The Evolution of Searchable Encryption Technology and Security Challenges in the Post Quantum Era

Jialong Shi, Ze Wang

***Abstract*—Searchable encryption (SE) enables secure retrieval over encrypted data, balancing privacy and usability in cloud storage. This paper reviews SE's evolution, contrasting symmetric (SSE) and asymmetric (ASE/PEKS) models, and summarizes breakthroughs in dynamic data support, multi-keyword search, and leakage resilience. Current challenges include efficiency in complex queries, dynamic scenario adaptability, and quantum threats. Future directions focus on lightweight protocols, post-quantum designs (e.g., lattice-based cryptography), and integration with blockchain/homomorphic encryption to advance privacy-preserving frameworks. This work provides critical insights for SE's development in the post-quantum era.**

***Index Terms*—Searchable encryption; Privacy-preserving computation ; Dynamic data support; Data security;**

I. Introduction

With the rapid advancement of cloud computing and big data technologies, outsourced data storage has become a common practice for enterprises and individual users. However, hosting sensitive data (e.g., medical records, financial transactions) on third-party cloud platforms introduces significant privacy leakage risks. According to IBM's 2023 Cost of a Data Breach Report, the average global cost of data breaches reached $4.45 million, with cloud storage scenarios accounting for over 60% of incidents. While traditional encryption ensures data confidentiality, encrypted data loses searchability, hindering efficient retrieval of target information. This contradiction becomes particularly acute in scenarios with large-scale data and frequent retrieval demands, such as encrypted email systems and electronic medical record sharing.

To address these challenges, searchable encryption (SE) has emerged. Its core objective is to enable secure keyword-based retrieval over encrypted data without revealing plaintext information or search patterns to the server. Since Song et al. [1] proposed the first symmetric searchable encryption (SSE) scheme in 2000, SE has evolved into two branches—symmetric (SSE) and asymmetric (ASE/PEKS)—achieving breakthroughs in dynamic updates, multi-keyword search, and post-quantum security.

The research value of SE lies in two dimensions: Theoretically, it balances privacy and efficiency through cryptographic protocols (e.g., trapdoor generation, secure index construction), driving innovation in ciphertext data processing. Practically, SE provides viable privacy-enhancing solutions for cloud storage, blockchain-based data sharing, and privacy-preserving computation. For example, healthcare institutions can utilize SE to enable cross-institution retrieval of encrypted medical records while preventing patient privacy leaks, and enterprises can securely perform compliance audits on encrypted databases.

Nevertheless, SE faces critical challenges: (1) Efficiency bottlenecks—existing schemes incur high computational and communication costs when supporting complex queries (e.g., fuzzy or range searches); (2) Adaptability to dynamic scenarios—frequent data updates may compromise forward/backward security, leading to historical information leakage; (3) Post-quantum security threats—most schemes rely on classical public-key cryptography (e.g., RSA, ECC), which is vulnerable to quantum computing attacks.

This paper systematically reviews the technical framework, research progress, and future directions of SE. First, it conducts a comparative analysis of core models and representative schemes for symmetric and asymmetric SE. Next, it summarizes key technological breakthroughs across three dimensions: dynamic data support, functional expansion, and security enhancement. Finally, it explores potential research directions for SE, including efficiency optimization, post-quantum design, and cross-technology integration, aiming to provide theoretical guidance for future studies.

II. Model and Key Technology Breakthrough n

A. Core Model and Typical Solutions

Searchable encryption (SE) technology can be categorized into two classes based on cryptographic systems and application scenarios: symmetric searchable encryption (SSE) and asymmetric searchable encryption (ASE/PEKS). SSE, rooted in shared-key mechanisms, suits scenarios where the data owner and searcher are the same entity. Its core principle involves encrypting data via symmetric algorithms (e.g., AES) and constructing secure indexes for keyword retrieval. For instance, in the first SSE scheme proposed by Song et al. [1] in 2000, the data owner generates a symmetric key, encrypts documents, extracts keywords to create pseudo-random hash values as index entries, and generates keyword trapdoors using the key. These trapdoors are submitted to the server, which matches the index to return encrypted documents. Such schemes excel in computational efficiency for large-scale data retrieval but suffer from high key leakage risks and initially supported only static single-keyword searches.

