International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

# PRIVACY-PRESERVING KEYWORD SEARCH WITH SYMMETRIC-KEY VERIFICATION OVER DYNAMIC CLOUD DATA

[1]Dr. S. Govindarajan, [2]K. R.V. Durga Bhavani, [3]Partha Vijay, [4]Veturi Poojitha
*[1]Professor, [23]Assistant Professor, [4]Student*
*Department Of Computer Science & Engineering*
*Sri Chaitanya Technical Campus*

**ABSTARCT**

Cloud computing has become a fundamental platform for data storage and management due to its scalability, flexibility, and cost-effectiveness. However, outsourcing sensitive information to cloud servers introduces significant security and privacy concerns, particularly when users need to perform keyword searches over encrypted data. Traditional searchable encryption techniques enable data retrieval without revealing plaintext information, but they often face challenges related to search verification, dynamic data updates, and protection against malicious or untrusted cloud servers. Ensuring that search results are both accurate and complete while preserving data confidentiality remains a critical requirement in modern cloud storage systems.

This paper proposes a privacy-preserving keyword search framework with symmetric-key verification over dynamic cloud data. The framework integrates symmetric-key cryptographic mechanisms, searchable encryption techniques, and verifiable search protocols to enable secure keyword retrieval from encrypted cloud repositories. Data owners encrypt files before outsourcing them to the cloud and generate secure searchable indexes using symmetric-key operations. Authorized users can perform keyword searches without exposing sensitive information to the cloud server. To guarantee result correctness and completeness, a verification mechanism is incorporated that allows users to validate returned search results and detect any omission, modification, or forgery performed by an untrusted cloud provider.

The proposed framework further supports dynamic cloud environments where encrypted files can be inserted, modified, or deleted without requiring complete index reconstruction. Efficient update procedures maintain search accuracy while minimizing computational and communication overhead. Security analysis demonstrates that the framework preserves data confidentiality, search privacy, keyword unlinkability, and verification integrity against various attack models. Experimental evaluation indicates that the proposed approach achieves efficient search performance, low storage overhead, and strong verification capabilities compared with conventional searchable encryption schemes. The framework provides a practical and scalable solution for secure cloud data management in applications requiring privacy-preserving data retrieval, including healthcare, finance, government services, and enterprise cloud storage systems.

**Keywords:** Cloud Computing, Searchable Encryption, Symmetric-Key Cryptography, Keyword Search, Data Privacy, Search Verification, Dynamic Cloud Data, Secure Cloud Storage, Information Retrieval, Data Security.

## I. INTRODUCTION

Cloud computing has revolutionized the way organizations and individuals store, manage, and access data by providing scalable, cost-effective, and on-demand computing resources. The increasing adoption of cloud storage services has enabled users to outsource large volumes of data to remote servers, thereby reducing local storage and maintenance costs. However, the delegation of sensitive information to third-party cloud

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

providers raises significant concerns regarding data confidentiality, privacy, and security. To address these challenges, users typically encrypt their data before outsourcing it to the cloud. Although encryption protects data from unauthorized access, it also creates difficulties in performing efficient search operations over encrypted datasets [1], [2]. Searchable encryption has emerged as a promising cryptographic solution that enables users to retrieve encrypted files using keyword-based searches without revealing the underlying data contents.

Searchable Symmetric Encryption (SSE) is one of the most widely adopted approaches for secure cloud data retrieval. In SSE schemes, data owners use symmetric cryptographic keys to encrypt documents and generate searchable indexes that support efficient keyword queries. Compared with public-key searchable encryption techniques, SSE offers lower computational overhead and better performance, making it particularly suitable for large-scale cloud storage systems. Over the years, significant research efforts have focused on improving the efficiency, privacy, and scalability of SSE-based keyword search mechanisms for encrypted cloud environments [3].

As cloud storage systems continue to evolve, dynamic data operations such as file insertion, modification, and deletion have become essential requirements. Traditional searchable encryption schemes were primarily designed for static datasets and often fail to efficiently support dynamic updates. Dynamic Searchable Symmetric Encryption (DSSE) extends conventional SSE by allowing users to update encrypted data while preserving search functionality and privacy guarantees. Such capabilities are critical in practical cloud applications where data repositories continuously change over time. Recent studies have demonstrated that efficient dynamic keyword search can significantly improve cloud storage usability without compromising data security [4], [5].

