Search over Encrypted Data Using Advanced AES & Parallels Computing

Shubhada Lohake[1],Samruddhi Jadhav[2] ,Anushka Gijare[3] ,Sharvari Mindhe[4] ,Phadale T. I.[5]
[1,2,3,4]Student, Department of Computer Engineering, Jaihind Polytechnic, Kuran, Pune
[5]Lecturer, Department of Computer Engineering, Jaihind Polytechnic, Kuran, Pune

Abstract — In the modern era of cloud computing, data security and privacy have become critical concerns. Organizations often outsource their data to third-party cloud servers for storage and management, which raises the risk of unauthorized access. To address this, the proposed system enables secure search operations over encrypted data using Advanced Encryption Standard (AES) combined with parallel computing techniques. AES ensures strong encryption and confidentiality of stored data, while parallel computing enhances the efficiency and speed of encryption, decryption, and search processes. The system allows users to perform keyword-based searches without revealing the data or search queries to the server. This approach achieves both data privacy and high performance, making it suitable for large-scale, real-time cloud storage applications. The proposed model ensures minimal latency, optimized resource utilization, and robust protection against data breaches.

Keywords— Searchable Encryption, AES Encryption, Parallel Computing, Cloud Security, Data Privacy, Secure Search, Cryptograpghy, Data Confidentiality, Encrypted Database, High Performance Computing.

I. INTRODUCTION

Cloud computing provides on-demand access to shared resources like servers, storage, and applications through the internet. It helps individuals and organizations store and manage large amounts of data without maintaining expensive hardware. Because of its scalability, flexibility, and low cost, cloud storage is widely used by businesses, government sectors, and individuals.

However, storing sensitive data such as financial records, medical information, or personal details on third-party cloud servers raises security and privacy concerns. To protect this data, it is encrypted before being stored in the cloud. Encryption keeps the data safe but makes it difficult to search within the stored information.

To solve this problem, Searchable Encryption (SE) techniques are used. These techniques allow users to search for specific keywords in encrypted data without revealing the actual data or the search query to the cloud server. The system ensures data security, efficient searching, and privacy protection.

II. LITERATURE REVIEW

Several researchers have proposed different techniques to improve secure keyword search over encrypted cloud data. Tianyue Peng introduced a ranked multi-keyword search scheme that allows multiple data owners to encrypt files with different keys and use a tree-based index structure for efficient searching. Xiang Gao proposed a method for keyword-based cloud data integrity auditing using a special label (RAL) that verifies files without revealing sensitive information.

Jianchao Tang developed an encrypted database query scheme using double AES encryption to protect against frequency attacks while maintaining efficient queries. Xueyan Liu proposed an attribute-based keyword search scheme with data deduplication and verifiable search results to improve data confidentiality and efficiency.

Hua Dai introduced a privacy-preserving multi-keyword ranked search method for hybrid clouds, improving search efficiency through clustering and partition algorithms. Osama Ahmed Khashan developed OutFS, an encrypted file system that secures outsourced cloud files using hybrid encryption and identity-based encryption for safe file sharing.

Alexandros Bakas proposed a hybrid encryption scheme combining searchable encryption and attribute-based encryption to enable secure data sharing and access control. Lianggui Liu introduced

mechanisms for ranked keyword search and category group indexing to improve search speed, reduce storage cost, and support data updates. Lili Zhang proposed a secure multi-attribute keyword search scheme that supports document insertion and deletion with efficient indexing. Lingbing Tao developed a feature-based joint keyword matching technique to reduce index size and improve search efficiency.

Xinrui Ge presented a verifiable keyword search scheme that ensures correctness of search results using secure index structures. Dan Yang proposed a privacy-preserving similarity search scheme using CP-ABE and garbled circuits for secure data search.

Finally, Xiaoxia Dong developed a privacy-preserving regression model over encrypted data to support secure data analysis in the cloud.

Overall, these studies focus on improving security, privacy, efficiency, and scalability in searching encrypted cloud data while ensuring that sensitive information remains protected.

III. PROPOSED SYSTEM

The proposed system provides a secure and efficient method to perform keyword searches over encrypted data stored in the cloud. In this system, the data owner encrypts the files and creates a secure keyword index before uploading them to the cloud server. Encryption ensures that sensitive information remains confidential and cannot be accessed by unauthorized users or the cloud service provider.