ASE/PEKS, in contrast, relies on public-key cryptography. Here, the data owner encrypts data using a public key, while

Manuscript received May 13, 2025
Jialong Shi, School of computer science and technology, Tiangong University, Tianjin, China
Ze Wang, School of Software, Tiangong University, Tianjin, China

other users generate search trapdoors via private keys. A representative example is the public-key encryption with keyword search (PEKS) proposed by Boneh et al. [2] in 2004. In this model, the data owner publishes a public key for others to encrypt data. Searchers use their private keys to generate irreversible trapdoors, and the server performs bilinear pairing operations to test keyword matches, returning results while preserving search privacy. This approach inherently supports multi-user collaboration (e.g., encrypted email retrieval in public cloud environments) but incurs substantial computational overhead due to public-key operations, limiting its practicality for complex queries.

Technically, SSE and ASE/PEKS exhibit significant differences in key management, efficiency, and functional scalability:

SSE leverages the efficiency of symmetric keys, making it ideal for single-user rapid retrieval in private cloud environments.

ASE/PEKS enables secure multi-user interactions through public-key infrastructure but requires trade-offs between computational efficiency and resistance to collusion attacks.

Over time, both paradigms have evolved to support dynamic data updates, multi-keyword Boolean queries [3], and complementary applications in medical data sharing and blockchain privacy protection. However, their core challenges remain: overcoming efficiency bottlenecks, enhancing forward security in dynamic scenarios, and resisting quantum computing threats.

B. Key Technological Breakthroughs

The research breakthroughs in searchable encryption (SE) technology are primarily reflected in three dimensions: adaptive support for dynamic data, diversified expansion of retrieval functionalities, and continuous enhancement of security defenses.

1. Dynamic Data Support

Early SE schemes were limited to static datasets and struggled to handle frequent data addition, deletion, and modification in real-world scenarios. To address this, researchers proposed dynamic searchable encryption (DSSE) frameworks, which enable dynamic data management through updatable encrypted index structures (e.g., searchable binary trees or hash tables). For example, the Σοφος scheme by Bost et al. [4] employs chained hashing and key rotation mechanisms to ensure that newly added data does not leak associations with historical records, thereby achieving forward security. To mitigate risks of document-keyword mapping exposure during deletions, some solutions integrate oblivious random-access memory (ORAM) technology to obfuscate access patterns and conceal update traces. However, dynamic operations often sacrifice efficiency—for instance, ORAM introduces logarithmic-scale latency in retrieval. Balancing security and practicality remains a critical challenge.

2. Functional Expansion

Efforts to extend functionality aim to transcend single-keyword exact matching, supporting complex queries while maintaining robustness. The Themis scheme proposed by Zheng et al. [5] pioneers the integration of lightweight client requirements with robustness, enabling fault-tolerant mechanisms during dynamic data updates (additions/deletions). Through an error operation alert mechanism and oblivious map, Themis ensures system security and correctness even when clients perform erroneous operations (e.g., duplicate deletions or removal of non-existent entries). Compared to traditional robust schemes (e.g., ROSE), Themis achieves a 5x improvement in search efficiency with search time independent of error frequency, making it suitable for large-scale dynamic databases. Its design concepts (e.g., "concept tree" structures) provide an extensible framework for multi-condition compound queries. Future enhancements could integrate homomorphic encryption or differential privacy to support range queries and fuzzy searches.

3. Security Enhancement

Security advancements focus on minimizing information leakage and defending against novel attacks. Traditional SE schemes risk metadata exposure through search patterns (e.g., trapdoor reuse) or access patterns (e.g., document return sequences). Recent studies address these vulnerabilities via lattice-based solutions [6][7]. Lin et al. [6] proposed the first identity-based SE scheme with lattice cryptography, supporting disjunctive (OR), conjunctive (AND), and range searches while resisting quantum attacks. Key innovations include:

A privacy-preserving test mechanism that allows servers to verify keyword matches without exposing keyword contents.

A dual-set inclusion judgment algorithm and fast range keyword verification method, decoupling ciphertext/trapdoor storage costs from keyword quantities to enhance efficiency.

Experimental results show a 30% reduction in ciphertext size and search time compared to traditional schemes (e.g., SPX), with support for diverse multi-keyword complex queries. Under the random oracle model (ROM), the scheme satisfies indistinguishability against adaptive chosen-keyword attacks (IND-CKA) and demonstrates post-quantum resistance via the hardness assumption of the learning-with-errors (LWE) problem. This makes it applicable to high-security scenarios like finance and healthcare.

III. FUTURE DEVELOPMENT AND POTENTIAL RESEARCH DIRECTIONS

The future development of searchable encryption (SE) technology necessitates advancements in efficiency optimization, post-quantum security design, and cross-technology integration to address performance limitations and emerging security challenges.