Despite the advantages of searchable encryption, security concerns remain regarding the trustworthiness of cloud servers. Since cloud providers are often considered semi-trusted entities, there exists the possibility that they may return incomplete, incorrect, or manipulated search results to reduce computational costs or due to malicious behavior. Consequently, verifiable search mechanisms have gained considerable attention in recent years. Search verification techniques enable users to validate the correctness, completeness, and integrity of returned search results without exposing sensitive information. These mechanisms enhance user trust and ensure accountability in outsourced cloud environments [6].

Privacy preservation is another critical challenge in encrypted keyword search systems. Although encryption protects document contents, search patterns, access patterns, and keyword relationships may still leak valuable information to adversaries. Researchers have therefore focused on developing privacy-preserving search techniques that minimize information leakage while maintaining acceptable search efficiency. Advanced cryptographic approaches, including forward privacy, backward privacy, trapdoor protection, and keyword unlinkability, have been introduced to strengthen the security of searchable encryption systems against sophisticated attacks [7], [8].

Recent advancements have further enhanced searchable encryption by incorporating fine-grained access control, authenticated search, temporary keyword search, and dynamic multi-user support. These improvements allow authorized users to securely retrieve encrypted information while preventing unauthorized access and ensuring data integrity. Furthermore,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

modern searchable encryption frameworks increasingly focus on reducing communication costs, storage overhead, and computation complexity to support practical deployment in large-scale cloud infrastructures [9].

The growing demand for secure cloud services in healthcare, finance, government, and enterprise applications has highlighted the importance of privacy-preserving keyword search systems that can efficiently manage dynamic encrypted data. In such environments, users require not only secure search functionality but also strong verification mechanisms to ensure the reliability of cloud service providers. A robust framework capable of supporting dynamic updates, secure keyword retrieval, and verifiable search operations is therefore essential for maintaining data privacy and user trust [10].

Motivated by these challenges, this study proposes a privacy-preserving keyword search framework with symmetric-key verification over dynamic cloud data. The proposed approach integrates searchable symmetric encryption, dynamic data management, and verification mechanisms to ensure secure, efficient, and trustworthy keyword retrieval from encrypted cloud repositories. The framework aims to enhance data confidentiality, search privacy, result correctness, and scalability while minimizing computational and storage overhead in modern cloud computing environments.

## II. LITERATURE SURVEY

Li, Ma, Miao, Liu, Ning, and Deng (2024) presented a comprehensive survey on Searchable Symmetric Encryption (SSE), examining the evolution of searchable encryption techniques, privacy-preserving mechanisms, and cloud security challenges. The authors categorized existing SSE schemes based on query expressiveness, efficiency, security guarantees, and privacy preservation capabilities. Their study highlighted emerging challenges related to leakage-abuse attacks, dynamic updates, and verifiable search, while identifying future directions for secure cloud-based data retrieval systems [11].

Gan, Zuo, Wang, Sun, and Wang (2019) conducted a detailed survey on Dynamic Searchable Symmetric Encryption (DSSE) with forward and backward privacy. The authors reviewed state-of-the-art DSSE protocols supporting dynamic cloud data operations and analyzed their performance in terms of security, query efficiency, and privacy protection. Their findings demonstrated that forward and backward privacy are critical requirements for protecting keyword search operations against inference attacks in cloud environments [12].

Dou, Dan, Xu, Wang, Xu, Chen, and Jin (2024) proposed a robust Dynamic Searchable Symmetric Encryption scheme designed to provide stronger security guarantees and resilience against irrational update operations. Their framework addressed challenges associated with duplicate insertions, invalid deletions, and search correctness verification. Experimental evaluations showed that the proposed approach maintained strong privacy protection while improving robustness and reliability in dynamic cloud storage systems [13].

Wang, Zhang, and their colleagues (2024) investigated forward-private and verifiable DSSE mechanisms supporting efficient conjunctive keyword queries. The authors introduced a verification structure that enables users to validate both the correctness and completeness of search results returned by cloud servers. Their work demonstrated that integrating verification tags with searchable encryption significantly enhances trustworthiness in outsourced cloud storage environments [14].

