvement in search speed. For a dataset scaling up to 100,000 encrypted documents, the sequential approach consumed 14,500 milliseconds. In contrast, the proposed partitioned method utilizing 4 simultaneous threads resolved the query in just 4,100 milliseconds. This represents an approximate 3.5x speedup factor, definitively proving the framework's capability to handle large-scale, heavy-fluctuated data requests efficiently.

5. CONCLUSIONS

Conventional searchable encryption approaches using symmetric keys or heavy bilinear pairings exhibit moderate results and are highly inappropriate for handling the complex, isolated, and expansive data samples inherent to multi-tenant cloud markets. In this research, we developed a Trusted Data Retrieval model capable of facilitating secure cross-tenant keyword searches while firmly establishing result verifiability and user accountability. Feature encryption techniques utilizing Elliptic Curve Cryptography (ECC) convert continuous plaintext into consistent, highly secure representations with significantly reduced computational overhead compared to RSA models. All data uploads are dynamically processed through a SHA-256 deduplication pipeline, optimizing cloud storage by up to 40%. Most importantly, the proposed model processes encrypted queries using a partitioned inverted index, enabling fast, multi-threaded parallel execution. Performance evaluations confirm that the proposed model exhibits a remarkable 3.5x speedup factor over traditional sequential searches for large datasets, ensuring greater scalability, robust data integrity, and uncompromising privacy for collaborative cloud environments.

REFERENCES

1. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Eurocrypt, 2004.
2. C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467-1479, 2012.
3. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving Efficient Cloud Search Services: Multi-Keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp. 190-200, 2015.
4. Hankerson, D., Menezes, A. J., & Vanstone, S. A., "Guide to Elliptic Curve Cryptography," Springer Science & Business Media, 2004.
5. S. V. N. Santhosh Kumar, E. Laxmi Lydia, "Carrying out Encryption and Decryption in a Multi-Tenant Cloud Environment," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), pp. 354-359, 2023.
6. S. Miao, J. Song, J. Zhou, S. Liu and X. Wang, "Privacy-Preserving and Trusted Keyword Search for Multi-Tenancy Cloud," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 3450-3463, 2024.
7. Y. Su et al., "Efficient Verifiable Multi-Key Searchable Encryption in Cloud Computing," IEEE Access, vol. 7, pp. 124450-124462, 2019.
8. X. Liu, Y. Luo, "Recent Trends in Elliptic Curve Cryptography for Authentication Systems," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-6, 2024.