A Secure and Efficient Framework for Multi-User Encrypted Cloud Databases Supporting Single and Multiple Keyword Searches

J V S Arundathi[1], Dr. K V V Satyanarayana[2]
Ph.D Scholar, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India[1]
Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India[2]

***Abstract*—Multi-user encrypted cloud databases have become essential for secure data storage and retrieval, especially when supporting both single and multiple keyword searches. Ensuring data confidentiality, integrity, and efficient access within such systems is paramount, particularly when dealing with multiple data owners and users. This paper presents a Secure Encrypted Trie-based Search (SETBS) method that significantly enhances multi-owner authentication, data secrecy, and data integrity in cloud environments. The SETBS framework leverages a sophisticated Merkle hash tree for dynamic maintenance and autonomous user verification, ensuring that the identity of users is reliable and that personal information remains protected across various ownership domains. By optimally utilizing resources, SETBS provides a robust and efficient solution for managing data in cloud environments. The framework addresses the bottleneck issue by distributing the workload among first-level owners, resulting in fair resource distribution and increased system efficiency. A key feature of the SETBS method is its ability to guarantee data integrity without compromising security. Users can be assured that their data remains unaltered and protected from unauthorized access, thanks to the integration of the Merkle hash tree. This mechanism enables clients to confirm the integrity of their data stored in the cloud, providing peace of mind regarding its security. Moreover, SETBS proves to be a flexible and scalable solution for large-scale cloud deployments, efficiently managing multiple data owners and parallelizing the processing load. The framework's focus on data privacy ensures that personal data remains secure during search operations. With lower encryption and decryption times compared to existing methods such as SPEKS, DSSE, and MKHE, SETBS demonstrates superior performance and is implemented in Python. This comprehensive approach offers an all-encompassing solution for businesses seeking to enhance their cloud security architecture while ensuring efficient data management, from processing to real-time or batch data analysis.**

Keywords*—Secure keyword search; encrypted search; multi-user framework; encrypted cloud database; single and multiple key users

I. Introduction

The well-known advantages of outsourced data retrieval and sharing—convenient keeping and on-demand access—have made it popular in the big data era. The global web has developed so quickly that the huge data age has arrived. With the increasing data generation in daily life, cloud storage technology is developing. Cloud computing's exceptional benefits (including reduced expenses, improved work, effectiveness, and safety) have made it popular in the last few years [1]. Databases, which are storage, and servers are among its offerings. With a cloud storage system, individuals and file holders can examine the data remotely once it has been stored on cloud servers. This raises concerns about the confidentiality of data because the cloud server has access to the data and searches [2]. Employing safe cloud databases was the strategy of this paper in offering a hybrid model that tackles the issue of safe and effective information recovery in multi-user environments. The very purpose is the production of a structure that will maintain the confidentiality of information and will at the same time be able to be searched for by consumers using one or more keywords. Credible authentication techniques, which are very efficient with protected information, and work across many people, are only one of the main goals. Atlantis is a unique structure whose sole purpose is to increase the functionality and security of storing, retrieving data, and enabling research over the network, while maintaining safety, ensuring the prompt and precise recovery of data that is well-chosen, encrypted. Besides, it shields out hacker attempts by allowing several individuals to do searches at the same time. The recommended method is created to be the easiest and the one that is best for use in business settings where the efficiency and confidentiality are essential. The goal of this system is to provide a safe and reliable way for the recovered data from the cloud to combine the effective search algorithms as well as protection approaches. Along with these select search protections, developers must ensure that they choose the right encryption methods, have strict security measures in place, use fast, to create this innovative hybrid architecture, the organization would need to factor in the implementation and optimization of the algorithms and protecting the confidentiality of the information, as well as ensuring parallelism and adaptability, proper installation, and compliance with safety standards, amongst others.

Security and functionality are the goals of computer network models that let multiple users search encrypted data in cloud databases. Han et al. [3] developed a novel software-assuring technique which employs a combination of customizable encryption techniques attached to a public Blockchain to enhance strength against attacks on servers. Blockchain's unique approach to decentralized computing secures protection from system intrusions and only allows restricted access-awareness. Investigated on the Ethereum blockchain, the plan turned out to be much better in terms of effectiveness than traditional methods, the one big advantage was the cost-effective

