



International Journal of Advanced Research in Education and Technology (IJARETY)

Volume 13, Issue 3, May - June 2026

Impact Factor: 9.971



Efficient Access Control for Cloud Based User Data Storage and Sharing

Shaikh Mohamad¹, Uppari Smrithi Raj², K.B. Varun Kumar Reddy³, Thokala Manideep⁴

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India¹

Department of CSE, Guru Nanak Institute of Technology, Hyderabad, India^{2,3,4}

ABSTRACT: Cloud computing provides flexible and scalable data storage services, but ensuring data security and privacy in cloud environments remains a major challenge. Traditional cloud storage systems expose sensitive information to unauthorized access and cyber threats. This paper presents an efficient searchable encryption scheme for secure cloudbased user data storage and sharing. The proposed system supports privacy-preserving data retrieval using regular language searchable encryption and deterministic finite automata (DFA)-based searching techniques. The system protects encrypted cloud data from unauthorized access and offline keyword guessing attacks while ensuring efficient search performance. The proposed framework improves confidentiality, integrity, and secure data sharing in cloud environments.

KEYWORDS: Cloud Computing, Searchable Encryption, Data Security, Privacy Preservation, DFA, Keyword Search, Cloud Storage

I. INTRODUCTION

Cloud storage has become an important component of modern computing because it allows users to store, manage, and access data from anywhere through the internet. Organizations and individuals increasingly depend on cloud services for scalable and cost-effective data management. However, storing sensitive data on remote cloud servers introduces major security and privacy concerns. Since cloud servers are controlled by third-party providers, users lose direct control over their information. This project focuses on designing an efficient and secure searchable encryption mechanism for cloud environments.

II. LITERATURE SURVEY

Li et al. (2016) Li et al. proposed efficient traffic usage techniques for cloud synchronization services such as Dropbox, Google Drive, and OneDrive. Their research mainly focused on improving the efficiency of data synchronization between local devices and cloud servers. They also analyzed traffic usage efficiency in different cloud storage services through experiments and real-world data analysis. Their work helped cloud providers optimize synchronization mechanisms and improve overall network performance. The proposed techniques reduced communication overhead and enhanced user experience in cloud environments.

Sookhak et al. (2017) Their approach ensured that outsourced cloud data remained secure and unaltered without requiring users to store data locally. The system supported dynamic operations such as data insertion, deletion, modification, and updating. They also designed an efficient data structure called Divide and Conquer Table (DCT) to reduce computational overhead during auditing processes. Their framework improved the reliability, integrity, and security of large-scale cloud storage systems. The proposed method significantly reduced communication and computation costs for both cloud servers and auditors.

Zhang et al. (2017) Their work focused on improving data classification accuracy while maintaining privacy in cloud environments. The researchers proposed a Double Projection Deep Computation Model (DPDCM) for efficient feature extraction from large datasets. To preserve privacy, they integrated encryption mechanisms based on the BGV encryption scheme into the learning process. Cloud computing resources were utilized to improve training efficiency through distributed data processing.

III. EXISTING SYSTEM

Cloud storage systems have become widely popular because they provide users with scalable storage, remote accessibility, and cost-effective data management services. Individuals and organizations can store large amounts of data on cloud servers and access them anytime from anywhere using internet-enabled devices. Although cloud storage offers flexibility and convenience, it also introduces serious security and privacy concerns because sensitive data is stored on third-party servers that are not fully trusted.

To protect confidential information, traditional cloud systems use encryption techniques before uploading data to the cloud. However, once the data is encrypted, searching over encrypted files becomes difficult. Existing searchable encryption schemes allow users to search encrypted data using keywords, but most of these methods support only simple exact keyword matching. They do not provide flexible and expressive search capabilities such as pattern matching, regular expression search, or advanced query processing.