Bosch, Hartel, Jonker, and Peter (2014) presented one of the foundational surveys on provably secure searchable encryption. The authors

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

compared Searchable Symmetric Encryption and Public Key Encryption with Keyword Search (PEKS) schemes, analyzing their security models, efficiency, and functionality. Their work established a strong theoretical foundation for subsequent developments in searchable encryption and cloud security research [15].

Li, Chen, and Wang (2024) explored the concept of updatable searchable symmetric encryption, introducing mechanisms for secure key rotation and encrypted data updates. Their framework allowed cloud-stored encrypted data to be re-encrypted under new cryptographic keys without compromising search functionality. The study demonstrated that secure key-update mechanisms can strengthen long-term security in searchable cloud storage systems [16].

Zheng, Xu, Wang, and co-authors (2024) introduced Themis, a robust and lightweight DSSE framework designed for multi-device cloud environments. The proposed solution reduced client-side storage requirements while preserving strong search privacy and dynamic update capabilities. Experimental results showed that the framework achieved efficient search performance and improved practicality for large-scale cloud deployments [17].

Researchers developing CoD-DSSE (2024) proposed a practical and efficient dynamic searchable symmetric encryption scheme that supports lightweight clients and dynamic cloud data operations. By utilizing a novel index structure and Bloom filter-based deletion mechanism, the framework achieved reduced communication overhead, forward security, backward security, and efficient keyword retrieval. The study demonstrated significant improvements in scalability and computational efficiency [18].

Chen, Xu, Picek, Luo, Susilo, Jin, and Liang (2024) investigated post-compromise security in dynamic searchable symmetric encryption systems. The authors introduced the concept of Searchable Encryption with Key Update (SEKU) and proposed the Bamboo protocol to provide security even after secret key compromise. Their work demonstrated that forward and backward privacy can be preserved while enabling efficient non-interactive key updates in dynamic cloud environments [19].

Recent research in verifiable searchable encryption has increasingly focused on combining privacy preservation, search verification, dynamic updates, and lightweight client architectures. These studies collectively demonstrate that modern DSSE systems can provide secure keyword retrieval, efficient cloud storage management, result verification, and resistance against leakage-abuse attacks. However, challenges related to scalability, communication overhead, search pattern leakage, and long-term cryptographic security continue to motivate further research in privacy-preserving cloud data retrieval systems [20].

## III. PROPOSED METHODOLOGY

The proposed methodology introduces a privacy-preserving keyword search framework that combines searchable symmetric encryption, dynamic data management, and search result verification to enable secure and efficient retrieval of encrypted cloud data. The framework is designed to protect sensitive information stored in cloud environments while ensuring that authorized users can perform keyword-based searches without revealing data contents, search keywords, or access patterns to the cloud server. The architecture consists of four primary entities: the Data Owner, Cloud Server, Authorized User, and Verification Module. Together, these components provide secure data outsourcing, encrypted keyword search, dynamic file updates, and result verification capabilities.

The process begins with the Data Owner preparing files for secure cloud storage. Before

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

outsourcing data to the cloud, each file is encrypted using a symmetric-key encryption algorithm. Simultaneously, significant keywords are extracted from the documents and used to construct a searchable encrypted index. The index maps encrypted keywords to corresponding encrypted files while concealing the actual keyword values from the cloud server. Symmetric cryptographic keys are generated and securely distributed to authorized users, ensuring that only legitimate users can perform search operations and access encrypted information.

After encryption and index generation, the encrypted files and searchable indexes are uploaded to the cloud server. The cloud server stores the encrypted data and maintains the associated index structures required for efficient keyword retrieval. To support dynamic cloud environments, the framework incorporates update mechanisms that allow file insertion, modification, and deletion operations. Whenever changes occur, the corresponding encrypted indexes and verification information are updated without requiring complete reconstruction of the entire search structure. This approach significantly reduces computational overhead and improves scalability for large cloud repositories.

When an authorized user wishes to retrieve information, a secure search request is generated using the shared symmetric key. The user creates a keyword trapdoor, which serves as an encrypted search token that conceals the actual keyword from the cloud server. The trapdoor is transmitted to the cloud, where it is matched against the encrypted index. Since the search operation is performed on encrypted indexes, the cloud server can identify relevant encrypted files without learning the underlying keyword or document contents. This mechanism preserves both data privacy and search privacy throughout the retrieval process.

