IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

INDEX BASED SEARCHABLE ENCRYPTION ON CLOUD DATA USING ASYMMETRIC ENCRYPTION ALGORITHM

S.VARSNI[1*], S.UMA[1], P.JAGADEESH[2]

[1] Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India

[2] Department of Mechanical Engineering, K.S.R. College of Engineering, Tiruchengode, India

Abstract: Retaining the privacy, integrity and security of records stored inside the cloud server has end up increasingly more important as cloud storage services are used extra often. Using encryption techniques to encrypt data before uploading it to the cloud is one way to solve this problem. However, because the data must first be decrypted, typical encryption techniques make it more difficult to search for and retrieve certain information from the encrypted data. The effectiveness and utility of cloud storage solutions are hampered by this restriction. To overcome this challenge, this research propose a novel approach for keyword based search on encrypted data in cloud storage using an Elliptic Curve Cryptography (ECC) encryption approach. By leveraging the ECC encryption approach, the proposed solution ensures the confidentiality of data stored in the cloud while enabling efficient keyword-based search operations without the need for decryption. This approach utilizes a combination of cryptographic techniques such as ECC encryption and index structures to enable efficient keyword search operations on the encrypted data. Develop a secure search system that supports multi-keyword ranking searches over encrypted cloud data as well. A secure index is generated during the encryption process, which allows for efficient retrieval of encrypted data related to specific keywords. Based on the search keyword ranking method, the index of the keyword was dynamically updated. The encrypted data remains confidential, as only authorized users possess the necessary decryption keys to retrieve the plaintext information. The results demonstrate that the keyword search on encrypted data in cloud storage using the ECC encryption approach achieves a balance between data privacy and search functionality. Also implement blockchain technology for enhancing the database security. The solution offers an effective means to securely store and retrieve data from the cloud while ensuring that sensitive information remains protected from unauthorized access.

Keywords - Cloud Data Storage, Data Encryption, Multi Keyword Creation, Index Generation, Keyword Ranking, Index Update, Verifiable Data Sharing.

I. INTRODUCTION

With the arrival of cloud computing, information proprietors are pushed to outsource their complex facts management structures from neighborhood sites to the commercial public cloud, providing substantial flexibility and fee financial savings. This is accomplished through the searchable encryption approach. However, with a purpose to protect records privacy, touchy records should be encrypted before being outsourced, rendering plaintext keyword search obsolete for maximum data consumption. Therefore, it is crucial to enable an encrypted cloud data search service. Because there are loads of facts customers and files inside the cloud, it's far vital to permit a multiple keywords in the search request and return documents within the order that they're applicable to those phrases. Similar efforts on searchable encryption tend to concentrate on keyword or Boolean searches rather than sorting the keyword search results. For the first time, the tough privateness-maintaining multi-keyword ranked seek over encrypted cloud information (MRSE) hassle is defined and solved within the present research. Here, build a set of stringent privacy specifications for a system that uses cloud data in a secure manner [1]. To capture the relevance of facts files to the quest question, pick the effective similarity degree of "coordinate matching" (i.e., as many matches as feasible) from many of the many index-primarily based keyword semantics. To evaluate this similarity metric scientifically, use "inner product similarity" as an additional tool. A comprehensive analysis of the effectiveness and privacy assurances of the recommended systems is offered. Tests conducted on the real-world dataset additionally show that there is very minimal computational and transmission cost associated with the suggested strategies.

As one data owner is taken into account in the system models of the available studies, it follows that in their solutions, the data owner and data users can easily converse and exchange sensitive information. Secret information exchange will result in a significant increase in communication overhead when multiple data owners are involved in the system. Examine the problems of comfortable multi-keyword look for multiple facts owners and a couple of statistics clients inside the context of cloud computing. In this study, talk about safe keyword searching over secured cloud data [2].

Unauthorized individuals may access the files if they weren't encrypted. Here encrypt the data and conceal it to prevent unauthorized access. Information is changed through the process of encryption such that no one else can read it except for those who have the key that enables them to transform the information back to its original, readable form. When a person searches and lists using just one term, without all of its permutations, this is known as a single-keyword search [3]. A user conducts a multi-keyword search when they look for several versions of the same keyword. Here, choose the efficient coordinate matching principle from a range of multi-keyword semantics to seize the similarity between the search keyword and the stored documents.