When an authorized user wants to search for a specific file, the user generates a secure search token (trapdoor) using a keyword. This token is sent to the cloud server instead of the actual keyword to maintain query privacy. The cloud server then uses the encrypted index to match the token with the stored encrypted keywords and identifies the relevant files without decrypting the data.

After the search process, the cloud server returns the matched encrypted files to the user. The user can then decrypt the files locally using the secret key to access the original information. In this way, the system ensures that the cloud server never learns the actual content of the data or the search query.

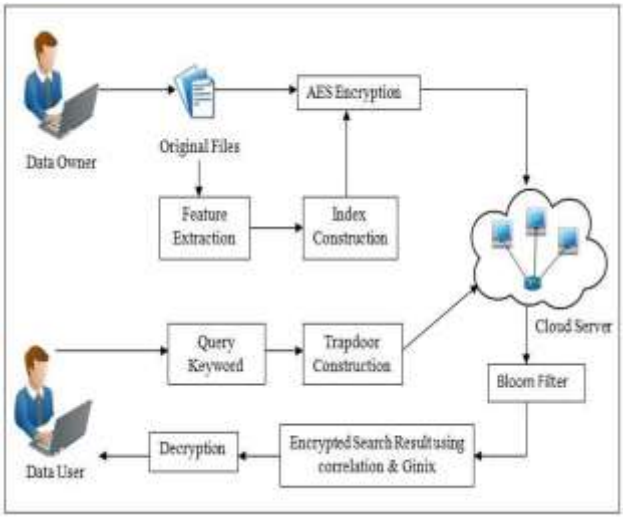

Fig. Architecture Diagram

IV. IMPLEMENTATION

The implementation of the proposed system Search over Encrypted Data using Advanced AES and Parallel Computing is designed to ensure secure storage and efficient keyword search on cloud data. In this system, the data owner first uploads files to the cloud after encrypting them using the Advanced Encryption Standard (AES) algorithm, which provides strong data confidentiality. During the encryption process, important keywords from the documents are extracted and an encrypted index is created to support secure searching. These encrypted files and indexes are then stored on the cloud server so that the server cannot access the original content of the data.

When a user wants to retrieve information, the user enters a keyword which is converted into a secure search token. The cloud server uses this token to match it with the encrypted index and identify relevant files without decrypting the actual data. To improve the speed and efficiency of encryption, decryption, and search operations, parallel computing techniques are used, allowing multiple operations to run simultaneously. After the matching process, the cloud server returns the corresponding encrypted files to the user, and the user decrypts them locally using the secret AES key. This implementation ensures data privacy, fast searching, reduced processing time, and secure cloud storage, making the system suitable for large-scale cloud applications.

V. ALGORITHM

a. The data owner registers and logs into the system and selects files to upload to the cloud.
b. The selected files are processed by extracting keywords and encrypting them using the AES algorithm with a secure key.
c. A keyword index is created from the extracted keywords and encrypted to prevent unauthorized access.
d. The encrypted files and encrypted index are uploaded and stored on the cloud server securely.
e. An authorized user logs into the system and enters a
keyword to search for a required file.
f. The entered keyword is converted into a secure search token (trapdoor) and sent to the cloud server.
g. The cloud server matches the token with the encrypted keyword index using parallel computing to perform fast searching.
h. The server identifies the matching encrypted files and sends them to the user.
i. The user decrypts the received files using the AES secret key and views the original data securely.

VI. HARDWARE & SOFTWARE ARCHITECTURE

The hardware requirements include a system with an Intel Core i5 processor, 8 GB DDR RAM, and 500 GB hard disk to ensure smooth processing and storage of data. For the software requirements, the system is developed using the Java programming language with the Java Development Kit (JDK) for compiling and running the program. The Swing framework is used to design the graphical user interface for user interaction, and the application is developed using the NetBeans Integrated Development Environment (IDE), which provides tools for coding, debugging, and testing the application efficiently.