searchable encryption. However, issues such as heavy file processing and the demand for additional internet resources are the main imperfections. The issue of cumbersome computation needs and internet resources is a great problem in the cloud. Only the challenges are alluring Han et al.'s approach introduces a step closer to the full implementation of the said cloud technology. It already provides rapid and secure data transfer to online users who maybe just residents in New York or the Illinois area. Moreover, under security concerns cryptography protocols were applied. Cui et al. [4] gave the first account of the Multi-User Safe and Verifiable K Nearest Neighbor (MSVkNN) search idea that deals with the privacy and integrity of the multithreaded areas as included among the K Nearest Neighbor queries in the cloud-based location services. A concise and improved version is here the abstract of this framework, which makes use of, the Verifiable and Secure Index (VSI) structure, and its corresponding protocols have been designed to safeguard the issue of data, the queries, the results, and the access patterns. Thanks to VSI technology, it is also possible to delink the ownership of private information, which makes it a privacy-protecting method in both respects, that is, it allows anonymity of the query and the completeness verification of the result. Critically, the MSVKNN method supported the possibility of using multiple keys for different users, which led also to improving the security through rigorous security proofs and empirical testing. In the words of Cui et al., the solution provided by their approach is exhaustive and it not only protects the privacy and integrity of the searches of cloud systems which are based on the new trends in IAR but it can also be applicable in the more complex environments of multi-user.

Blockchain technology is applied in the experimenting of the use of database architectures together with indexed structures by the authors in the ongoing review articles. New approaches are proposed to be used in the data retrieval process as well as through the privacy issue. The integrity of data and confidentiality become stronger when blockchain becomes the security platform, therefore, important data such as those regarding shipments of essential supplies are protected. The fault is, thereby, shifted by the use of data-mining technologies to resolve usually requiring operations away. Traditional research problems such as allocating resources and processing overhead are overcome by the research groups through their continuous improvement of these strategies. The success of search processes involving encrypted data in cloud computing through the deployment of more effective and more secure encryption techniques is based on the success or failure of the initiatives. In this context, the enhancements offered by data encryption search systems also bring about cloud computation systems to the right procedure, which is more secure and more efficient, hence, promising additional security for increasingly expanding Data access/retention embedded in the changing research.

The main breakthrough of that study is the formulation of a newly established hybrid model meant for the secure and efficient management of cryptographic information in a cloud database that is accessible by multiple users search by single or multiple keywords. The design has been modified such that the latest security requirements are met, and the design that already exists will be coordinated with the current cloud service. This allows it to be the proof that not only do those regulations guarantee the protection of the data but also meet the industry standards and the operability with several cloud providers that in turn create the possibility for using it in different corporate environments without risk of both safety and productivity.

- Introduces an authenticated Search method for multi-owner cloud environments namely Secure Encrypted Trie-based Search that keeps the data secrecy and integrity up to the mark.
- Implements a Merkle hash tree of the latest generation for dynamic operation and self-organizing user verification, and guarantees the authenticity of users and the confidentiality of their data.
- Enhances the management of resources in SC environments, and solves bottleneck problems through an equitable share of the tasks with the first-level owners enhancing the system efficiency.
- Offers a strong and reliable avenue in which the users can verify data stored in the cloud and the security of such data.
- Shows that SETBS is easily scalable and implements well for large-scale applications in the cloud to handle numerous data owners and distribute loads.

The paper is organized as follows: Section II presents other works regarding multi-user encrypted cloud databases and the requirement of having a secure database and efficient storage of data. Problem statement of the paper is given in Section III. The proposed SETBS method is described in the subsequent Section IV. The findings of the paper have been presented and analyzed in the last section known as Section V. Section VI closes with an evaluation of the framework to resource allocation, followed by a consideration of the former for scalability of resource management for massive Cloud provisioning.

II. Related Work

Yoon et al., [5] articulated one of the most innovative advances in the state of the data leveraging Intel SGX as a trusted executor platform. This method decreases computation and communication costs by practically rendering cryptographic processes to its specific enclave in combination with a trusted execution environment (TEE) to prevent cloud-centric side-channel attacks. The architecture benefitting from SGX, SPEKS (Secure and Privacy-Enhancing Keyword Search), is a cryptosystem that allows safe keyword search over the cryptographic texts through the SGX enclave that stores the data. Encryption and geological data security as well as the cryptographical technique is said to be the study's solution which is the way of the magnification of secret key cryptography in computer-generated and general intellectual processes even though it has no reference to the database. The problem with the SPEKS is data security and its necessity for an SGX-capable device that may hamper its usage in devices that do not have these features. Accordingly, the SPEKS approach allowed the computing time for the PEKS, Trapdoor, and Search algorithms to be reduced dramatically. For example, the PEKS calculation durations have gone down from 8.123 ms in previous systems to just 0.0919 ms. Furthermore, it adjacently embeds franchised

transmission and volatile space, therefore, posted offers secured keyword searches in encrypted settings. These developments clarify that SPEKS is a dependable choice that will be - ever since it is - safe for choice for user-friendly and malware-free keyword searches in the latest cloud system.