Blockchain Technology

Blockchain is a distributed, trustworthy, public ledger of transactions that anybody may access but that no one user has complete control over. It is a distributed database that tracks an expanding set of encrypted transaction data records to guard against manipulation and alteration. Three distinct types of blockchain exist: consortium, private, and public blockchains [4]. Anyone from anyone can join and be released at any time on public blockchains like Ethereum and Bitcoin. The sophisticated mathematical operations serve as proof for this. The company's internal public ledger is called the private blockchain, and consumers can only join it with permission from the blockchain's owner. Due to the smaller number of nodes, the private blockchain's block creation and mining speeds are far faster than those of the public blockchain.

However, there is a consortium blockchain that is used by businesses or groups of businesses, and it uses membership criteria as opposed to consensus to more effectively regulate blockchain transactions. Since the blockchain in this study is to be regulated by a national body in the nation, consortium blockchain is being used. The block is the fundamental unit of the blockchain [5]. Fig 1 shows blockchain creation process. The transactions that are being written to the system are contained in the body of each block, which also has a header. The block header contains details about the block, such as the preceding hash, nonce value, difficulty, and time stamps of the block and the transactions. It is estimated that the block's length varied from 1 to 8 MB. Only its header serves as an indicator of the block that has to be inserted.

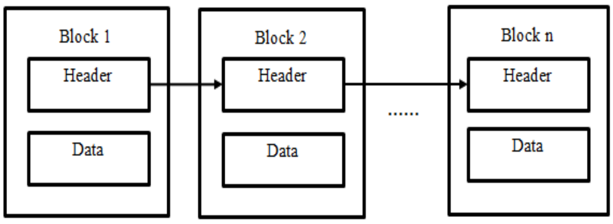

Fig 1: Blockchain Creation

II. RELATED WORK

Li, Haiyu, et.al., [6] developed a public-key encryption system based on verifiable blockchain technology, with the verification process being outsourced to the True Bit network. This design allows the suggested technique to achieve strong verifiability while lowering the miners' computational costs. Additionally, the suggested plan creates a fair charging methodology for many record owners and information consumers. Additionally, the owner of the facts may withdraw consent for any report they previously shared. A public-key encryption technique utilizing key-word seeks and principally based on blockchain is suggested as a means to accomplish honest and decentralized searchable encryption. Here, the existing plan was enhanced to achieve publicly verifiable, and the crucial thing-combination strategy was applied to lower the cost of vital protection. The proposed method uses a clever contract to create fair financing and gain access to manage information between information owners and users. They will be paid by the information user automatically as long as the data owner grants access to the records person and the cloud server displays the search results accurately. The suggested plan combines smart settlement with satisfactory-grained bills in a multi-owner context. In particular, the individual in charge of records can pay the actual search fee based entirely on the portion of results that are verified again through the cloud server, with the remaining amount being returned to their account. Additionally, fact owners receive a good wage based on the quantity of documents they produce.

Li, Jin, et.al., [7] suggested an ultra-modern SSE scheme known as Khons, which satisfies proposed safety perception (with the particular beforehand privacy belief) and is also green. Here provide an reason for the security problem of cutting-edge in advance privateness and recommend an stronger notion beforehand are seeking privateness, which guarantees that searches over newly brought files do now .not leak the past query information. Point out that forward search private SSE will leak lots much less statistics than SSE which handiest satisfies the unique FP notion. Also describe its applications in constructing comfortable encrypted programs and improving efficiency in the format of encrypted databases. To reap this protection intention, advanced the contemporary forward non-public method, hidden pointer approach (HPT). Finally, construct the Khons scheme reaching each forward search privateness and backward privacy. Experiment consequences show that Khons is efficient and realistic.