Efficiency optimization remains a critical focus, as current SE schemes suffer from high computational and communication costs when handling complex queries like multi-keyword Boolean or fuzzy searches, particularly in asymmetric SE due to computationally intensive bilinear pairing and exponentiation operations. Promising approaches include adopting lightweight cryptographic primitives—such as hash-based pseudorandom permutations to replace traditional public-key operations—and leveraging parallel computing architectures like CUDA-based GPU acceleration for trapdoor generation and index matching. Distributed retrieval protocols, such as sharded indexes and multi-server collaboration, could further enhance scalability. Hardware security modules (HSMs) or trusted execution environments

(TEEs) may accelerate critical operations, while incremental index update algorithms could reduce the overhead of frequent data updates in dynamic scenarios.

Post-quantum security design is essential to counter quantum computing threats. Most existing SE schemes rely on classical public-key cryptography (e.g., RSA, ECC), which is vulnerable to attacks enabled by Shor's algorithm. Lattice-based cryptography has emerged as a leading candidate, with schemes utilizing ring learning with errors (RLWE) or NTRU-based protocols to construct quantum-resistant trapdoor functions. However, these methods currently lag in retrieval efficiency compared to classical approaches. Future efforts should optimize lattice-based operations—for instance, accelerating polynomial multiplication via number-theoretic transforms—and explore lightweight frameworks based on hash-based signatures or code-based cryptography. Hybrid schemes combining quantum-safe and classical cryptography could facilitate transitional compatibility. Establishing standardized evaluation criteria for post-quantum SE is also crucial to define security assumptions and performance benchmarks.

Cross-technology integration aims to transcend SE's standalone capabilities by combining it with complementary technologies. Integrating SE with blockchain enables decentralized systems where smart contracts ensure transparent key management and auditable search operations, as seen in medical data sharing scenarios requiring tamper-proof audit trails. Synergy with homomorphic encryption (HE) allows direct computations on retrieved ciphertexts—for example, using SE to locate encrypted medical records followed by HE-based privacy-preserving analysis on specific fields. Embedding SE into federated learning (FL) frameworks supports secure data retrieval and sample filtering during distributed model training. Additionally, incorporating differential privacy (DP) during index construction—by injecting controlled noise to obscure keyword distributions—could mitigate statistical inference attacks. While challenges like protocol compatibility and joint security proofs persist, these integrations hold transformative potential for applications in financial risk management, smart cities, and other domains requiring rigorous privacy guarantees.

IV. CONCLUSION

Searchable encryption (SE) achieves a critical balance between privacy preservation and data usability through secure retrieval mechanisms for encrypted data. Despite significant advancements in dynamic updates, multi-keyword search, and leakage-resilient design, core challenges—including efficiency bottlenecks, quantum security threats, and cross-scenario adaptability—continue to impede its large-scale adoption. Future research must focus on optimizing lightweight protocols, improving the practicality of post-quantum algorithms (e.g., lattice-based cryptography), and fostering deep integration of SE with blockchain and homomorphic encryption to build more versatile and efficient privacy-preserving computation frameworks. Technical standardization and compliance adaptations will accelerate SE's deployment in domains such as healthcare and finance, establishing a trusted foundation for secure data circulation.

REFERENCES

[1] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data[C]//Proceeding 2000 IEEE symposium on security and privacy. S&P 2000. IEEE, 2000: 44-55.
[2] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[C]//International conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 506-522.
[3] [10] Kamara S, Papamanthou C. Parallel and dynamic searchable symmetric encryption[C]//Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17. Springer Berlin Heidelberg, 2013: 258-274.
[4] Bost R, Minaud B, Ohrimenko O. Forward and backward private searchable encryption from constrained cryptographic primitives[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 1465-1482.
[5] Zheng Y, Xu P, Wang M, et al. Themis: robust and light-client dynamic searchable symmetric encryption[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 8802-8816.
[6] Lin Z, Li H, Chen X, et al. Identity-Based Encryption with Disjunctive, Conjunctive and Range Keyword Search from Lattices[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 8644-8657.
[7] Dai X, Chen J, Wu W, et al. Lattice-based, more general anti-leakage model and its application in decentralization[C]//Australasian Conference on Information Security and Privacy. Singapore: Springer Nature Singapore, 2024: 44-63.
[8] Li H, Wang T, Qiao Z, et al. Blockchain-based searchable encryption with efficient result verification and fair payment[J]. Journal of Information Security and Applications, 2021, 58: 102791.
[9] Amorim I, Costa I. Leveraging searchable encryption through homomorphic encryption: A comprehensive analysis[J]. Mathematics, 2023, 11(13): 2948.
[10] Choi S G, Dachman-Soled D, Gordon S D, et al. Compressed oblivious encoding for homomorphically encrypted search[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021: 2277-2291.