Liu et al., [6] The IKGAs were scrutinized closely using a lattice-like PEKS system chip to examine the advanced IKGAs. The researchers pay special attention to the PEKS method by Zhang et al. which is called FS-PEKS PEKS for the generation of random files of equal length code for the IKGAs. On the one hand, as said by Liu et al., the security layer, [fs-peks] based on the generation of several derived vulnerabilities to the design is why the intrinsic vulnerabilities of the secure layer of the FS-PEKS that can be derived are the main reasons for the success of the vulnerability research done by the two researchers. Also, the security layer that can be removed at several points of the design, has been referred to as various derived vulnerabilities by the calling. As for the testing of the protocol's consistency and the recognition of threats, the investigation applies such algorithms by changing variables and using some technical skills. A security threat concerning the IKGA inside the system architecture is being reported. The basic principle of dishonest employees' designs to detect the keywords in the system is explored in the paper. They pointed out that none of these technologies can be used in reality, and even if they were used, it would take nature longer time to recover than usual. Their findings imply that more robust PEKS that can deal with insider attacks are requisite for a secure keyword search on encrypted data in sensitive and risky areas like the IoT.

Bulbul et al., [7] suggested a study that tests the suggested plan using the Enron dataset, which consists of a substantial amount of email correspondence between Enron personnel. Dynamic Searchable Symmetric Encryption (DSSE) is the framework that is being employed; it is intended for usage in multiple-user scenarios. Through the use of symmetrical encryption, keyword-based combat, and random number generation for key updates following every query, it guarantees forward as well as reverse secrecy. One of the noted limitations is that creating a doorway requires a longer period than alternatives since reward positions for particular keywords must be determined before the analysis. Despite this, the DSSE method boasts from low connectivity overhead, database creation, and query effectiveness. This studies' findings show that the DSSE approach works better than other approaches in terms of index creation and query effectiveness, proving its usefulness and low-weight architecture in networked settings. Extensive empirical assessments confirmed the approach's exceptional effectiveness in real-life situations and its extraordinary effectiveness in index production.

Li et al., [8] explained a strategy for multi-key homomorphic encryption, which expanded key in the technique, which is based on the DGHV encoding framework, enables secure homomorphic calculations involving various consumers. The current MKHE systems and this improved DGHV program are contrasted. The computational efficiency measurements of many MKHE systems across different security parameter levels (Toy, Small, Medium, Large) make up the assessment dataset. The research's algorithm is an enhanced version of the DGHV technique that has been optimized to decrease the public key space and boost computational efficacy. According to the findings, the suggested MKHE scheme is more effective concerning of computational difficulty and capacity. Compared to current systems, the period needed for key generation and homomorphic operations (ciphertext extension, addition, multiplication, and decryption) is greatly decreased. For example, the suggested system takes 0.05 seconds to decode at the Moderate protection point, whereas ciphertext extension and multiplication take 0.98 and 3.34 seconds, correspondingly. The necessity to interface with CP-ABE for improved DU assign reliability and optimize the ACC's attribute verification algorithm to save petrol expenses are obstacles, nevertheless.

Liu et al., [9] suggested a plan using the Enron dataset, an extensive set of emails exchanged between Enron workers. For analysing retrieval of data algorithms, this dataset offers an accurate and varied measurement. The Key Generation Centre, Cloud Platform, Internal Servers, Data Providers, and Request Users are some of the stakeholders involved in the decentralized framework that is being deployed. The technique maintains privacy and confidentiality while supporting inquiries with multiple keywords. Potential access pattern leakage when users obtain records from search outcomes is one of the suggested scheme's limitations. Furthermore, relative to different systems, the method of searching could take longer, especially as the number of terms rises. The findings demonstrate that the recommended approach outperforms compared approaches in these areas and is efficient in index creation and gateway computing. However, owing to network delay, the search procedure can take longer. Because the technique protects data, search, and search pattern privacy, it may be used in actual-life situations where effectiveness and safety are crucial.

Cui et al. [4] proposed the Multi-User Safe and Verifiable k Nearest Neighbor search (MSVkNN) which is a k-nearest neighbor query architecture in a cloud database environment that is both secure and verified. At this time, large-scale data that might be brought into play for KNN searches. The proposed model takes advantage of multiple users joining the process of inquiring cloud storage data and integrates public-private cryptographic methods to secure data and verify query results. The writer, however, emphasizes that the design also carries some drawbacks, such as discontinuity problems that have an impact on real-time applications and the computational costs of encryption and verification procedures. The result shows that the architecture maintains strong security and verifiability while achieving high query precision. Nevertheless, the proposed model lacks to access the pattern of privacy protection.