Liu, Xueqiao, et.al., [8] have presented a brand-new searchable encryption system that solves all of the aforementioned problems at once, making it practical for distributed structures to use. Not only does it facilitate multi-keyword searches over encrypted data under a multi-writer/multi-reader setup, but it also guarantees the privacy of search patterns and statistics. The suggested method uses a multi-server architecture to prevent KGA. This reduces the chance of key leakage; speeds up seek reaction, and spread the workload by enabling the best legal servers to simultaneously verify if a search token matches a stored ciphertext. The fundamental idea behind the suggested technique is also a unique subset determination mechanism, which may be used to various uses besides keyword search. In addition to providing matching keys to CPs and ISs, the Key Generation Centre is responsible for creating public parameters, system keys, and CP and IS keys. An organization's administrator, for example, could assume the role of KGC. Documents and their related searchable ciphertexts uploaded through DPs are stored by the Cloud Platform. With the help of ISs, it manages seek requests and produces the (encrypted) search result for RUs. It retrieves the file indexes by decrypting the quest results that were returned back from CP using the search query.

Asharov, et.al., [9] have presented strict limits at the trade-off between the general frameworks' gap overhead, locality, and read efficiency of SSE methods. While such frameworks reflect the memory access pattern that underlies all existing techniques, there is no guarantee that lower bounds cannot be evaded by employing alternative procedures. Therefore, the main unresolved issue resulting from the suggested study is to demonstrate tight boundaries for any SSE technique. Proving such tight limitations for dynamic SSE schemes and investigating the aforementioned change-off for searchable encryption inside the public-key putting are two more naturally occurring unresolved topics. Any SSE scheme's search procedure may be broken down into a series of consecutive reads from the encrypted database EDB; the number of these reads is referred to as the locality. Locality is specifically defined by considering the Search set of rules of an SSE scheme as a collection of rules that only obtains oracle get right of entry to the encrypted database, not actually entering it. The c programming language [ai, bi] that makes up each query to this oracle is answered by the oracle using gadget phrases that are stored in this c programming language of EDB. The range of sub-lists and the range of padded items Every listing is divided into sections that work best during each listing; each hash desk is made up of encrypted elements with pseudorandom labels; and each hash table's size is best determined by the size of the database.

Song, Qiyang, et.al., [10] established the effective SAPSSE searchable symmetric encryption scheme, which safeguards all access patterns and search methods inside the designated database location. Protective search patterns employ re-encryption cryptosystems to shuffle index entries over various clouds, which is a key concept. Here, relaxed indexes are distributed to several clouds in order to protect access to styles. An index redistribution protocol is then recommended, enabling users to update index entries inside clouds. This suggested device enables several people to search through and update encrypted files. Three events comprise SAP-SSE: The system consists of three main components: (i) a group of authorized users who can search and replace encrypted files; (ii) a person control centre that manages user control; and (iii) a fixed cloud that stores encrypted files and also offers search and update functions to ensure sample safety. To keep things simple, the system is presented using just two clouds, S1 and S2, although the suggested machine can be expanded to include more clouds. The creation of secure indices that can be moved and shuffled between S1 and S2 is the fundamental understanding of defensive access and search patterns. Consequently, the associated seek tokens may be modified, making it impossible for clouds to deduce search strategies.

Belchior, et.al., [11] have presented a literature overview on blockchain interoperability by means of gathering 284 papers and a 120 grey literature files, constituting a corpus of 404 documents. Three classes are used in this overview to group studies: Hybrid Connectors, Blockchain of Blockchains, and Public Connectors. Based on predetermined criteria, each category is further subdivided. Here, use the Blockchain Interoperability Framework to classify 67 existing solutions into a single subcategory, giving a comprehensive overview of blockchain interoperability. Describe the field of blockchain interoperability research, providing the relevant history and emphasising definitions that are appropriate for both academic and industry settings. Explain what blockchain interoperability is and go over the various standards and architectures for it. Introduce the Blockchain Interoperability Framework (BIF), a framework that outlines standards for evaluating solutions for blockchain interoperability. Specifically, proposed analysis draws from multiple sources (e.g., whitepapers, blog posts, technical reports, peer-reviewed publications) to provide a comprehensive picture of each solution's range in the intervening time and its roadmap—that is, the goals and intentions of its creators. In order to accomplish this, here methodically got in touch with the writers of industrial solutions and grey literature articles. This is proposed creative endeavour providing reader access to top notch material in this quick growing area of observe. With the help of this technique, user may get current, trustworthy information that is frequently difficult to obtain.

