IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155241

Privacy-Preserving Intelligent Collaboration Platform with Searchable Encryption and Client Side AI: A Survey of Privacy-Preserving Methods for Secure Collaboration

Dr. Kothapalli Venkata Rao[1], Priya H M[2], Saniya Fatima[3], and Varsha R[4]

Professor & Head, Dept. of CSE, K.S. School of Engineering & Management, Bengaluru, India[1]

Student, Dept of CSE, K.S. School of Engineering & Management, Bengaluru, India[2–4]

Abstract: The rapid growth of cloud-based collaboration platforms has introduced significant privacy concerns, as traditional systems expose sensitive user data to servers and third-party services during storage, indexing, and AI-based processing. Existing platforms routinely access user files for operational purposes, creating substantial risks for confidential information. This paper surveys recent privacy-preserving techniques including searchable encryption, end-to-end encryption, federated learning, and on-device AI inference, analyzing their strengths and limitations in the context of secure collaboration. Based on identified research gaps, we propose a unified Privacy-Preserving Intelligent Collaboration Platform that integrates client-side AES encryption, searchable symmetric encryption with secure tokens, RSA-based key sharing, and locally-executed AI inference to enable secure file storage, encrypted search, and intelligent features without exposing user data to servers.

Keywords: Privacy-Preserving Systems, Searchable Encryption, End-to-End Encryption, Client-Side AI, Federated Learning, Cloud Security, Secure Collaboration, AES Encryption, RSA Key Exchange, DevSecOps

I. INTRODUCTION

The proliferation of cloud collaboration platforms such as Google Drive, Dropbox, and Microsoft OneDrive has transformed how individuals and organizations manage and share digital information. While these platforms offer significant convenience and scalability, they fundamentally rely on server-side data access for indexing, storage management, and AIenhanced features. This architecture introduces considerable privacy risks, particularly for users handling sensitive personal, financial, or organizational data.

Traditional cloud platforms retain the ability to read, index, and process user files at the server level. Although encryption in transit and at rest is commonly applied, server-side decryption for indexing and AI processing means that user data is never truly private from service providers. High-profile data breaches and insider threats at cloud providers have further highlighted the inadequacy of conventional server-side security models.

Recent advances in cryptographic techniques, particularly Searchable Symmetric Encryption (SSE) and Public Key Encryption with Keyword Search (PEKS), have demonstrated pathways toward enabling search and retrieval operations directly over encrypted data without server-side decryption. Simultaneously, the emergence of lightweight on-device machine learning frameworks such as TensorFlow Lite and ONNX Runtime has made it feasible to execute AI inference locally on user devices, enabling intelligent features without transmitting sensitive content to external servers.

This paper surveys five representative studies published between 2004 and 2025 related to privacy-preserving storage, searchable encryption, federated learning, and hybrid encryption systems. The reviewed works are critically analyzed based on methodology, privacy guarantees, search capability, computational overhead, and deployment limitations. Based on identified research gaps, we propose a Privacy-Preserving Intelligent Collaboration Platform designed to integrate clientside encryption, searchable encryption, secure key exchange, and local AI inference within a unified mobile-first application.

A. Research Contributions

This survey and the associated proposed system make the following research contributions:

- A structured comparative analysis of recent privacy-preserving storage, searchable encryption, and client-side

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155241

AI systems.

- Identification of critical gaps in existing research related to integrated searchable encryption, mobile deployment, and AI-assisted features without server-side data exposure.
- Proposal of a unified privacy-preserving collaboration platform integrating AES encryption, searchable symmetric encryption, RSA key exchange, and on-device AI inference.
- Introduction of secure encrypted search token generation enabling keyword search over encrypted files without revealing search patterns to servers.
- Integration of client-side AI inference for document summarization and smart suggestions without transmitting sensitive data externally.

II. RELEVANT LITERATURE

A. Paper 1: Attribute-Based Searchable Encryption: A Survey (Yan et al., 2024)

Yan et al. [1] presented a comprehensive survey on Attribute-Based Searchable Encryption (ABSE) techniques designed to enhance privacy and fine-grained access control in cloud storage systems. The study analyzed various searchable encryption frameworks that combine attribute-based encryption with secure keyword search, enabling authorized users to retrieve encrypted data without exposing sensitive file contents or search keywords to cloud servers.

