Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Index Based Searchable Encryption on Cloud Data Using Asymmetric Encryption Algorithm

D.Manojkumar[1], P. Rajeswari[2], A. Jayalakshmi[3], R. Karthick[4]
Assistant Professor
[1,3,4] Department of Computer Science and Engineering
[2]Department of Information Technology,
Dr. Mahalingam College of Engineering and Technology, Pollachi.

Abstract: - Index-based searchable encryption (SE) techniques allow users to securely search over encrypted data without revealing sensitive information to the cloud server. However, existing SE schemes often suffer from efficiency and security trade-offs. We propose a novel approach for index-based searchable encryption on cloud data using an asymmetric encryption algorithm. With the increasing adoption of cloud storage services, ensuring the privacy and security of data stored in the cloud has become a serious concern. Proposes a novel approach for keyword search on encrypted data in cloud storage using an Elliptic Curve Cryptography (ECC) encryption approach. It utilizes index structures to enable efficient keyword search operations on the encrypted data. A secure index is generated during the encryption process, which allows for efficient retrieval of encrypted data related to specific keywords. Furthermore, our scheme introduces an indexing mechanism that preserves the confidentiality of the search queries while enabling efficient search operations. Only authorized users possess the necessary decryption keys to retrieve the plaintext information.

Keywords*: SE, ECC, encryption, cloud data.*

1. Introduction

Data sharing has become a crucial aspect of daily life for end users seeking access to various systems, services, and applications. In order to prevent data breaches, real-world cloud storage services are turning to block chain technology with cryptographic functions. Blockchain has garnered considerable interest in the realm of financial technology. It operates as an append-only list of cryptographically signed records or transactions, known as blocks that multiple parties aim to update. Each time a block is further to the chain, it becomes linked to the preceding block in a continuous sequence. Cloud computing has transformed the storage and accessibility of data, providing users and organizations with scalability, flexibility, and cost-effectiveness. However, the increasing use of cloud storage services has raised concerns regarding the security and privacy of sensitive information. While traditional encryption methods offer confidentiality, they often limit the ability to search encrypted data directly. Index-based searchable encryption (SE) techniques have been developed to tackle this issue, allowing users to search encrypted data without compromising its security.

Existing SE schemes typically rely on symmetric encryption algorithms, anywhere the same key is used for both encryption and decryption. While symmetric encryption provides efficient search capabilities, it often requires the cloud server to possess the decryption key, raising security concerns regarding data confidentiality. Additionally, symmetric encryption schemes may suffer from scalability issues when dealing with large-scale data storage systems. This paper introduces a Creative method for index-based searchable encryption of cloud data using an asymmetric encryption algorithm. Asymmetric encryption, also referred to as public-key cryptography, involves a pair of keys - public and private - for encryption and decryption, respectively. This innovative approach tackles the security issues linked with symmetric encryption by enabling users to conduct secure searches on encrypted data without disclosing sensitive information to the cloud server. Our proposed scheme leverages the benefits of

asymmetric encryption to achieve a balance between security and efficiency in searchable encryption. By separating the indexing process from the search process, our scheme ensures that sensitive data remains confidential even during search operations. Furthermore, we introduce an efficient indexing mechanism that preserves the privacy of search queries while enabling fast and accurate search operations on cloud data.

2. Literature Review

Data outsourcing is a generally used operation in moment's digital world. Searchable encryption (SE) plays a pivotal part icing data irretrievability while also maintaining data sequestration. In the trouble model of Searchable encryption schemes, the pall garcon is generally assumed to be Honest- But-Curious, although this supposition may not always be accurate in reality. Block chain- grounded Searchable encryption technology serves as a interference for vicious pall waiters, precluding them from sinning from the established protocol. Still, in this system, hunt results are validated by miners. Normal miners may conclude to skip the confirmation step and directly accept the block to save computational coffers, leading to the Verifier's Dilemma, which compromises the verifiability of block chain- grounded SE schemes. To attack this issue, our exploration introduces an empirical block chain- grounded public- crucial encryption scheme that delegates verification tasks to the True Bit network. This innovative approach enhances the verifiability of our scheme, reducing the computational burden on miners. likewise, our scheme establishes a fair payment protocol between multiple data possessors and users, enabling data possessors to drop access to participated documents as necessary. (1) We give security attestations and analysis of our proposed scheme, along with performance evaluations pressing the outflow associated with hunt operations on pall waiters and deals on Ethereum smart contracts. Our experimental findings demonstrate the practicality and effectiveness of our proposed solution. By recognizing the benefits of incorrect results generated by the cloud server, we offer significant advantages to data users. The search operation is conducted by miners within the block chain, ensuring both security and time-consuming process.