Wang, et.al., [12] suggested a unique blockchain-based framework for tracking facts utilization and consider-unfastened personal statistics computation. The distributed ledgers maintain an immutable and obvious report of information utilization, at the same time as clever contracts are used to specify great-grained information usage policies (i.e., who can get admission to what sorts of facts, for what functions, and at what price). The off-chain smart contract execution technique that relies on a trusted execution environment (TEE) is also utilised to handle private user datasets and reduce computational cost in blockchain systems. To guarantee the atomicity of records transactions in computing result release and payment, a -phase atomic transport protocol is created. The proposed framework, which is based on DPaaS mode, can be a supplement to the existing data sharing ecosystem, where authorised service providers only receive the processed data outputs rather than raw data. Here also develop off-chain private data storage and computing technique to address the concerns of secrecy and poor smart contract execution. Under this technique, real user data is encrypted and stored in the cloud, and sensitive user data is computed in smart contracts utilising a trusted execution environment (TEE), such Intel SGX. Furthermore, contract theory asserts that in an information-asymmetric environment, the optimal contract items—data utility and price—are developed to maximise utility business profit while promoting user engagement and high-quality data sharing.

III. Background of the Work

The goal of Searchable Encryption (SE) is to retrieve data that can't be decrypted using conventional encryption techniques. Usually, SE techniques work by building an encrypted index. The encrypted data and the index are sent to the service provider by the DO. For a given keyword, the Data User (DU) provides the search token; the service provider then utilizes search algorithms to discover matches using the encrypted index and token. Earlier methods returned findings by scanning, and their efficiency decreased linearly with the size of the database. By building an index and extracting keywords so that the query complexity is only connected to the keywords in the file set, numerous academics have improved SE technology to meet the efficiency issue. However, most of the early schemes are static and cannot be changed dynamically. Users that save data on a cloud server often need to update it. In order to achieve these goals, dynamic SE technology has emerged, increasing the flexibility and accessibility of the SE scheme. Because the attacker can observe the data updating process and determine the links between keywords and files in order to steal or alter the data, the security analysis becomes more challenging. Security designs against a malicious server have not received enough attention, and the majority of current solutions primarily concentrate on an honest yet inquisitive cloud server. When there is an external assault or an issue with internal setup, the cloud server becomes malicious and can lead to altered or leaked encrypted data, wrong query results, and more.

IV. Encrypted Multi Keyword Search with Ranking based Index Construction

The rapid growth of cloud storage services has provided users with convenient and scalable data storage solutions. However, the outsourcing of data to third-party cloud providers raises significant concerns regarding data privacy and security.