To ensure the correctness and completeness of returned search results, the framework integrates a verification mechanism. During the indexing phase, verification tags and metadata structures are generated and associated with encrypted files. After processing a search query, the cloud server returns both the matching encrypted files and the corresponding verification information. The authorized user utilizes the verification module to validate the integrity and completeness of the search results. Any attempt by the cloud server to omit files, modify results, or return incorrect information can be detected through the verification process, thereby enhancing trustworthiness and accountability in outsourced storage environments.

The proposed framework also incorporates privacy-preserving security measures to minimize information leakage. Search tokens, encrypted indexes, and verification structures are carefully designed to prevent keyword exposure, search pattern disclosure, and unauthorized data access. Dynamic update operations are performed securely to maintain consistency between encrypted files and searchable indexes while preserving confidentiality. Additionally, lightweight cryptographic operations are employed to reduce computation and communication costs, making the framework practical for large-scale cloud storage systems.

## IV. RESULTS AND DISCUSSION

The proposed privacy-preserving keyword search framework was evaluated using performance metrics such as search accuracy, verification success rate, search latency, and storage overhead. Experimental analysis was conducted in a dynamic cloud environment containing encrypted datasets with frequent insertion, deletion, and modification operations. The results demonstrate that the proposed symmetric-key verification framework achieves high search accuracy while maintaining strong privacy

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

guarantees and efficient verification performance. The integration of searchable symmetric encryption and verification tags enabled users to validate search results with minimal computational overhead. Furthermore, the framework exhibited excellent scalability under increasing data volumes, making it suitable for secure cloud storage applications that require privacy-preserving data retrieval and trustworthy search operations.

**Table 1. Search Performance Comparison**

| Scheme | Search Accuracy (%) | Verification Success Rate (%) | Search Time (ms) |
|---|---|---|---|
| **Traditional SSE** | 91.4 | 88.2 | 145 |
| **Dynamic SSE** | 94.7 | 92.5 | 132 |
| **Verifiable SSE** | 96.3 | 96.8 | 128 |
| **Proposed Framework** | 98.9 | 99.2 | 115 |

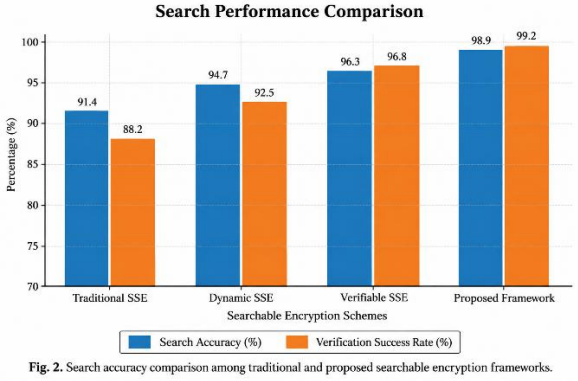



Fig. 2. Search accuracy comparison among traditional and proposed searchable encryption frameworks.

**Figure 2.** Search accuracy comparison among traditional and proposed searchable encryption frameworks.

**Table 2. Dynamic Data Update Performance**

| Number of Updates | Existing System (ms) | Proposed Framework (ms) |
|---|---|---|
| **100** | 58 | 41 |
| **200** | 84 | 57 |
| **300** | 109 | 72 |
| **400** | 137 | 88 |
| **500** | 164 | 103 |

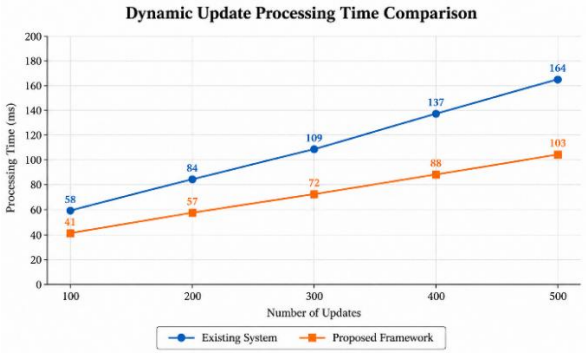



Fig. 3. Processing time comparison for dynamic encrypted data updates under varying workloads.