Searchable Symmetric Encryption (SSE) is a popular method of searching data in encrypted databases. Despite its efficacy and versatility, SSE is frequently exposed to information leaks. Recent assaults have highlighted the importance of forward privacy, which prevents data leakage during update processes, as a critical feature for any future SSE schemes. Even with forward privacy in place, search operations can still reveal significant amounts of information. To improve security measures, we expanded the concept of forward privacy to include forward search privacy. Essentially, this means that searches on freshly added documents should not reveal any information about previous queries. This increased security requirement offers new issues for SSE design. To address these difficulties, we developed the hidden pointer technique (HPT) and created a new SSE mechanism called Khons. [2] Khons not only meets our security requirements (including the original forward privacy notion), but it also displays efficiency. Our implementation of Khons, together with experiments on a large dataset (Wikipedia), demonstrates its better performance over previous SSE techniques with forward privacy features. Dual takes the longest to complete its search due to memory access, but Khons is the most cost-efficient. The potential applications for this solution may be restricted. With the increasing use of cloud storage in many applications, the issue of protecting data secrecy though allowing for effective data search and recovery in a dispersed context has emerged as a major research priority. Current searchable encryption techniques have both functionality and security have shown to be inadequate. The issues of providing multi-keyword search in a multi-user setting, concealing search and access patterns, and defending against keyword guessing attacks are extremely challenging.

In this paper, we present a novel searchable encryption method that solves all three problems simultaneously, which makes it perfect for application in distributed systems. This method protects the security of the data and search patterns in addition to enabling multi-keyword searches on encrypted material in a multi-writer/multi-leader scenario. We employ a multi-server architecture to mitigate KGA, which increases search response times, distributes the effort, and lowers the risk of key leakage by enabling only authorised servers to jointly determine whether a search token corresponds to a stored cypher text. Moreover, the fundamental idea behind our scheme is a novel subset choosing procedure, which has many uses beyond keyword search. We performed security proofs and assessed the computational and communication efficiency of our approach to show that it is feasible. [3] We effectively lower the risk of key leakage, enhancing protection against unauthorised access and preserving the confidentiality of sensitive data by limiting access to authorised servers for token matching with stored cypher

text. It is critical to understand that when the number of keywords rises, the effectiveness of our scheme may decrease.

SSE schemes are intended to offer clients with a secure way to store their data on untrusted servers while still allowing them to conduct keyword searches. Recent tests have demonstrated that the efficacy of these methods is dependent on striking the correct balance between space overhead, location, and read efficiency. Researchers such as Cash and Tessaro (EUROCRYPT 14) and Asharov et al. (STOC 16) have created SSE methods with varying trade-offs and determined lower bounds for common frameworks. However, the ideal trade-off has yet to be identified, and there are significant discrepancies between existing systems and lower bounds. [4] This emphasizes the necessity of additional study to comprehend SSE technology on a deeper level. The capacity of SSE technology to increase reading efficiency by promptly and precisely retrieving IDs is a significant feature. Nevertheless, either a large gain in storing capacity or a deficiency in effective reading abilities frequently impedes this.