Several methods have been developed recently for safe keyword searches on encrypted data. SPEKS architecture lowers computing expenses and improves secrecy by using hardware that supports SGX. Vulnerabilities in lattice-based PEKS systems are assessed, exposing shortcomings in existing methods. Despite requiring longer setup times, DSSE exhibits efficient index generation and query performance in multiple user scenarios. Enhanced MKHE technique improves effectiveness and safety in cloud computing. Issues about access frequency leaking are addressed by a decentralized design that prioritizes capability and privacy in keyword searches utilizing the Enron dataset.

III. Problem Statement

Data privacy and query confidentiality in cloud databases are guaranteed by an effective encrypted multi-user system. The current approaches frequently have issues with scalability, safe efficient keyword search through encrypted data and control of access. The other existing models have limitations such as only SGX-enabled hardware is applicability[5], susceptible to insider threats, jeopardizing the integrity of the network [6], longer index construction time as a result of determining keyword placements [7], Problems with combined integration and attribute confirmation optimization [8], Possible problems with computing costs and applicability in real time [4]. The proposed approach is perfect for commercial applications requiring high secrecy and efficiency since it guarantees authorized, secret data access for numerous users, securely enables concurrent queries, and handles cloud-based multi-user problems.

IV. Proposed Secure Encrypted Trie-Based Search (SETBS) Method

Secure Encrypted Trie-based Search (SETBS) improves multi-owner authentication, data secrecy, and data integrity in cloud contexts. It uses a sophisticated Merkle hash tree for dynamic maintenance and autonomous user verification. The framework presented is a way to make the identity of a person more reliable and to protect personal information from a variety of different owners that in the end make available fine and secure data search operations. SETBS is a very robust framework for data management in cloud environments that are both safe and efficient since it optimally uses the resources and guarantees the data processes. Through the distributed scheme of the work over the first-level owners, the contribution to the fair resource distribution becomes the highest, the bottleneck issue is resolved and the efficiency of the whole system increases. A Merkle hash tree is a vital element of this approach. This algorithm helps users to know their data integrity without endangering the security. This shows that clients might have a guarantee and confirmation of the data stored in the cloud still being the same without anybody unauthorized touching it and the data is fully protected in this way. Set-Aside Transaction Broker Services (SETBS) are a flexible and feasible choice for big cloud setups as they may manage a multitude of data owners efficiently and parallelize the load. What is more, the focal point of privacy of data presupposes that personal data will be secure in the exploration process. SETBS thoroughly complicates the safety and authenticity of cloud computing systems by harmonizing these traits together. When businesses want to enhance their cloud security architecture, one all-inclusive approach offered for data management in the cloud consisting of such issues as data integrity, confidentiality, and efficient resource use ranging is from data processing to analyzing real-time or batch data.

The procedure of the suggested SETBS model should be presented. The graphic of the data processing pipeline is shown in this Fig. 1, which comprises of data collection, AES encryption, trie-based keyword search, cloud storage, and performance analysis.

A. Data Collection

The KOSARAK dataset provided by an online news portal from Hungary was an unstructured dataset of 41,269 unique items and 990,000 entries. Each record corresponds to the interaction of user interaction. The dataset consists of smallest and largest sequences, which are 1 and 2,498 items long, respectively, along with an average sequence length of 8.10 items per sequence. At the news portal, this data set tell about the order in which pages or articles are viewed, thus, in brief, it gives details about navigation patterns by portraying user movements [1]. User engagement is recognized, and the effectiveness of content, in addition, website techniques and content recommendation software are evaluated using this data [10].