Another major limitation of traditional searchable encryption systems is their vulnerability to security attacks. In many systems, attackers can perform offline keyword guessing attacks by analyzing search tokens or encrypted indexes to predict user search keywords. This creates a significant risk to user privacy and may lead to unauthorized access to sensitive information. Furthermore, many existing systems depend heavily on centralized cloud servers, which increases the chances of data leakage, insider attacks, and single-point failures.

Existing System Disadvantages

- ❑ Limited support for flexible and expressive search operations.
- ❑ Increased risk of unauthorized data access.
- ❑ Weak resistance against keyword guessing attacks.
- ❑ High computational overhead during encrypted data retrieval.

IV. PROPOSED SYSTEM

The proposed system introduces an advanced and efficient searchable encryption framework for secure cloud-based data storage and sharing. The framework is designed to enhance both security and search efficiency while preserving user privacy. It enables users to securely upload encrypted files to the cloud and perform keyword-based searches without revealing the actual content of the files or search queries to the cloud server.

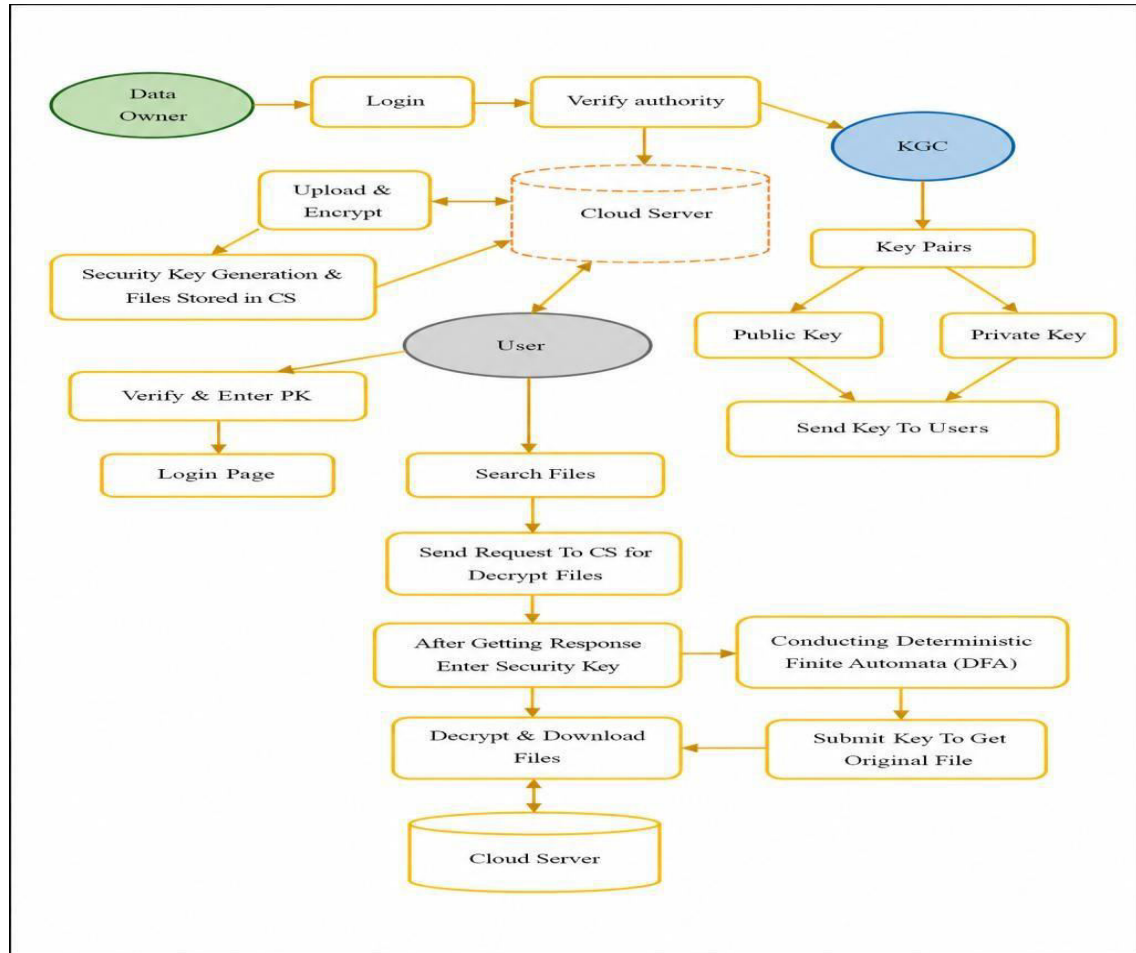
The system supports Regular Language Searchable Encryption (RLSE) and Deterministic Finite Automata (DFA)-based encrypted data retrieval techniques. Using DFA-based searching, the framework can process more expressive and flexible search patterns compared to traditional exact keyword search methods. This allows users to perform advanced search operations efficiently on encrypted cloud data while maintaining complete confidentiality.