Users can search encrypted documents in untrusted cloud environments using a new technology called Searchable Symmetric Encryption (SSE) without giving the cloud providers access to the search keywords. Although current SSE methods accomplish very high search efficiency, they often create security flaws by unintentionally disclosing search patterns and access. A significant risk to user privacy is presented by this leak, which renders a significant portion of the query phrases recoverable by clouds. To solve this issue, researchers have developed several techniques to preserve search or access patterns. Nevertheless, none of these techniques offers total security from all kinds of access and searches. Moreover, a number of customers that want encrypted document access in a generic database configuration encounter difficulty with the proper operation of existing SSE systems. We provide a novel SSE scheme, SAPSSE, to address these issues. This plan is especially made to protect hunt patterns in a generic database environment as well as access. Using exercise-encryption cryptosystems to equivocate indicator entries over several shadows is the abecedarian notion underlying guarding search patterns. We deploy secure indicators to various shadows and implement an indicator revision protocol that enables users to update indicator entries in the shadows, ensuring the security of access patterns. Similarly, SAP-SSE gives users the ability to customise security policies, allowing them to find a balance between security and efficacy. We show that SAP-SSE successfully eliminates pattern leakage with minimal outflow through formal security analysis and experimental evaluation. Users can strike a balance between security and efficacy with the help of our platform's customised security policy. The improved security measures greatly outweigh this small inconvenience, even though the proposed scheme's hunt time shows a modest rise.

3. Proposed System

Figure 1: The proposed data flow for outsourcing data to third-party cloud providers raises significant concerns regarding data privacy and security. To address these concerns, it is essential to implement advanced encryption techniques, such as Index-Based Searchable Encryption (IBSE), to ensure secure data retrieval. IBSE allows users to store their data in an encrypted form on the cloud and conduct keyword-based searches on the outsourced data.

Elliptic Curve Cryptography (ECC) technology has emerged as a promising approach for encrypting data and keywords before storing them on the server. ECC encryption guarantees that the outsourced data remains confidential and secure. IBSE facilitates efficient keyword-based searches on the encrypted data stored in the cloud, providing fine-grained access control over the outsourced data. This search method enables users to search for specific information without having to decrypt the entire dataset, enhancing both security and usability. In this system we focused on only authorized users possess the necessary decryption keys to retrieve the plaintext information and high security of information system. The index construction approach complements ECC encryption by allowing for efficient search operations on the encrypted data