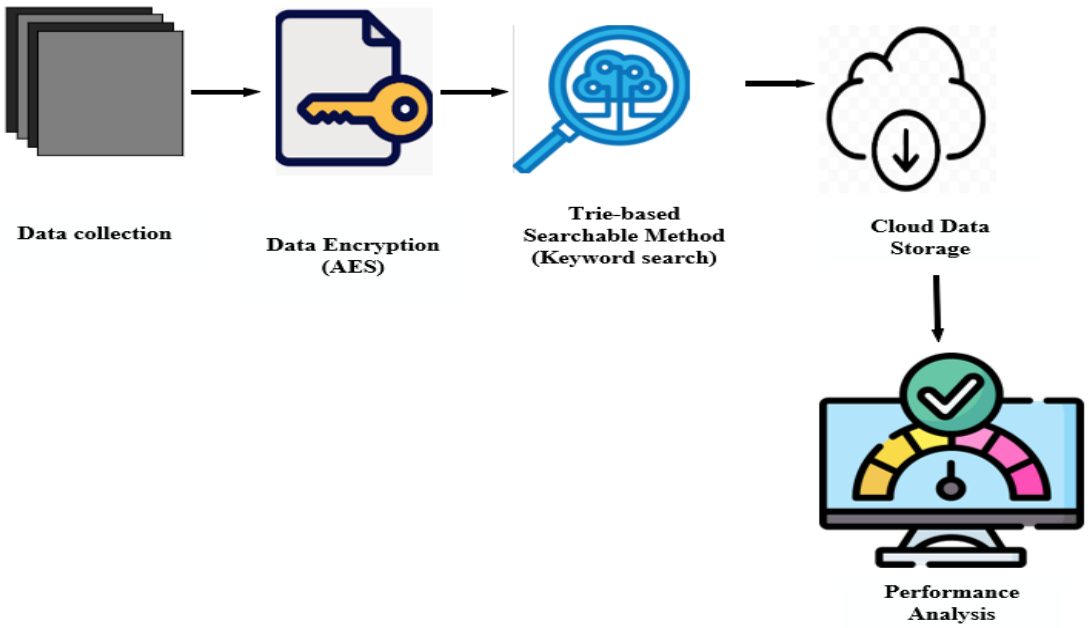

Fig. 1. Block diagram of proposed SETBS model.

The experimental setup included a thorough description of the methodologies employed, focusing on the KOSARAK dataset obtained from a Hungarian online news portal. This dataset, consisting of 41,269 unique items and 990,000 entries, captures user interactions, reflecting the order in which pages or articles are viewed. With sequence lengths ranging from 1 to 2,498 items and an average length of 8.10 items, the dataset effectively illustrates user navigation patterns. Additionally, the analysis emphasizes user engagement and evaluates the effectiveness of content and website strategies, providing a robust foundation for assessing the proposed model's performance and validity.

B. Data Encryption

Data encryption is the process of converting plaintext information into an unreadable format using an algorithm and an encryption key, which can only be decrypted by authorized parties with the help of the decryption key. The purpose of this is to protect your data from unauthorized access and cyber threats [11]. This survey introduces Advanced Encryption Standard (AES) for data encryption. Encryption algorithms are often based on mathematical calculations to convert plaintext to ciphertext. The following is an often-used symmetric encryption Eq. (1) that is inserted below:

$$Ciphertext = AES_{Encrypt}(Plaintext, Key) \quad (1)$$

where, is a symmetric encryption algorithm called AES Advanced Encryption Standard.

1) Advanced Encryption Standard: AES - Advanced Encryption Standard is a symmetric encryption algorithm, and one of the most commonly used ones when it comes to the transfer of data of a sensitive nature. In the context of encrypting data in a dataset as large as KOSARAK, such an algorithm is operated by splitting the data into fixed-size blocks, for instance 128 bits each in the case of AES-128 [12]. The Eq. (2) for AES encryption is described in below:

$$E_k(P) = C \quad (2)$$

where E_k represents encryption with key k, P is the plaintext, and C is the resulting ciphertext.

Here's a detailed explanation of how AES encrypts data:

a) Key expansion selection: AES requires a key for encryption and decryption, typically 128, 192, or 256 bits in length. Before encryption begins, the key undergoes an expansion process to generate a set of round keys, which are used in each round of the encryption process [13].

b) Initial round key addition: Each block of plaintext (or data) is divided into smaller blocks called state arrays. AES starts by performing an initial round key addition. Here, the state array is combined with the first-round key using a bitwise XOR operation.

c) Rounds of substitution and permutation: AES operates through multiple rounds (10 rounds for AES-128) of substitution and permutation.

d) Substitution: Bytes in the state array are substituted with corresponding bytes from a substitution box (S-box), which is pre-defined in the AES specification. This step adds confusion to the data.

e) Permutation: Rows in the state array are shifted cyclically, and columns are mixed using a matrix multiplication operation known as the Mix Columns step. These operations introduce diffusion in the data.

f) Final round: The final round of AES excludes the Mix Columns step to simplify the implementation. Instead, it consists of substitution, permutation, and a final round key addition.

g) Cipher text generation: After completing all rounds, the resultant state array, now transformed through substitution, permutation, and key addition, is the cipher text. This encrypted data is output as the final result of the AES encryption process [14].