The survey examined different ABSE architectures, security models, indexing mechanisms, and access control strategies proposed in recent research. The authors highlighted how ABSE schemes improve confidentiality by enforcing attribute driven authorization policies while maintaining efficient encrypted search functionality. The paper also discussed applications of ABSE in healthcare, cloud computing, IoT, and secure data-sharing environments.

The study identified several challenges in existing ABSE systems, including high computational complexity, increased storage overhead, search latency, and difficulties in supporting dynamic attribute updates and large-scale deployment. The authors further emphasized the need for lightweight, scalable, and mobile-friendly searchable encryption solutions capable of integrating with modern AI-assisted cloud collaboration platforms.

B. Paper 2: Lightweight Public Key Encryption with Keyword Search (Wang et al., 2024)

Wang et al. [1] proposed a lightweight Public Key Encryption with Keyword Search (PEKS) scheme for secure cloud storage, enabling users to search encrypted files without revealing document contents or search keywords to the cloud server. The proposed method utilized encrypted keyword indexes and secure trapdoor generation to support privacy preserving keyword retrieval in public-key cryptographic environments.

The scheme established an efficient framework for secure cloud search, demonstrating that encrypted data can be searched securely while maintaining confidentiality. Experimental evaluation confirmed improved computational efficiency and scalability compared to traditional PEKS approaches, making the system suitable for mobile and resource-constrained devices.

Although the lightweight PEKS scheme reduced computation overhead, the approach still incurred higher processing costs than symmetric searchable encryption methods. The system also faced performance challenges when handling extremely large datasets and complex keyword matching operations.

C. Paper 3: Efficient and Privacy-Preserving Searchable Encryption for Cloud Storage (Chen et al., 2024)

Chen et al. [2] proposed a dynamic Searchable Symmetric Encryption (SSE) scheme designed to support efficient keyword searches over encrypted cloud storage while preserving data privacy. The framework introduced encrypted index structures that allow efficient document retrieval based on secure search tokens without revealing keyword or document content to the server.

The proposed scheme supported dynamic document updates including insertion and deletion operations, addressing a significant limitation of earlier static SSE systems. The system demonstrated improved search efficiency compared to previous SSE approaches while maintaining formal security guarantees against keyword guessing attacks.

Despite its improvements, the Chen et al. framework exhibited search pattern leakage, wherein repeated search queries could allow a server to infer relationships between searches. The system also introduced high index construction complexity and did not incorporate on-device AI processing, secure file sharing mechanisms, or end-to-end encryption compatible with mobile environments.

D. Paper 4: Federated Learning for Privacy-Preserving AI on Mobile Devices (Nguyen et al., 2024)

Nguyen et al. [3] proposed a federated learning framework enabling privacy-preserving AI model training across distributed mobile devices without transmitting raw user data to central servers. The framework utilized differential privacy mechanisms and secure aggregation protocols to protect individual user contributions during collaborative model training.

 This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IJARCCE.2026.155241

The study demonstrated that federated learning could enable mobile AI applications with meaningful privacy guarantees, supporting use cases including predictive text, document classification, and personalized recommendations without centralizing sensitive data.

However, the federated learning approach introduced substantial communication overhead and computational cost associated with model update transmission and aggregation. The framework focused exclusively on distributed model training and did not address encrypted file storage, searchable encryption over user data, or secure file sharing between users.

E. Paper 5: Privacy-Preserving Data Sharing in Cloud using Hybrid Encryption (Patel & Sharma, 2025)

Patel and Sharma [4] proposed a hybrid encryption framework combining AES symmetric encryption for bulk data encryption with RSA asymmetric encryption for secure key exchange in cloud storage environments. The framework enabled encrypted file sharing between users through encrypted key transmission, ensuring that servers could not access plaintext file contents.

The hybrid approach demonstrated practical applicability for secure cloud file sharing, offering strong confidentiality guarantees with reasonable performance for typical file sizes. The system provided a deployable architecture for client-side encryption with server-side ciphertext storage.

Despite its contributions, the Patel and Sharma framework exhibited key management complexity for multi-user environments and did not support search operations over encrypted files. The system also lacked AI-assisted features and was not evaluated within mobile deployment contexts, limiting its applicability to modern collaboration platforms.

F. Paper 6: Lightweight Cryptographic Techniques for Mobile Cloud Security (Singh & Verma, 2025)

Singh and Verma [5] explored lightweight cryptographic approaches targeting the performance-security trade-off in mobile cloud environments. The study evaluated multiple symmetric and asymmetric encryption schemes in the context of constrained mobile hardware, aiming to identify configurations that balance security strength with computational efficiency.