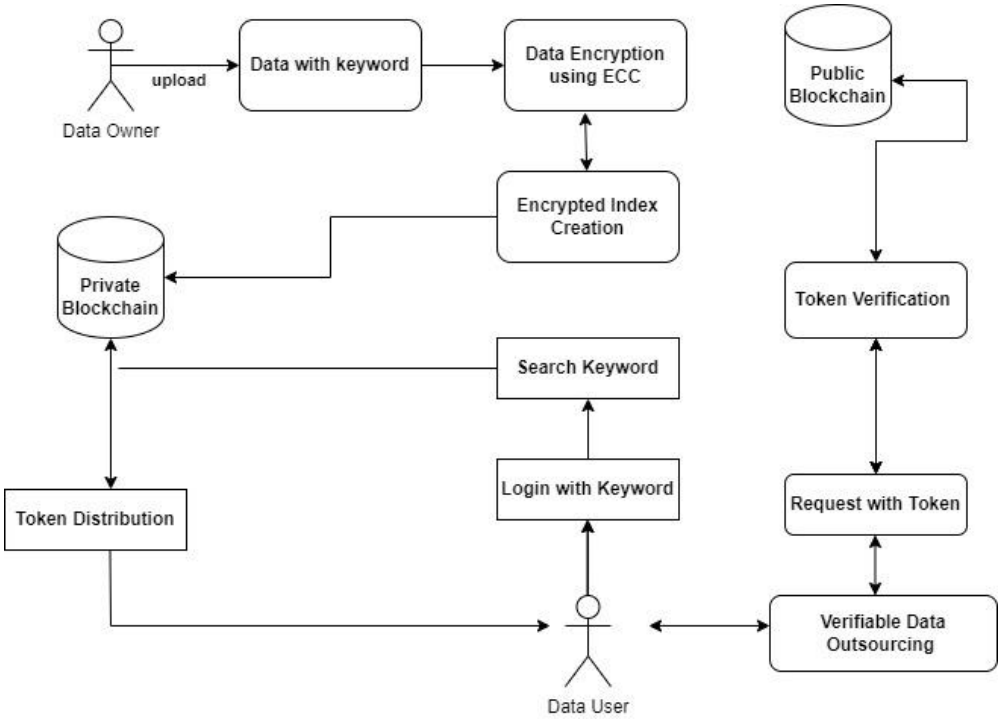

Figure A1. System Architecture of Proposed System

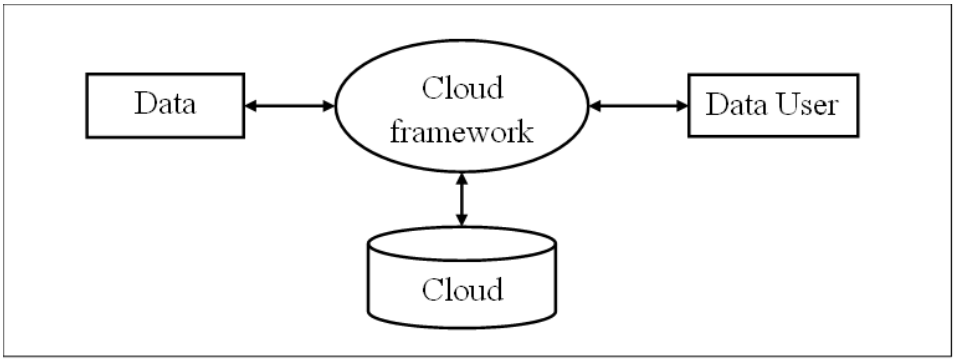

Figure A2: Dataflow Diagram of Level 0

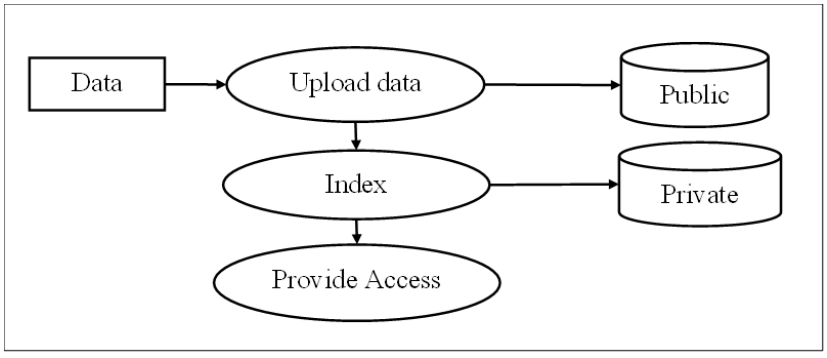

Figure A3: Dataflow Diagram of Level 1

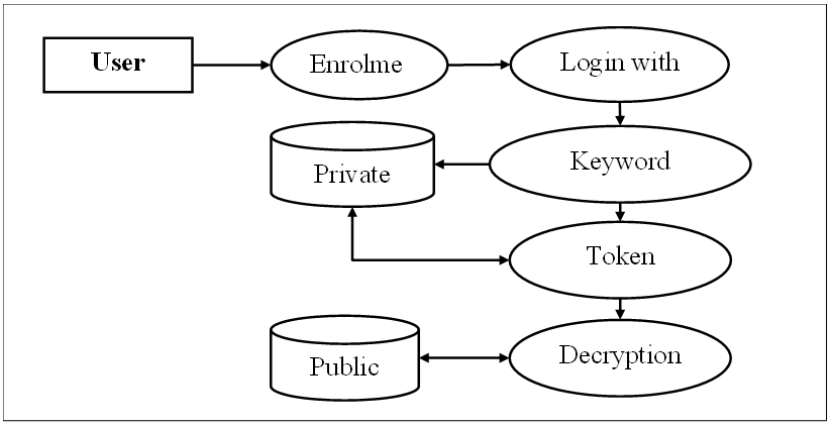

Figure A4: Dataflow Diagram of Level 2

3.1 Data Storage Framework

Cloud computing is the realization of the long-held vision of computing as a utility, allowing customers to store their data remotely in the cloud. This module consists of three types of users: the cloud owner, cloud server, and regular users. The module assists the owner in registering their details and creating login credentials for authorized access to the system, adding an extra layer of security to user data. The login credentials are encrypted for security purposes and decrypted by the server to prevent eavesdropping. The server has the capability to store files in cloud storage, while users can easily search for files using keywords.