C. Multi-Owner Authentication

This solution guarantees the cloud server database by applying a highly protected multi-owner authentication method. The data proprietor first uploads the data in an encrypted way employing an enhanced Merkle hash tree technique to the cloud server. The user is given a public key to see and download the data. The data owner uses the public key to confirm if the user is authorized or not. The data owner gives the user a decryption key if the user permits so they may decode the data. To process the work that the user wants done, a load-balancing notion is also implemented. The user suggestion is finally sent to the cloud server. The user research is answered by the cloud server if the user has effectively [15].

1) Data owner: The data owner must first register on the server of the cloud service provider. Following registration, the data owner receives both public and private keys generated by the cloud service provider. The relevant data are uploaded to the cloud server after being encrypted using the Enhanced Secure storing a lot of data, the cloud service provider also controls user and data owner identification [17]. The cloud server routes the user-requested work to any queue to process it. Virtual machines are used to handle user requests in the queue.

2) Third-party auditor: To verify the integrity of the data stored in the cloud, TPA is applied to encrypted cloud data. The data is submitted by the data owner, and the TPA audits the data upon request. To audit user-requested data, the TPA must register with the cloud server. After bilinearly mapping the user data, the cloud provides the evidence to the TPA. The data supplied by the user and the data from the cloud are compared by the TPA. The file's security is safeguarded by the encrypted data.

3) Bilinear mapping: The first stage of encryption to express the data in mapping form is called bilinear mapping. The input of the data is its cyclic group, and the bilinearly mapped output is denoted by the letter e. Think of group G as a prime order p gap Diffie-Hellman group. Assuming that GT is a prime order multiplicative cyclic group, a bilinear map is created [18]. The following characteristics of a useful $e: G \times G \rightarrow GT$, where GT is a prime order, multiplicative cyclic

group. A useful e has the following (3), (4), (5) properties shown in below: To change the default, adjust the template as follows.

4) Encrypted Trie-based search (SETBS) technique[16]. A public key is used by the sender to encrypt data, and only the holder's private key may be used to decode the appropriate data.

5) User: To utilize the network, the user must first register for an account. The user creates an account, signs in, and asks the cloud service provider to review their account. The cloud service provider will process the work at the request made by the user. Languages for programming like Java and NET are used by the network to communicate with the cloud server. By contacting the cloud service provider, the user may obtain the desired data. The client retrieves cloud data using the provided private key for Secure Encrypted Trie-based search (SETBS).

6) Cloud service provider: The cloud service provider offers flexible online processing and storage of data by combining hardware and software resources. In addition to

$$\text{Bilinearity} - \forall m,n \in G \Rightarrow e(ma,nb) = e(m,n)^{ab} \quad (3)$$

$$Non-degeneracy — \forall m \in G, m = 0 \Rightarrow e(m,m) = \quad (4)$$

$$Computability — e\ should\ be\ efficiently\ computable \quad (5)$$

It is possible to express data using a two-dimensional vector is known as bilinearity; the ability to degenerate data back to its original form is known as non-degeneracy; and the capacity to solve a problem effectively when a and b are real random values is known as computational capability [19].

7) SETBS: Cloud databases with encryption provide a complete solution for secure and effective multi-user keyword searches with the Secure Encrypted Trie-based Search (SETBS) paradigm. The SETBS model offers different ways of protection and is, therefore, more functional and secure, since it is secured through keyword indexing, access control, and trie data structure [20]. Its ability to handle searches using one or more keywords and provide search results that others can check makes it a key addition to searchable encryption in cloud computing. The Secure Encrypted Trie-based Search (SETBS) system offers a reliable and scalable answer for encrypted cloud databases. This model uses a trie data structure because it works well and has potential. To protect the security and integrity of search queries and results, it also combines trie data structure with encryption methods. The SETBS model tries to solve the challenge of supporting both single and multiple keyword searches while meeting strict function and safety needs [21].

8) Trie-data structure: The SETBS model relies on the trie-data structure to organize and index keywords. In this structure, each node stands for a character in a term. Complete keywords are shown by paths that end at leaf nodes. Large volumes of encrypted data may be easily managed with the trie's hierarchical structure, which enables quick keyword lookup and retrieval. Verified Data Structure MTrie. Our proposal for MTrie, a new authenticated data structure based on MHT and Trie, is presented in this part of the paper. This study provides the relevant analysis of every node in the Trie, by the idea that MHT uses an organizational hash mechanism to offer query-based verification.

To obtain the root signature Sroot, as indicated in the equation below, DO first computes the hash value of each MTrie node. Then, using the secret key sk, it signs the hashed level of the MTrie root or Sroot in Eq. (6).

$$s_{root} = si_{sk}^{g}(h_{root}) \quad (6)$$

where s_{root} is produced by the use of a secret key signature technique si_{sk}^{g} the hash of the root value h_{root} The legitimacy and reliability of the root value are guaranteed by this procedure.