The research demonstrated that AES-128 with optimized key scheduling provided acceptable security while remaining computationally feasible on contemporary mobile processors. The study contributed benchmarking data useful for designing mobile security applications.

Although the Singh and Verma study provided useful performance insights, it focused primarily on encryption performance benchmarking and did not address searchable encryption, secure file sharing, AI integration, or practical deployment within collaborative platforms. The study also did not evaluate complete end-to-end privacy-preserving workflows.

III. COMPARATIVE ANALYSIS OF EXISTING SYSTEMS

Table I presents a structured comparison of the reviewed privacy-preserving storage, searchable encryption, and AI-assisted systems.

TABLE I. COMPARISON OF EXISTING RESEARCH ON PRIVACY-PRESERVING COLLABORATION SYSTEMS

Ref.	Year	Technique Used	Privacy Level	Search Support	Key Limitation
Yan et al.	2024	Attribute-Based Searchable Encryption (ABSE)	High	Fine-Grained Secure Search	High computational overhead
Wang et al.	2024	Lightweight PEKS (Public Key Encryption with Keyword Search)	High	Secure Keyword Search	Higher processing cost than symmetric encryption.
Chen et al.	2024	Dynamic SSE	Medium	Partial	Search pattern leakage
Nguyen et al.	2024	Federated Learning	High	None	High communication overhead
Patel & Sharma	2025	AES + RSA Hybrid	High	None	Complex key management
Singh & Verma	2025	Lightweight Crypto	Medium	Limited	Security vs performance trade-off

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155241

IV. GAP ANALYSIS

Based on the review of the five studies, the following critical gaps are identified in the existing literature.

A. Absence of Unified Integrated Platforms

Existing research primarily addresses individual privacy techniques independently. Searchable encryption systems generally do not incorporate AI-assisted features, while federated learning frameworks lack encrypted search and secure file sharing capabilities. No single deployable platform integrates searchable encryption, client-side AI inference, end-to-end encrypted storage, and secure multi-user file sharing within a unified mobile application.

B. Limited Mobile Deployment Readiness

Most reviewed systems were evaluated in server-side or desktop contexts and were not designed for mobile deployment. Lightweight mobile-compatible implementations combining searchable encryption with client-side AI inference remain largely unexplored in the literature.

C. Absence of Client-Side AI Integration

None of the reviewed privacy-preserving storage and encryption systems incorporated on-device AI inference. Intelligent features such as document summarization, smart suggestions, and content classification are absent from existing privacypreserving collaboration platforms.

D. Search Pattern Leakage in Existing SSE Systems

Dynamic SSE schemes reviewed in the literature exhibit search pattern leakage vulnerabilities that could allow server-side inference of search query relationships. More secure token-based search mechanisms suitable for practical mobile deployment remain an active research challenge.

E. Limited Practical Deployment Orientation

Most reviewed systems remain research-oriented cryptographic constructions without practical deployment-oriented implementations suitable for real-world mobile collaboration environments. Integration with modern mobile development frameworks and cloud backend services is largely absent from existing research.

V. PROPOSED SYSTEM DESIGN

A. System Overview

To address the identified gaps, we propose a Privacy-Preserving Intelligent Collaboration Platform. The proposed system integrates client-side AES file encryption, searchable symmetric encryption with secure keyword tokens, RSA-based key exchange for secure file sharing, and locally-executed AI inference within a unified mobile application built using Flutter.

The system is designed as a privacy-first collaboration platform capable of supporting secure file storage, multi-user sharing, keyword search over encrypted files, and intelligent AI-assisted features without exposing user data to servers or third-party services.

B. System Workflow

The proposed workflow follows a structured sequence:

- User registers and generates a local RSA key pair stored securely on the device.
- Files are encrypted using AES on the client device before upload to the cloud backend.
- Encrypted search tokens are generated from file keywords and stored alongside encrypted files.
- Search queries generate matching tokens that are compared against stored tokens without revealing plaintext keywords.
- File sharing is performed by encrypting the AES file key with the recipient's RSA public key.
- On-device AI models perform document summarization and smart suggestions locally.
- Only ciphertext, encrypted tokens, and encrypted keys are transmitted to or stored on the server.

C. AI Components

The proposed platform incorporates two primary on-device AI-assisted components:

AI Component 1: Document Summarization Engine — This module utilizes a lightweight transformer-based model running locally on the user device to generate concise summaries of decrypted documents, enabling intelligent content overview without transmitting document content externally.