3.2 Data Encryption

Here implementing Elliptic Curve Cryptography (ECC) encryption to secure data stored in the cloud. ECC, known for its efficient use of resources and strong security properties, is used to encrypt data before it is uploaded to the cloud. This guarantees that even if unauthorized access occurs, the data remains indecipherable. With ECC encryption and the index-based system in place, data owners can trust that their information is safeguarded and accessible only to authorized parties.

3.3 Index Creation

To enhance data security and privacy, it is essential to design and implement a robust data structure for storing encrypted keywords and their corresponding index details. This structure can take the form of a database table, a key-value store, or any other suitable data storage mechanism. When handling encrypted keywords and generating an index, it is crucial to prioritize security measures to safeguard sensitive information.

3.4 Data Access Request

The process of searching for and accessing data involves securely retrieving encrypted information. To begin a search, the user must create a query specifying the desired data. This query is then encrypted using a suitable algorithm and transmitted as a data access request through a secure channel. The system receiving the request verifies the user's authentication and securely handles the request while maintaining the encryption of the search query. The encrypted search query is then matched with the encrypted keywords in the index to retrieve the relevant index details.

3.5 Token Distribution

When granting access permissions to the query user for retrieving encrypted data, a token distribution system is employed. The system generates unique tokens that act as access credentials for authorized users. These tokens are securely distributed to users who have been granted access to specific data or resources. The token serves as proof of authorization and allows the query user to retrieve the encrypted data. By using token distribution, access permissions can be controlled and monitored effectively.

3.6 Verifiable Data Access

In order to ensure a secure and verifiable data access process, a system can implement token verification and data access using a shared decryption key. This system works by verifying the authenticity and validity of the token to confirm that it has not been altered and is issued by a trusted authority. Once the token is successfully verified, the system securely shares a decryption key with the user. This shared decryption key enables the user to decrypt the requested data while maintaining its confidentiality.

4. Result and Experiments

For simulation, we use the system windows 10 OS with Intel i5 CPU and 4G RAM and 15 GB hard disk. Data-science programs appropriate for Windows, Linux, and macros are included in the bundle. Anaconda, Inc. created and maintains it.

- The proposed solution uses an ECC-based encryption technique to improve data sharing security.
- The parameters used to estimate the speed of the proposed system when interacting with cloud users include the time taken for encryption and decryption processes.
- The shorter time demonstrates the user and cloud server's high-speed communication.
- Here, the system calculates the time required for encryption and decryption using the recommended ECC algorithm compared to the current AES technique

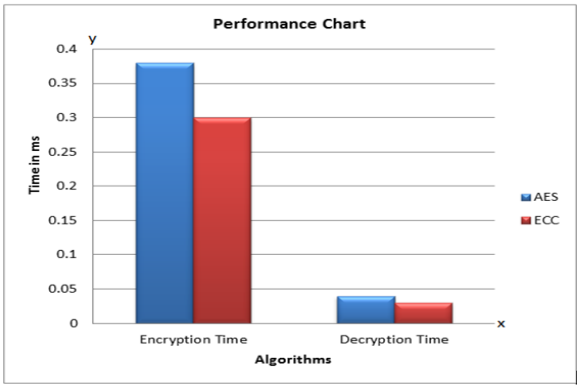

Figure 5 Performance Graph

5. Conclusion and Future Work

Searchable encryption offers a powerful solution for preserving the privacy and confidentiality of sensitive data while enabling efficient search operations. ECC provides a high level of security with smaller key size. The index construction approach complements ECC encryption by allowing for efficient search operations on the encrypted data. It offers a balance between data confidentiality and search functionality, and achieves both privacy and efficient data retrieval. In future extend the keyword search method that supports multiple keywords with keyword ranking based search results retrieval process.

References

[1] Li, Haiyu, Tao Wang, Zirui Qiao, Bo Yang, Yueyang Gong, Jingyi Wang, and Guoyong Qiu. "Blockchain-based searchable encryption with efficient result verification and fair payment." Journal of Information Security and Applications 58 (2021): 102791.

