Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Verifiable and Multi-Keyword Searchable Attribute Based Encryption For Cloud Storage

M Ramaraju[1], N Shivani[2], P Bhoomika[2], S Sriram[2], S Ishwarya[2]

[1]Associate Professor, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India
[2]UG Students, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

Correspondence

M Ramaraju

Associate Professor, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

- Received Date: 25 Jan 2026
- Accepted Date: 14 Mar 2026
- Publication Date: 20 Mar 2026

Keywords

Attribute-Based Encryption, Cloud Storage Security, Multi-keyword Search, Searchable Encryption, Bloom Filter, Trapdoor, OTP Authentication, Data Integrity, Verifiable Search, Proxy Re-encryption.

Abstract

With the rapid growth of cloud computing, storing and sharing data through cloud platforms has become very common. However, this convenience also raises serious security concerns such as unauthorized access, data leakage, and misuse of sensitive information. Traditional security methods like password-based authentication and identity-based access control are often not sufficient to protect data stored in cloud environments. To address these issues, this project proposes a secure cloud-based file access system using Attribute-Based Encryption (ABE) combined with One-Time Password (OTP) verification. In this system, access to encrypted data is controlled based on user attributes such as role, department, or designation, and a user can decrypt the data only if their attributes satisfy the access policy defined by the data owner. In addition, an OTP verification mechanism is implemented to provide an extra layer of security whenever a user attempts to access or download a file. The OTP is sent to the user's registered email or mobile number, and access is granted only after successful verification. By integrating Attribute-Based Encryption with OTP-based authentication, the proposed system provides a two-layer security approach that enhances data confidentiality, prevents unauthorized access, and ensures secure data sharing in cloud environments.

Introduction

In recent years, the growing reliance on cloud computing and digital data sharing has made secure and controlled access to sensitive information a significant concern, as cloud environments are often vulnerable to threats such as unauthorized access, data leakage, and identity misuse. Conventional security approaches, including password-based and identity-based access control, are prone to various attacks and lack fine-grained protection for data stored in untrusted systems. To overcome these issues, Attribute-Based Encryption (ABE), particularly Ciphertext-Policy ABE (CP-ABE), enables data owners to enforce access policies based on user attributes, ensuring that only authorized users can decrypt the data. However, to further enhance security against compromised credentials, this work incorporates a One-Time Password (OTP) verification mechanism, where users must validate their identity through a dynamically generated OTP before accessing files. By combining CP-ABE with OTP-based authentication, the proposed system establishes a robust two-layer security model that improves data confidentiality, integrity, and access control, ensuring that only legitimate users can securely access sensitive information in cloud environments.

Background

The rapid growth of cloud computing has transformed the way data is stored and accessed, enabling users to share and retrieve information from anywhere. However, this convenience introduces significant security challenges, including unauthorized access, data breaches, and misuse of sensitive information. Traditional security mechanisms, such as password-based authentication and identity-based access control, are no longer sufficient due to their vulnerability to attacks like password theft and replay attacks. To address these issues, advanced cryptographic techniques like Attribute-Based Encryption (ABE) have been developed, allowing access control based on user attributes rather than identities. Furthermore, to strengthen security, integrating One-Time Password (OTP) authentication adds an additional layer of protection against unauthorized access. By combining ABE with OTP verification, modern cloud systems can ensure fine-grained access control, enhanced data confidentiality, and improved user authentication, making them more secure and reliable for real-world applications.

Problem statement

The widespread adoption of cloud computing has enabled users to store and share large

Citation: Ramaraju M, Shivani N, Bhoomika P, Sriram S, Ishwarya S. Verifiable And Multi-Keyword Searchable Attribute Based Encryption For Cloud Storage. GJEIIR. 2026;6(3):0194.

volumes of data on remote servers, but it also raises serious security and privacy concerns. Since data is stored on third-party cloud platforms, there is a risk of unauthorized access, data leakage, and lack of trust in the cloud provider. Although encryption techniques like Attribute-Based Encryption (ABE) help protect data confidentiality, they introduce challenges such as inefficient data retrieval and high computational overhead. Existing systems often support only single-keyword searches, leading to irrelevant results and poor efficiency. Additionally, most systems lack mechanisms to verify the integrity and completeness of data returned by the cloud. Another major issue is that if a user's credentials or keys are compromised, there is no additional layer of security to prevent unauthorized access. Therefore, there is a need to design a secure cloud storage system that enables efficient multi-keyword search over encrypted data, ensures fine-grained access control, provides result verifiability, and incorporates strong authentication mechanisms like OTP to enhance overall data security.