To strengthen security, the proposed system incorporates robust cryptographic mechanisms that protect against offline keyword guessing attacks. Search tokens and encrypted indexes are generated securely so that attackers cannot infer the actual keywords even if they gain access to the encrypted data or search patterns. The framework ensures that the cloud server learns nothing about the stored data or user queries except the minimum necessary search results.

Advantages:

- ❑ Provides secure and privacy-preserving cloud data storage.
- ❑ Supports efficient encrypted keyword searching.
- ❑ Protects against offline keyword guessing attacks.
- ❑ Enhances data confidentiality and access control.

V. SYSTEM ARCHITECTURE



System Architecture

The proposed system architecture is designed to provide secure cloud-based data storage and searchable encryption. The system consists of five main entities: User Interface, Key Generation Center (KGC), Data Owner, Cloud Server, and Data User. The KGC generates secure public and private keys for authorized users, while the Data Owner encrypts files before uploading them to the cloud server. The Cloud Server stores encrypted data and performs secure search operations without revealing the original content. The Data User retrieves encrypted files using secure search tokens and decrypts them using valid keys.

VI. METHODOLOGY

The proposed methodology combines searchable encryption with regular language matching and Deterministic Finite Automata (DFA)-based retrieval.

MODULES NAME:

1. User Interface Design
2. Key Generation Center
3. Cloud Server
4. Data Owner
5. Data User

Modules Explanation:

User Authentication:

☐ Users must first register into the system by providing valid details such as username and password. After registration, users can securely log into the application using their credentials. The authentication mechanism verifies user identity and prevents unauthorized access to cloud resources and sensitive data.

1. Key Generation:

☐ The Key Generation Center (KGC) is responsible for generating secure public and private keys for all authorized users. These keys are used during encryption and decryption processes to maintain data confidentiality and privacy. The generated keys are securely distributed and managed within the system.

2. File Encryption:

☐ Before uploading files to the cloud server, the data owner encrypts sensitive information using searchable encryption algorithms. Encryption converts plaintext data into unreadable ciphertext, ensuring that unauthorized users cannot access the original content. This improves security for cloud-stored data.

4. Secure Data Storage:

☐ The encrypted files are securely stored on the cloud server along with encrypted search indexes. Since the data is stored in encrypted form, even if the cloud server is compromised, attackers cannot understand or misuse the information. This ensures strong data privacy and protection.

5. Secure Search Mechanism:

☐ Authorized data users generate secure search tokens using their private keys to perform keyword-based searches on encrypted cloud data. The cloud server uses DFA-based matching algorithms to identify relevant encrypted files without revealing the actual data or search keywords. This enables efficient and privacy-preserving searching.

6. Data Retrieval:

☐ After successful verification of the search request, the cloud server returns the matching encrypted files to the authorized user. The user then decrypts the files locally using valid decryption keys to obtain the original information securely. This process ensures safe and controlled data access.