D. VO Construction

CSP employs Algorithm 1 to compute the query findings create the VO according to the query outcomes and execute the approximation string query q. In particular, VO contains the following four categories of data: utilizes Algorithm 1 to extract the last VO in the following manner, considering the query string q = "inf" and the distance to edit threshold d = 1.

$$VO = \left[I\left[*\,n\,[*\,n,*\,t]\right], t\,[(e,h6),(o,h9)]\right] \quad (7)$$

The query outcome set {"in","inn","int"} that satisfies the distance to edit threshold criterion has been incorporated in the VO, which is at last returned to the user via CSP together with the sign of the root node.

Initializing keys and an empty trie structure is the first step in the process. Before entering a keyword into the trie, it is hashed and encrypted. To find correspondence, search tokens are created and compared to the trie. Results include decrypting, compiling, and presenting matching data. Before revealing results or pointing up security flaws, tests make sure that reliability, honesty, and secrecy are met. This technique guarantees reliable data recovery while upholding strict security protocols during the process of searchable encryption.

Fig. 2 is a visual representation of the interaction between a client and an encryption module that encrypts data and places it in a trie data structure of the cloud server. The user's search queries are sent to the server, which processes these queries. Decrypted answers are sent back to the users by means of a decryption module.

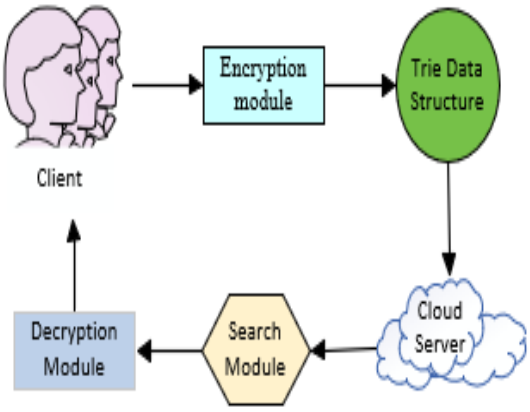

Fig. 2. System model.

The focal point of the proposed framework is bettering the safety through the gaining of a protected storage and data tool as well as the realization of the abilities of cloud databases to be a source of the information. The try-crypto-organized data structure, which does the encryption of the keywords hierarchically, that, allows for the function of search in fast and effective manner is one of the major building blocks of the system. Incoming up with an encrypted word search system where each keyword is encrypted using a safe cryptographic procedure before being put in the trie is an effective strategy. Users have to prove their authentic identity and then are assigned only the authority to execute the search a part of the procedure in order to make sure that only those with the right to a specific access can carry out searches and see data. This is accomplished by constructing the tree structure, which can go through the encrypted keywords and the matching procedure for both single and multiple keywords. The structure guarantees that the process of searching is not discerned and the operation goes on without the user decrypting the data, hence the data is safe from being read by unauthorized people. The protected query is then run through hashing to the encrypted trie. After that, the user receives the encrypted results which they may return to their plaintext using their private key [22]. One of the features of the infrastructure is a powerful access control system. It is the system which manages the different rights and access of the users, and it supports the presence of many users as well. It even ensures that the users' search queries and results are top secret and there are no unauthorized accesses. Additionally, this approach is useful in that it increases the safety of the cloud database applications but on the other hand, it also optimizes the search performance.

V. Results and Discussion

The result section provides a holistic overview of the study findings of Secure Encrypted Trie-based Search (SETBS) technology. It describes the method's advantages over SPEKS, DSSE, and MKHE. Since it is clear. Speaking about the result, which is the performance of SETBS in comparison to the other ones, SETBS being properly clear and fast on its own was more par than this one. Now, it confirms the right way for the technical development to ensure that SETBS excels in achieving fast and scalable cloud database processing. The set of techniques specifies SETBS's benefits when compared to the traditional techniques and presents the application ideas in all areas. For enterprises who want faster search and high scalability in a cloud environment, SETBS is a potential alternative since it enables faster search speeds and scalable without damaging privacy. These results demonstrate that this feature of SETBS is very useful and the injecting of the searchable security algorithms into data-intensive computing.

A. Performance Evaluation

The performance evaluation of the framework is achieved through these metrics in cloud systems operated by more than one person. The accuracy point guarantees correct results, the scalability point determines the system's possibilities of development, the security point stands for the data that is safe and the retrieval time fact checks the operational efficiency. They jointly offer a profound insight into the usability and robustness of the system in cloud settings.