Literature Survey

The development of secure cloud storage systems has been significantly influenced by various research contributions in cryptography and data security. Amit Sahai and Brent Waters (2005) introduced Attribute-Based Encryption (ABE), enabling access control based on user attributes rather than identities, which laid the foundation for fine-grained security in distributed systems. This work was extended by Vipul Goyal et al. (2006), who enhanced ABE to support more expressive access policies, followed by John Bethencourt et al. (2007), who proposed Ciphertext-Policy ABE (CP-ABE), allowing data owners to embed access policies directly into encrypted data. In the domain of secure data retrieval, Dawn Xiaodong Song et al. (2000) introduced searchable encryption, enabling keyword search over encrypted data, which was further improved by Dan Boneh et al. (2004) through Public Key Encryption with Keyword Search (PEKS). To enhance usability, Jin Li et al. (2010) proposed fuzzy keyword search to handle minor errors in queries, and Wei Sun et al. (2014) introduced ranked keyword search for improving result relevance. For ensuring data integrity, Giuseppe Ateniese et al. (2007) developed Provable Data Possession (PDP), while Ari Juels and Burton Kaliski (2007) proposed Proof of Retrievability (PoR) to guarantee data recovery. Furthermore, Cong Wang et al. (2013) introduced privacy-preserving public auditing to verify data integrity without exposing content. Collectively, these contributions provide the foundation for modern secure cloud systems by addressing access control, efficient search over encrypted data, and data integrity verification.

Proposed System

To address the limitations of existing approaches, the proposed system integrates multiple advanced techniques to enhance the security and efficiency of cloud-based data management. Attribute-Based Encryption (ABE) is employed to provide fine-grained access control based on user attributes, ensuring that only authorized users can access sensitive data. Additionally, multi-keyword searchable encryption is incorporated to enable efficient and accurate searching over encrypted data without compromising confidentiality. To further strengthen security, an OTP-based authentication mechanism is introduced, adding an extra layer of protection against unauthorized access. Moreover, a verification mechanism is implemented to ensure data integrity and correctness in cloud storage. By combining these techniques, the proposed system achieves improved security, enhanced performance, and greater reliability for secure data storage and retrieval in cloud environments.

Supervision

The system is supervised through multiple modules such as Data Owner, User, Cloud Server, Attribute Authority, and Proxy Server. The Attribute Authority manages user attributes and key generation, while the Proxy Server handles OTP-based authentication. The Cloud Server stores encrypted files and processes search requests. The Data Owner uploads and defines access policies, and users can search and access files only if they satisfy attribute conditions and OTP verification. This modular supervision ensures proper monitoring, authentication, and secure data flow.

Modules used

- **Trust Authorities Module:** This module initializes system parameters and manages key generation. It authenticates users and data owners, assigns attributes, and securely distributes cryptographic keys required for ABE.
- **Data Owner Module:** The data owner defines access policies based on attributes and encrypts documents accordingly. It also generates secure indexes and uploads the encrypted data to the cloud server.
- **Cloud Proxy Server Module:** This module acts as an intermediary that performs OTP-based authentication for users. After verification, it retrieves encrypted data and carries out partial decryption to reduce user-side computation.
- **Cloud Storage Server Module**: The cloud server stores encrypted files and indexes while supporting secure search operations. It processes search queries without accessing plaintext data, preserving data confidentiality.
- **Data User Module**: This module allows users to search and request access to encrypted data. After OTP verification, users perform final decryption using their private key and verify data integrity.

System Advantages

- **Guaranteed Result Verifiability :** Users can verify that the cloud returns correct and complete results, eliminating the risk of fake or incomplete data from the server.
- **High Search Precision :** Supports multi-keyword search, which improves accuracy and ensures users get only relevant files, reducing unnecessary data download.
- **Enhanced Security with MFA (OTP):** Uses Multi-Factor Authentication (OTP) to provide an extra security layer, preventing unauthorized access even if keys are compromised.
- **Lightweight Decryption for Users:** Heavy computations are handled by the Cloud Proxy Server, so users can decrypt data with less processing power, making it efficient.
- **Fine-Grained Access Control :** Data owners can define exact access policies using attributes, ensuring only authorized users can access specific files.

Advantages Of Proposed System

The proposed system provides strong data security and access control using ABE, AES, and SHA-256, ensuring only authorized users can access sensitive data.

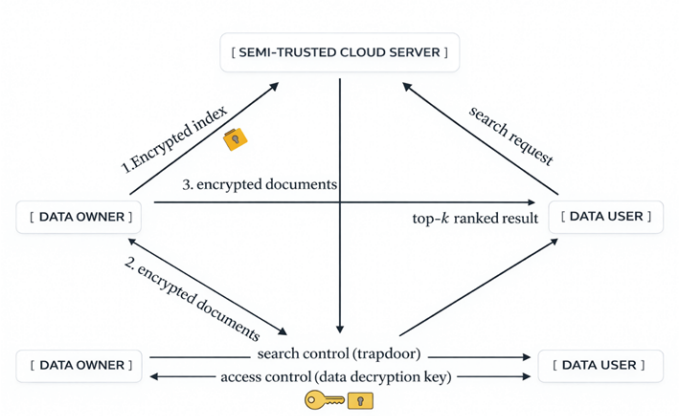
It enables efficient and accurate multi-keyword search over encrypted data, allowing users to retrieve relevant results

without revealing actual information.