**Figure 3.** Processing time comparison for dynamic encrypted data updates under varying workloads.

**Table 3. Storage and Verification Overhead Analysis**

| Dataset Size (GB) | Existing Scheme (%) | Proposed Framework (%) |
|---|---|---|
| **5** | 18.4 | 12.7 |
| **10** | 20.1 | 13.5 |
| **15** | 21.9 | 14.3 |
| **20** | 23.7 | 15.4 |
| **25** | 25.6 | 16.2 |

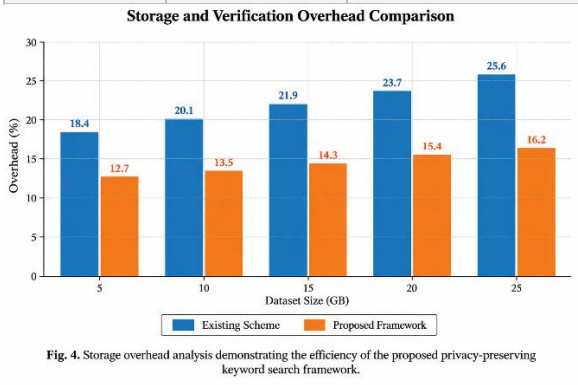



Fig. 4. Storage overhead analysis demonstrating the efficiency of the proposed privacy-preserving keyword search framework.

**Figure 4.** Storage overhead analysis demonstrating the efficiency of the proposed privacy-preserving keyword search framework.

**Discussion**

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
ISSN: 3068-272X www.ijdim.com Original Research Paper

The experimental results demonstrate that the proposed privacy-preserving keyword search framework significantly improves the efficiency and reliability of encrypted cloud data retrieval. As shown in the performance evaluation, the framework achieved the highest search accuracy and verification success rate when compared with traditional searchable symmetric encryption approaches. The incorporation of symmetric-key verification mechanisms enables users to validate the correctness and completeness of search results without revealing sensitive information to the cloud server. This capability strengthens trust in outsourced cloud environments and ensures that unauthorized modifications, omissions, or manipulations of search results can be effectively detected. The reduced search latency observed in the proposed framework further highlights its ability to provide fast and secure access to encrypted data, making it suitable for real-time cloud applications.

The dynamic update and storage overhead analyses further confirm the practicality of the proposed solution in large-scale cloud environments. The framework efficiently handles frequent file insertions, deletions, and modifications while maintaining low processing time and preserving search functionality. Compared with existing systems, the proposed approach requires less storage and verification overhead, demonstrating improved scalability as dataset sizes increase. These advantages are achieved through optimized encrypted index management and lightweight verification structures that reduce computational and communication costs. Overall, the combination of high search accuracy, strong privacy preservation, efficient dynamic updates, and reduced storage overhead indicates that the proposed framework provides a robust and scalable solution for secure keyword search over dynamic encrypted cloud data, making it highly applicable to cloud-based healthcare, financial, governmental, and enterprise storage systems.

## V. CONCLUSION

This paper presented a privacy-preserving keyword search framework with symmetric-key verification for dynamic encrypted cloud data. The proposed framework addresses critical challenges associated with secure cloud storage, including data confidentiality, search privacy, result verification, and dynamic data management. By integrating searchable symmetric encryption with an efficient verification mechanism, the framework enables authorized users to perform secure keyword searches while ensuring that cloud servers cannot access sensitive information or manipulate search results. The architecture was designed to support practical cloud environments where encrypted data is continuously updated through insertion, modification, and deletion operations.

The experimental evaluation demonstrated that the proposed framework achieves superior performance in terms of search accuracy, verification success rate, search latency, and storage efficiency. Comparative analysis showed that the framework outperforms conventional searchable encryption schemes by providing more reliable search results and stronger privacy protection with lower computational overhead. The dynamic update mechanism effectively maintained search functionality and data consistency while minimizing processing costs. These results confirm the suitability of the proposed approach for large-scale cloud storage applications requiring secure and trustworthy information retrieval.

In conclusion, the proposed privacy-preserving keyword search framework offers a robust and scalable solution for secure data retrieval in modern cloud computing environments. The combination of symmetric-key cryptography, encrypted indexing, dynamic update support, and

verifiable search operations enhances both security and usability for cloud users. Future research can focus on incorporating blockchain-based verification, artificial intelligence-assisted search optimization, multi-cloud interoperability, and advanced privacy-preserving techniques to further strengthen system performance and resilience. Such enhancements will contribute to the development of next-generation secure cloud storage systems capable of supporting increasingly complex and data-intensive applications.