[2] Li, Jin, Yanyu Huang, Yu Wei, Siyi Lv, Zheli Liu, Changyu Dong, and Wenjing Lou. "Searchable symmetric encryption with forward search privacy." IEEE Transactions on Dependable and Secure Computing 18, no. 1 (2019): 460-474.

[3] Liu, Xueqiao, Guomin Yang, Willy Susilo, Joseph Tonien, Ximeng Liu, and Jian Shen. "Privacy-preserving multi-keyword searchable encryption for distributed systems." IEEE Transactions on Parallel and Distributed Systems 32, no. 3 (2020): 561-574.

[4] Asharov, Gilad, Gil Segev, and Ido Shahaf. "Tight tradeoffs in searchable symmetric encryption." Journal of Cryptology 34 (2021): 1-37.

[5] Song, Qiyang, Zhuotao Liu, Jiahao Cao, Kun Sun, Qi Li, and Cong Wang. "SAP-SSE: Protecting search patterns and access patterns in searchable symmetric encryption." IEEE Transactions on Information Forensics and Security 16 (2020): 1795-1809.
[6] Zhong, Hong, Zhanfei Li, Jie Cui, Yue Sun, and Lu Liu. "Efficient dynamic multi-keyword fuzzy search over encrypted cloud data." Journal of Network and Computer Applications 149 (2020): 102469.
[7] Miao, Yinbin, Robert H. Deng, Kim-Kwang Raymond Choo, Ximeng Liu, and Hongwei Li. "Threshold multi-keyword search for cloud-based group data sharing." IEEE Transactions on Cloud Computing 10, no. 3 (2020): 2146-2162.
[8] Dai, Xuelong, Hua Dai, Chunming Rong, Geng Yang, Fu Xiao, and Bin Xiao. "Enhanced semantic-aware multi-keyword ranked search scheme over encrypted cloud data." IEEE Transactions on Cloud Computing 10, no. 4 (2020): 2595-2612.
[9] Wang, Haoyang, Kai Fan, Hui Li, and Yintang Yang. "A dynamic and verifiable multi-keyword ranked search scheme in the P2P networking environment." Peer-to-Peer Networking and Applications 13 (2020): 2342-2355.
[10] Tariq, Husna, and Parul Agarwal. "Secure keyword search using dual encryption in cloud computing." International Journal of Information Technology 12 (2020): 1063-1072
[11] Liang, Yanrong, Yanping Li, Qiang Cao, and Fang Ren. "VPAMS: Verifiable and practical attribute-based multi-keyword search over encrypted cloud data." Journal of Systems Architecture 108 (2020): 101741.
[12] Zhang, Dong, Qing Fan, Hongyi Qiao, and Min Luo. "A public-key encryption with multi-keyword search scheme for cloud-based smart grids." In 2021 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1-6. IEEE, 2021.
[13] Liu, Xueyan, Tingting Lu, Xiaomei He, Xiaotao Yang, and Shufen Niu. "Verifiable attribute-based keyword search over encrypted cloud data supporting data deduplication." IEEE Access 8 (2020): 52062-52074.
[14] Cui, Yuanbo, Fei Gao, Yijie Shi, Wei Yin, Emmanouil Panaousis, and Kaitai Liang. "An efficient attribute-based multi-keyword search scheme in encrypted keyword generation." IEEE Access 8 (2020): 99024-99036.
[15] He, Kun, Jing Chen, Qinxi Zhou, Ruiying Du, and Yang Xiang. "Secure dynamic searchable symmetric encryption with constant client storage cost." IEEE Transactions on Information Forensics and Security 16 (2020): 1538-1549.
[16] Ramprasath, J., Ramakrishnan, S., Tharani, V., Sushmitha, R., Arunima, D. (2023). Cloud Service Anomaly Traffic Detection Using Random Forest. In: Tiwari, S., Trivedi, M.C., Kolhe, M.L., Singh, B.K. (eds) Advances in Data and Information Sciences. Lecture Notes in Networks and Systems, vol 522. Springer, Singapore.
[17] M Balakrishnan, AB Christopher, AS Murugavel, J Ramprasath, “Prediction of Data Analysis Using Machine Learning Techniques”, Int. J. of Aquatic Science, Volume 12, Issue 3, pp. 2755-2762, 2021.