VII. APPLICATION WITH REAL-LIFE EXAMPLE

a. Healthcare: Hospitals store patient records in encrypted cloud storage. Doctors can search patient files using keywords like patient name or disease while keeping medical data secure.
b. Banking: Banks store financial records and transaction data in encrypted form in the cloud. Employees can securely search customer details without exposing sensitive financial information.
c. Education: Universities store student records, results, and documents in the cloud. Authorized staff can search student information using keywords while maintaining data privacy.

VIII. FUTURE SCOPE

The system can be improved by implementing more advanced encryption techniques to provide stronger data security and privacy in cloud storage. The search process can be enhanced by supporting multi-keyword and semantic search, which will allow users to get more accurate results. The system can also be integrated with machine learning techniques to improve search efficiency and data management. Additionally, the model can be expanded to support large-scale cloud environments and mobile applications, making it more scalable and accessible. Further improvements may include faster processing using advanced parallel computing methods and better protection against emerging cyber security threats.

IX. RESULTS AND DISCUSSION

The proposed system successfully provides secure storage and keyword search over encrypted cloud data. Files are encrypted using the AES algorithm before uploading to the cloud, which protects sensitive information. Users can search data using secure keywords, and the cloud server returns the correct encrypted files without accessing the actual content. The use of parallel computing improves the speed of encryption and search operations. Overall, the system ensures data security, privacy, and efficient data retrieval.

X. CONCLUSION

A secure system for searching over encrypted cloud data was implemented using the AES encryption algorithm and parallel computing techniques. The system allows data owners to encrypt files before storing them in the cloud, ensuring that sensitive information remains protected. At the same time, authorized users can perform keyword searches without revealing the actual data or search queries to the cloud server.

The proposed approach improves data security, privacy, and search efficiency while reducing processing time. Overall, the system demonstrates that it is possible to achieve secure cloud storage along with efficient keyword search, making it suitable for real-

world applications such as healthcare, banking, and education where data confidentiality is very important.

REFERENCES

[1] *T. Peng, Y. Lin, X. Yao and W. Zhang, "An Efficient Ranked Multi-Keyword Search for Multiple Data Owners Over Encrypted Cloud Data," IEEE Access, vol. 6, pp. 11914–11933, 1018.*

[2] *X. Gao, J. Yu, Y. Chang, H. Wang and J. Fan, "Enabling Integrity Auditing Based on the Keyword With Sensitive*

[3] *Information Privacy for Encrypted Cloud Data," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp. 3774–3789, 1011.*

[4] *J. Tang, S. Fu and M. Xu, "An Effective Encrypted Scheme Over Outsourcing Data for Query on Cloud Platform," IEEE Access, vol. 7, pp. 66141–66150, 1019.*

[5] *X. Liu, T. Lu, X. He, X. Yang and S. Niu, "Verifiable Attribute-Based Keyword Search Over Encrypted Cloud Data Supporting Data Deduplication," IEEE Access, vol. 8, pp. 51061–51074, 1010.*

[6] *H. Dai, Y. Ji, G. Yang, H. Huang and X. Yi, "A PrivacyPreserving Multi-Keyword Ranked Search Over Encrypted Data in Hybrid Clouds," IEEE Access, vol. 8, pp. 4895–4907, 1010.*

[7] *X. Ge, J. Yu, C. Hu, H. Zhang and R. Hao, "Enabling Efficient Verifiable Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," IEEE Access, vol. 6, pp. 45715–45739, 1018.*

AUTHORS PROFILE

Ms. Shubhada Lohake, was born in Kotul, India in 2007 was currently pursuing her Diploma in Engineering in Jaihind Polytechnic, Kuran, Junnar, Pune, India. She attended many technical workshops and participated in many events conducted by different colleges. Her research interest includes Cloud Computing.

Ms. Anushka Gijare, was born in Junnar, India in 2008 was currently pursuing her Diploma in Engineering in Jaihind Polytechnic, Kuran, Junnar, Pune, India. She attended many technical workshops and participated in many events conducted by different colleges. Her research interest includes IOT.

Ms. Sharvari Mindhe, was born in Junnar, India in 2007 was currently pursuing her Diploma in Engineering in Jaihind Polytechnic, Kuran, Junnar, Pune, India. She attended many technical workshops and participated in many events conducted by different colleges. Her research interest includes Web Development.