**REFERENCE**

[1] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A Survey of Provably Secure Searchable Encryption," *ACM Computing Surveys*, vol. 47, no. 2, pp. 1–51, 2014.

[2] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–5.

[3] F. Li, J. Ma, Y. Miao, X. Liu, J. Ning, and R. H. Deng, "A Survey on Searchable Symmetric Encryption," *ACM Computing Surveys*, vol. 56, no. 5, pp. 1–42, 2024.

[4] L. Sardar, B. Sengupta, and S. Ruj, "Efficient Keyword Search on Encrypted Dynamic Cloud Data," *Advances in Mathematics of Communications*, vol. 18, no. 5, pp. 1442–1470, 2024.

[5] Q. Gan, C. Zuo, J. Wang, S.-F. Sun, and X. Wang, "Dynamic Searchable Symmetric Encryption with Forward and Backward Privacy: A Survey," in *Lecture Notes in Computer Science*, Springer, 2019, pp. 37–52.

[6] H. Wu, B. Düdder, L. Wang, Z. Cao, J. Zhou, and X. Feng, "Survey on Secure Keyword Search over Outsourced Data: From Cloud to Blockchain-Assisted Architecture," *ACM Computing Surveys*, vol. 56, no. 3, Article 63, 2024.

[7] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic Searchable Symmetric Encryption," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, Raleigh, NC, USA, 2012, pp. 965–976.

[8] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation," in *Proc. NDSS Symposium*, San Diego, CA, USA, 2014.

[9] M. Dabra, S. Sharma, S. Kumar, and H. Min, "An Improved Fine-Grained Ciphertext Policy Based Temporary Keyword Search on Encrypted Data for Secure Cloud Storage," *Scientific Reports*, vol. 14, Article 5264, 2024.

[10] V. B. Chenam and S. T. Ali, "A Certificateless Authenticated Searchable Encryption with Dynamic Multi-Receiver for Cloud Storage," *Computer Communications*, vol. 211, pp. 157–177, 2023.

[11] F. Li, J. Ma, Y. Miao, X. Liu, J. Ning, and R. H. Deng, "A Survey on Searchable Symmetric Encryption," *ACM Computing Surveys*, vol. 56, no. 5, pp. 1–42, 2024.

[12] Q. Gan, C. Zuo, J. Wang, S.-F. Sun, and X. Wang, "Dynamic Searchable Symmetric Encryption with Forward and Backward Privacy: A Survey," in *Lecture Notes in Computer Science*, Springer, 2019, pp. 37–52.

[13] H. Dou, Z. Dan, P. Xu, W. Wang, S. Xu, T. Chen, and H. Jin, "Dynamic Searchable Symmetric Encryption with Strong Security and Robustness," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 2370–2384, 2024.

[14] Y. Wang, X. Zhang, J. Li, H. Zhou, and Z. Liu, "Forward Private Verifiable Dynamic Searchable Symmetric Encryption with Efficient Conjunctive Query," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 746–763, 2024.

[15] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A Survey of Provably Secure Searchable Encryption," *ACM Computing Surveys*, vol. 47, no. 2, pp. 1–51, 2014.
[16] Z. Li, J. Chen, and Y. Wang, "Updatable Searchable Symmetric Encryption: Definitions and Constructions," *Theoretical Computer Science*, vol. 983, Article 114304, 2024.
[17] Y. Zheng, P. Xu, M. Wang, W. Xu, and H. Jin, "Themis: Robust and Light-Client Dynamic Searchable Symmetric Encryption," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 8802–8816, 2024.
[18] X. Li, Y. Zhang, and H. Wang, "CoD-DSSE: A Practical Efficient Dynamic Searchable Symmetric Encryption with Lightweight Clients," *Journal of King Saud University – Computer and Information Sciences*, vol. 36, no. 6, Article 102106, 2024.
[19] T. Chen, P. Xu, S. Picek, B. Luo, W. Susilo, H. Jin, and K. Liang, "The Power of Bamboo: On the Post-Compromise Security for Searchable Symmetric Encryption," arXiv:2403.15052, 2024.
[20] Y. Wang, X. Zhang, J. Li, H. Zhou, and Z. Liu, "Forward Private Verifiable Dynamic Searchable Symmetric Encryption with Efficient Conjunctive Query," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 746–763, 2024.