VII. IMPLEMENTATION

The implementation of the proposed system focuses on secure cloud-based data storage and privacy-preserving searchable encryption. The frontend interface is designed using Java Swing for secure interaction between users and the cloud environment. The backend handles encryption, authentication, and cloud communication operations.

The system supports:

- Secure login and registration
- Public and private key generation
- File encryption and upload
- DFA-based searchable encryption
- Secure data retrieval and decryption

Algorithm Used

Existing Algorithm

Traditional searchable encryption methods support only limited keyword-based searches and often suffer from high overhead and security vulnerabilities.

Proposed Algorithm

The proposed searchable encryption algorithm allows users to search encrypted data without revealing the original content. Users generate secure search tokens using private keys. The cloud server performs matching operations directly on encrypted data using Deterministic Finite Automata (DFA)-based retrieval techniques.

The algorithm provides:

- Privacy-preserving search operations
- Efficient encrypted data retrieval
- Resistance against keyword guessing attacks
- Improved scalability and performance

VIII. EXPERIMENTAL RESULTS



Figure 1: Home Page

This screen represents the **home page of the system**, providing a centralized entry point for all users including User, Cloud Server, Data Owner. It offers a simple and user-friendly interface for accessing different cloud services securely.

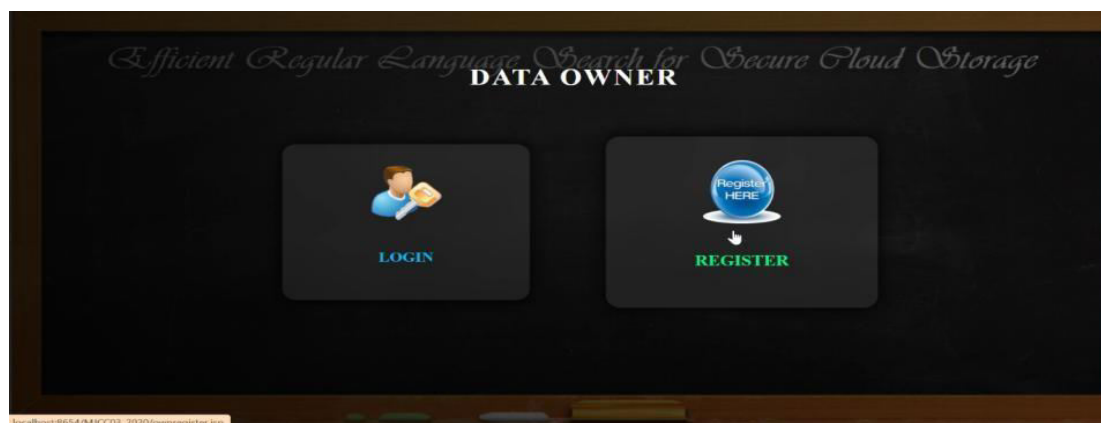


Figure 2: Data Owner Module

This snapshot shows the Data Owner interface containing Login and Register options. New users can create accounts using the Register option, while existing users can securely log into the system using valid credentials.