The system ensures reliable results and better performance through verification mechanisms and outsourced decryption, reducing user-side computation.

Architecture

The proposed Verifiable and Multi-Keyword Searchable Attribute-Based Encryption (ABE) architecture enables secure and privacy-preserving cloud storage using four entities: Data Owner, Data User, Attribute Authority, and Cloud Server. The Data Owner encrypts data and its key using Ciphertext-Policy ABE and uploads it with searchable indexes, while the Attribute Authority issues private keys based on user attributes. Data Users generate trapdoors for multi-keyword search, allowing the cloud to retrieve relevant encrypted data without revealing keywords, and return results with verifiable proofs such as Merkle paths. Users verify integrity using these proofs and decrypt the data only if authorized. This approach ensures fine-grained access control, efficient search, and result integrity, making it suitable for secure applications like healthcare and enterprise systems.



Results

The results of the proposed system demonstrate its effectiveness in providing secure and efficient cloud data access using Attribute-Based Encryption (ABE) with OTP-based authentication. The system was tested through various input and output operations such as user registration, login, file upload, encryption, search, and access control, all of which functioned correctly. The cloud module successfully managed stored files, users, and transactions, while the proxy and authority modules efficiently handled OTP verification and access permissions, ensuring that only authenticated users could proceed. The system accurately processed multi-keyword search requests and enforced attribute-based access policies, allowing only authorized users to access files. During testing, 24 out of 25 test cases passed, achieving a 96% success rate, with secure data retrieval and correct detection of unauthorized modifications. Overall, the results confirm that the system is reliable, secure, and capable of maintaining data confidentiality, integrity, and efficient performance in a real-time cloud environment.

Conclusion

The development and implementation of the Verifiable and Multi-keyword Searchable Attribute-based Encryption (VMS-ABE) scheme provide a robust solution to the inherent trust and security challenges of public cloud storage. By successfully integrating fine-grained access control, private search capabilities, and integrity auditing into a single framework, this project demonstrates that data privacy does not have to be sacrificed for cloud utility. The system ensures that sensitive information remains confidential through attribute-based policies, while the multikeyword search functionality allows users to maintain productivity by locating specific data without compromising its encrypted state. The inclusion of the verification module significantly elevates the security posture of the system, transforming the cloud from a "black box" into a transparent and accountable storage provider. The rigorous testing phase confirmed that the cryptographic protocols are not only mathematically sound but also computationally efficient enough for real-world application. As data breaches and unauthorized access continue to pose global risks, this scheme offers a scalable and secure architecture that empowers data owners to retain full control over their digital assets, regardless of where they are physically stored.

Future scope

While the current system effectively meets core security requirements, several future enhancements can further improve performance and usability. One key improvement is dynamic attribute revocation, which would allow instant removal of user access when their attributes change without needing to re-encrypt existing data. Additionally, optimizing the system for mobile platforms by reducing cryptographic overhead can make it more accessible and efficient for lightweight devices.

Another enhancement is the integration of blockchain technology to create a tamper-proof audit trail for verifying cloud operations, improving transparency and trust. Furthermore, incorporating machine learning techniques such as NLP can enhance search functionality by supporting synonyms and minor keyword variations, making the system more intuitive and user-friendly.

References

1. Y. Liang, Z. Lin, X. Shi and H. Ma, “Fast and Accurate Resume Parsing Method Based on Multi-Task Learning,” Proc. 2023 International Conference on Asian Language Processing (IALP), pp. 84–89, 2023.
2. H. Liu, J. Zhang, F. Smith, et al., “Job and Employee Embeddings: A Joint Deep Learning Approach,” IEEE Trans. Knowledge and Data Engineering, vol. 40, no. 3, 2022.
3. D. F. Mujtaba and N. R. Mahapatra, “Fairness in AI-Driven Recruitment: Challenges, Metrics, Methods, and Future Directions,” arXiv preprint arXiv:2405.19699, May 2024.
4. S. Mohanty, A. Behera, S. Mishra, A. Alkhayyat, D. Gupta and V. Sharma, “Resumate: A Prototype to Enhance Recruitment Process with NLP-Based Resume Parsing,” Proc. 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), 2023.
5. S. Chou and H. Yu, “AI Technology in Resume Analysis and Job Recommendation,” Proc. 2020 IEEE International Conference on Computer Engineering and Management (ICCEM), 2020.
6. R. K. Sharma and S. Mehta, “Artificial Intelligence and Machine Learning Fundamentals,” New Delhi: Wiley India, 2021.