AI Component 2: Smart Suggestion Engine — This module analyzes locally decrypted file metadata and content patterns to generate contextual suggestions for file organization, sharing recommendations, and collaboration workflows without server-side data processing.

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155241

D. Key Parameters

The proposed system incorporates the following major features:

- Client-side AES-256 file encryption before upload
- Searchable symmetric encryption with secure keyword token generation
- RSA-2048 key exchange for secure multi-user file sharing
- JWT-based authentication with encrypted cloud storage backend
- On-device AI inference for document summarization and smart suggestions
- Privacy-preserving collaboration with no server-side plaintext data access
- Cross-platform mobile application using Flutter/React Native

VI. EXPECTED OUTCOMES AND BENEFITS

A. Enhanced Privacy Guarantees

By performing all encryption and AI processing on the client device, the proposed platform ensures that servers cannot access plaintext file contents, search queries, or AI-processed data. This provides substantially stronger privacy guarantees than conventional cloud storage platforms.

B. Practical Searchable Encryption

The token-based searchable encryption mechanism enables efficient keyword search over encrypted files without revealing search patterns to the server. This addresses a significant limitation of existing SSE approaches while maintaining search usability for end users.

C. Intelligent Features Without Privacy Compromise

Client-side AI inference enables document summarization, smart suggestions, and content classification features comparable to server-side AI platforms, while preserving complete user data privacy. The platform demonstrates that intelligence and privacy can coexist in collaborative applications.

D. Secure Multi-User Collaboration

RSA-based key exchange enables secure file sharing between users without exposing file encryption keys to the server. Authorized users can decrypt shared files locally after receiving encrypted key packages, supporting safe multi-user collaboration with complete privacy control.

VII. CONCLUSION AND FUTURE WORK

This paper presented a comprehensive survey of recent privacy-preserving storage, searchable encryption, federated learning, and hybrid encryption systems. The reviewed studies demonstrate the growing importance of cryptographic privacy techniques within cloud collaboration environments. However, significant limitations remain regarding integrated deployable platforms that combine searchable encryption with on-device AI inference and practical mobile deployment.

To address these gaps, we proposed a Privacy-Preserving Intelligent Collaboration Platform integrating client-side AES encryption, searchable symmetric encryption with secure token generation, RSA key exchange for secure file sharing, and locally-executed AI inference within a unified mobile application.

Future work will focus on implementation and evaluation of the proposed platform using real-world collaboration scenarios, formal security analysis of the searchable encryption token scheme, and optimization of on-device AI model performance for resource-constrained mobile hardware environments.

VIII. ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the Department of Computer Science and Engineering, K. S. School of Engineering and Management (KSSEM), Bengaluru, for providing an excellent academic and research environment for this work. We extend our heartfelt thanks to our project guide, Dr. K Venkat Rao, Assistant Professor, Department of Computer Science and Engineering, for his valuable guidance, encouragement, and continuous support throughout the preparation of this paper. We also acknowledge the contributions of the cryptography and privacy research community whose foundational work provided valuable insights for this survey and proposed system.

REFERENCES

[1]. L. Yan, G. Wang, T. Yin, P. Liu, H. Feng, W. Zhang, H. Hu, and F. Pan, “Attribute-Based Searchable Encryption: A Survey,” *Electronics*, vol. 13, no. 9, p. 1621, 2024.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155241

[2]. W. Wang, X. Liu, and H. Zhang, "Lightweight Public Key Encryption with Keyword Search for Secure Cloud Storage," IEEE Access, vol. 12, 2024.

[3]. Y. Chen, J. Li, and K. Zhang, "Efficient and Privacy-Preserving Searchable Encryption for Cloud Storage," IEEE Access, vol. 12, 2024.

[4]. T. Nguyen, M. Pathak, et al., "Federated Learning for Privacy-Preserving AI on Mobile Devices," IEEE Communications Surveys & Tutorials, vol. 26, no. 2, 2024.

[5]. R. Patel and A. Sharma, "Privacy-Preserving Data Sharing in Cloud using Hybrid Encryption," Springer Lecture Notes in Networks and Systems, 2025.

[6]. P. Singh and D. Verma, "Lightweight Cryptographic Techniques for Mobile Cloud Security," in Proc. International Conference on Emerging Trends in Computing, 2025.

 This work is licensed under a Creative Commons Attribution 4.0 International License