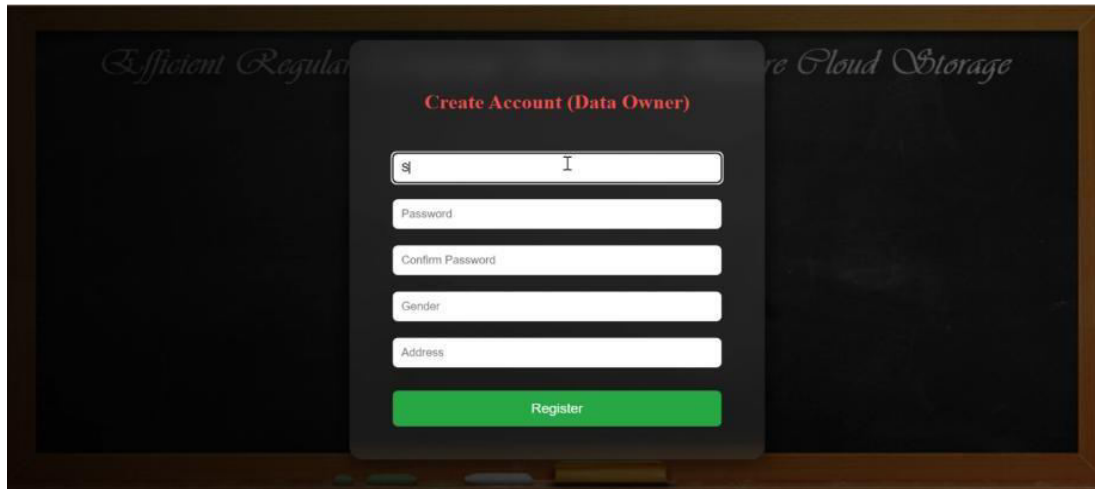
A screenshot of a web application interface for creating a new account. The background is dark with a light blue border. At the top, the text "Efficient Regular Language Search for Secure Cloud Storage" is written in a light blue, cursive font. In the center, there is a white rectangular box with a red title "Create Account (Data Owner)". Inside this box, there are five input fields: "Username" (with a cursor), "Password", "Confirm Password", "Gender", and "Address". Below these fields is a green button labeled "Register".

Figure 3: Data Owner Registration Page

This snapshot illustrates the registration process for data owners. Users enter details such as username, password, gender, and address to create secure accounts for accessing cloud storage services.



Figure 4: File Upload Success Page

This snapshot shows the successful upload of encrypted files to the cloud server. After encryption, the files are securely stored in the cloud, ensuring data confidentiality and privacy protection. The experimental results confirm that the proposed system successfully supports secure cloud storage, searchable encryption, authorized access control, and privacy-preserving data management with efficient performance.

IX. CONCLUSION

Cloud computing provides significant advantages for data storage and sharing, but security and privacy concerns remain major challenges. The proposed searchable encryption system provides secure cloud-based data storage and privacy-preserving data retrieval using regular language encryption and DFA-based search mechanisms. The system protects sensitive cloud data from unauthorized access and keyword guessing attacks while supporting efficient search functionality. Experimental analysis shows that the proposed approach improves security, scalability, and search efficiency compared with traditional searchable encryption methods.

X. FUTURE ENHANCEMENT

In future, the proposed system can be enhanced by integrating Artificial Intelligence and Machine Learning techniques for intelligent threat detection and secure access monitoring. The framework can also support multi-cloud environments to improve scalability, reliability, and distributed data storage management. Blockchain technology may be incorporated to provide decentralized access control and tamper-proof auditing of cloud activities. The system can be extended to support biometric authentication methods such as fingerprint or facial recognition for stronger user verification. Advanced searchable encryption techniques with semantic search capabilities can be implemented to improve search accuracy and flexibility over encrypted data.

REFERENCES

- [1] Li Z, Dai Y, Chen G, et al., "Toward Network-Level Efficiency for Cloud Storage Services," IEEE Transactions on Cloud Computing, 2016.
- [2] Sookhak M, Gani A, Khan M.K., et al., "Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing," Information Sciences, 2017
- [3] Zhang Q, Yang L.T., Chen Z, Li P., "Privacy-Preserving Double Projection Deep Computation Model," IEEE Transactions on Big Data, 2017.
- [4] Liu J.K., Liang K., Susilo W., et al., "Two-Factor Data Security Protection Mechanism for Cloud Storage System," IEEE Transactions on Computers, 2016.
- [5] Boneh D., Waters B., "Conjunctive, Subset, and Range Queries on Encrypted Data," Theory of Cryptography Conference, 2007.
- [6] Q. Zheng, S. Xu, and G. Ateniese, "VABKS: Verifiable Attribute-Based Keyword Search Over Outsourced Encrypted Data," IEEE INFOCOM, 2014.



International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 9.971