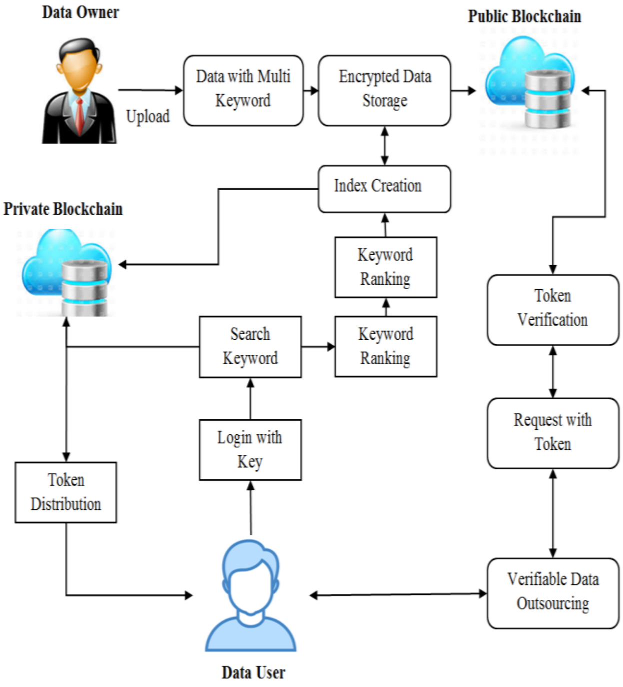

Fig 2: Proposed Framework

To address these concerns, researchers have developed advanced encryption techniques, such as Index-Based Searchable Encryption (IBSE), to enable secure data retrieval and search functionalities while preserving data confidentiality. Fig 2 explains the working process proposed data sharing approach. IBSE combines the benefits of searchable encryption and indexing techniques to enable efficient searching over encrypted data stored in cloud server. It enables users to keep their data encrypted on the cloud while still being able to perform keyword-based searches on the outsourced data. With the cloud service being more and more popular in modern society, ECC technology has become a promising orientation. Users can access files stored in encrypted form on a cloud server by using customizable access controls. Given a cipher text and a transformation key, CSP transforms a cipher text into a simple cipher text. To retrieve the plaintext from simple cypher text, the user just needs to incur a minimal computational overhead. By using this approach, users can securely store their data in the cloud while maintaining the ability to search for specific information without compromising data confidentiality. Provide a novel concept as well for doing multi-keyword ranked search. The dynamic modification of the keyword index was contingent upon the ranking of the keyword. The cloud server shouldn't infer any keyword information about the file set from secure indexes and trapdoors other than the search result. Indexes and appropriately represented, securely encrypted queries are necessary for maintaining keyword privacy. The proposed scheme aims to strike a balance between security and efficiency, ensuring that the data retrieval process is both fast and reliable.

Data Storage Framework

With the capacity to remotely store data in the cloud and access top-notch on-demand programmes and services from a pool of programmable computer resources, cloud computing symbolizes the long-awaited deployment of computing as a utility. People and companies are being pushed to outsource their local sophisticated data management system to the cloud because of its amazing flexibility and economic benefits. Here, examine the issue of keyword search over encrypted cloud data for the first time and lay forth stringent privacy requirements for this kind of safe cloud data usage system. Three different user categories are included in this module: users, cloud servers, and cloud owners. The owner can register their details and provide login information with the help of this module. Then legitimate user with system access to strengthen user data security. To prevent prying eyes, the login credentials are encrypted and subsequently decoded by the server. The files can be kept on a cloud storage server. Also, users can use keywords to search files. In addition to using blockchain technology for multi-keyword storage and data security, this suggested framework.

Data Encryption

This module facilitates the owner's upload of a file encrypted with the ECC algorithm. By doing this, the safe of the outsourced data could be guaranteed from unwanted access. The data owner logs into the system to upload data that has been crawled from the internet. The data is kept in a structured format for easy access. Since the data will be substantial, it needs to be saved in the right format. Public key cryptography includes Elliptic Curve Cryptography (ECC). In public key cryptography, every user provided a private key and a public key, together with a hard and fast of operations related to the keys to perform the cryptographic operations. However, the public key is shared with all users involved in the conversation, but the private key is known only to that particular user. Certain public key techniques require that a set of predefined constants be known by every device involved in the communication.

Index Creation

Design and implement a data structure to store the encrypted keywords and their corresponding index details. This structure could be a database table, a key-value store, or any other suitable data storage mechanism. When working with encrypted keywords and creating an index, special considerations need to be taken into account to guarantee the data's security and privacy.

Ranking based Index Creation

Cloud data storage is the need to continually update the index based on highly searched keywords. Cloud providers should prioritize indexing popular documents and data, making them readily accessible through search functionalities. This dynamic indexing process ensures that users can quickly find the most relevant information within their cloud storage, ultimately enhancing their experience.

An index is made up of a list of mappings for every term. The following details are included in the list for a certain keyword:

1. Each file has a unique id which based on the keyword
2. Calculate term frequency for keyword, which indicates the number of times a keyword presented in search process.
3. Each file's length
4. Each file's relevance score
5. The quantity of files containing the specific keyword. This data can be kept in data structures like tables.

The number search count of the keyword, the length of the file, and term frequency are utilized to determine the relevance score of search keywords using scoring procedures that will be covered in more detail in the Ranking modules. Each time a data file is saved, it undergoes preprocessing using the keywords that were extracted from the file (using a multiple string matching technique) to produce an index using the previously described data.

Data Access Request

The search and data access request process involves securely searching for and retrieving encrypted data. To initiate a search, the user formulates a query describing the desired data. The query is encrypted using an appropriate algorithm and sent as a data access request over a secure channel. The receiving system verifies the user's authentication and securely processes the request while keeping the search query encrypted. The system performs an index lookup using the encrypted query, identifying the relevant encrypted data entries. Match the encrypted search query with the encrypted keywords in the index to retrieve the corresponding index details. The system then retrieves the encrypted data or record identifiers that match the query.

Token Distribution

To provide access permissions to the query user for retrieving encrypted data, a token distribution system can be implemented. 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. To request access to encrypted data, the query user presents their token along with the data access request. The system verifies the authenticity and validity of the token to ensure that the user has the necessary permissions. 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. This approach enhances the security and privacy of encrypted data, ensuring that only authorized users with valid tokens can retrieve and decrypt the data they are permitted to access.

Verifiable Data Access

To facilitate a verifiable data accessing process, token verification and data access using a shared decryption key can be implemented. A verifiable data accessing process can be established through token verification and data access using a shared decryption key. Users requesting access for encrypted data using their access token. The system verifies the authenticity and validity of the token to ensure that it has not been tampered with and is issued by a trusted authority. The system securely provides the user with a decryption key after the token has been successfully validated. This shared decryption key allows the user to decrypt the requested data while ensuring its confidentiality. By implementing token verification and data access using a shared decryption key, the system ensures that only authorized users with valid tokens can access and decrypt the data.

Elliptical Curve Cryptography

Elliptical curve cryptography (ECC) is called as a public key based encryption approach that leverages elliptic curve principle to offer cryptographic keys which can be extra efficient, faster, and smaller. Rather of producing keys the usage of the fabricated from extraordinarily massive top numbers as is the standard method, ECC makes use of the properties of the elliptic curve equation to attain keys. The majority of public key based encryption methods, consisting of RSA and Diffie-Hellman, are well matched with the gadget. Some researchers claim that ECC can provide a degree of security that other systems only manage with 1,024-bit keys. ECC algorithm is widely employed in mobile based applications for the reason of equal security with less computational and battery resource demand. An algebraic structure known as an elliptic curve is used in cryptography. ECC includes key agreement techniques, encryption, and digital signatures. Sharing a secret key is made possible by the key distribution algorithm, private messaging is made possible by the encryption algorithm, and message integrity is confirmed by the digital signature algorithm:

Implementation Procedure

- Each participants share their public key to transfer data.
- Formulate the equation of Elliptic Curve
- Get values for the variables a and b
- Select Prime from elliptic curve, denoted p
- The elliptic based key pairs computed using the parameters generated from elliptic curve equation
- An elliptic group base point called B
- Comparable to the generator employed by modern cryptosystems
- Every user generates their own set of public and private keys.

○ Private Key = denoted as integer ‘x’, that selected from the range between [1, p-1]

○ Public Key = product of private key and defined base point, denoted as Q,

(Q = x*B)

Encryption

1. Describe an elliptic curve.
2. Using that elliptic curve points, generate a public key and private key pair for both participants.
3. From the key pair, create a shared secret key.
4. With the use of secret key shared by user, compute an encryption key.
5. Encrypt the data using the asymmetric encryption technique and that encryption key.

Decryption

The sender will both proportion the curve with receiver or sender and receiver could have the same use for the same curve form. Additionally, sender gives permission to recipient access to its public key.

1. Produce a public and personal key pair using the receiver's curve.
2. Using the sender's public key and the recipient's private key, regenerate a shared secret key.

3. Create an encryption key using the shared secret key.

4. Decrypt the data using the symmetric encryption algorithm and that encryption key.

V. Experimental Results

The following session discusses the encryption and decryption time performance comparison. The suggested solution uses an ECC-based encryption technique to improve data sharing security. Fig 3 shows the parameters that are utilized to estimate the speed of the proposed system when interacting with cloud users are the time taken for encryption and decryption process. The shorter time demonstrates the user and cloud server's high-speed communication. Here, the system estimates the time taken for encryption and decryption for the suggested ECC algorithm and the current AES technique. When compared to the figure below, the suggested architecture performs better in terms of encryption and decryption time.

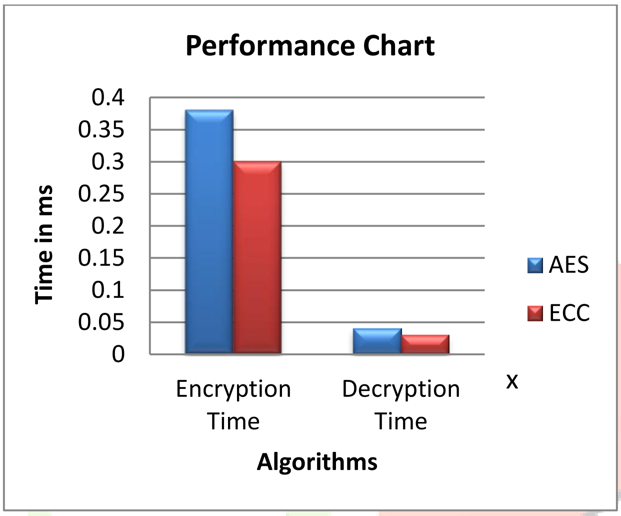

Fig 3. Comparison of Encryption and Decryption Time of Various Algorithms

VI. Conclusion

In this work, developed a website to store and access documents, utilized an ECC encryption method with verifiable outsourced decryption, demonstrating the system's security and verifiability. Searchable encryption offers a powerful solution for preserving the privacy and confidentiality of sensitive data while enabling efficient search operations. By employing ECC, a widely adopted asymmetric encryption algorithm, the searchable encryption scheme ensures strong cryptographic protection for the data. ECC has smaller key size and provides high level of security and has been extensively studied and tested for its resistance against various cryptographic attacks. The index construction approach complements ECC encryption by allowing for efficient search operations on the encrypted data. Through the construction of indexes or data structures that capture the necessary information about the encrypted data, the scheme enables keyword-based searches or other types of queries without requiring the decryption of the entire dataset. In order to enable result ranking, the similarity score is computed using the secure inner product computation after the keywords have been searched for similarity. This approach significantly improves the search efficiency while maintaining the privacy, integrity and security of outsourced cloud data.

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 Vol. 58 (2021).

[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 Vol. 18 (2019).

[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 Vol. 32 (2020).

[4] Pham Chien Thang, Ta Thi Nguyet Trang, Bui Trong Tai, A Prasanth, Multimedia Privacy, Security, and Protection within the Blockchain: A Review, Proceedings of IEEE 5th International Conference on Contemporary Computing and Informatics, (2022).

[5] K.B.Bhaskar, A.Prasanth, P.Saranya, An energy-efficient blockchain approach for secure communication in IoT-enabled electric vehicles, International Journal of Communication Systems, Vol. 35 (2022).

[6] Asharov, Gilad, Gil Segev, and Ido Shahaf. "Tight tradeoffs in searchable symmetric encryption." Journal of Cryptology Vol. 34 (2021).

[7] 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 Vol. 16 (2020).

[8] 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 Vol. 149 (2020).

[9] 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 Vol. 10, (2020).

[10] 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 Vol. 10 (2020).

[11] 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 Vol. 13 (2020).

[12] Tariq, Husna, and Parul Agarwal. "Secure keyword search using dual encryption in cloud computing." International Journal of Information Technology Vol. 12 (2020).

[13] 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 Vol. 108 (2020).

[14] 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), IEEE, (2021).

[15] 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 Vol. 8 (2020).

[16] 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 Vol. 8 (2020).

[17] 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 Vol. 16 (2020).

[18] Belchior, Rafael, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. "A survey on blockchain interoperability: Past, present, and future trends." ACM Computing Surveys (CSUR) 54, no. 8 (2021): 1-41.

[19] Wang, Yuntao, Zhou Su, Ning Zhang, Jianfei Chen, Xin Sun, Zhiyuan Ye, and Zhenyu Zhou. "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain." IEEE Transactions on Industrial Informatics Vol. 17 (2020).