TABLE I. Performance Metrics of Proposed Model

Metrics	SETBS (proposed)
Single Keyword Search Time (ms)	3.456
Multiple Keyword Search (ms)	5.678

Table I easily demonstrates the performance measures of the systematic mechanisms being the empirical results of SETBS. The search times are enclosed in the measurements both for single and multiple keywords. The search time of a single keyword is 3.456 milliseconds and this figures out the framework single-keyword queries quickly. The average response time for hunts with multiple keywords is longer at 5.678 milliseconds, once again showing its ability to handle not only simple queries but also more complex ones very fast. This shows the complete accuracy of SETBS which is used in cloud storage solutions and gives a snapshot of the search process to the user even in the shortest time.

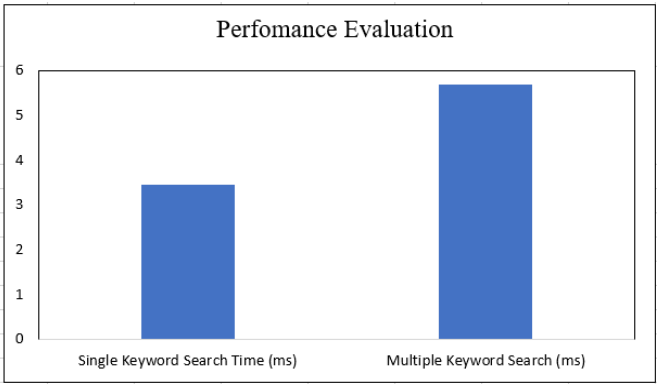

Fig. 3. Performance evaluation of proposed model.

In Fig. 3, the diagram symbolizes the search times of the search engine model SETBS, which was designed because of the one-day motivational improvement of, search times for both single and multiple keywords. The x-axis represents the type of search, while the y-axis denotes the search time in milliseconds. Two bars demonstrate the search times: 3.456 ms for a single keyword search and 5.678 ms for several keyword searches. The chart below indicates the performance of the SETBS model in terms of how quickly it handles searches with several keywords, which is explained above.

TABLE II. Proposed Model Comparison with Existing Models

Methods	Single Keyword Search Time (ms)	Multiple Keyword Search (ms)
SPEKS	8.123	10.234
DSSE	5.789	7.345
MKHE	6.912	8.567
SETBS (proposed)	3.456	5.678

The SETBS methodology greatly reduced the time required to get data for both single and multiple keyword searches when compared to other methods. The comparison of retrieval times for various approaches is displayed in Table II. This table includes SPEKS [23], DSSE [24], MKHE [25], and the suggested SETBS, compares the millisecond search times of

many models for single and multiple keyword searches. The speed at which each of the models can execute a search query is used to gauge its performance. The suggested SETBS model outperforms the existing models with the fastest search time of 3.456 ms for single-term searches. After the DSSE model once again, the times of 7.345 ms, 8.567 ms for MKHE, and 10.234 ms for SPEKS are the fastest. These findings show that, for both single and multiple keyword searches, the SETBS framework outperforms other models in terms of efficiency. SETBS appears to be a more efficient method, as seen by the notable decrease in searching times. This might result in enhanced performance and faster retrieval of data for systems that use encrypted keyword searches. SETBS continues to do exceptionally well when it comes to multiple keyword searches, recording the fastest search time of 5.678 ms.

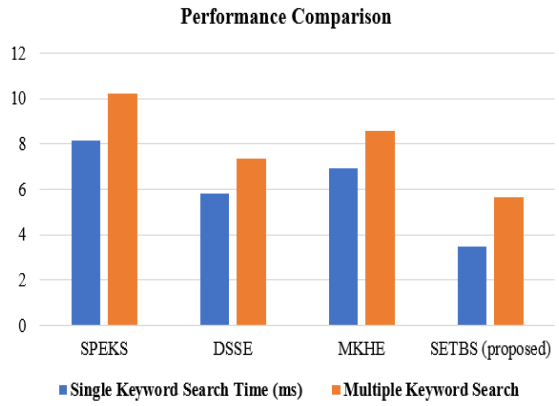

Fig. 4. Proposed model comparison with existing models.

The search durations for single and multiple keyword searches across four different frameworks —SPEKS, DSSE, MKHE, and the suggested SETBS—are graphically shown in Fig. 4. Two bars show the performance of each framework: an orange bar shows the multiple keyword search duration and a blue bar shows the single keyword search time (measured in ms). SPEKS shows comparatively long search times in this data, ranging from around 8 ms for single-word searches to about 10 ms for multiple-word searches. With a search duration of around 6 ms for single keyword searches and a little over 7 ms for multiple keyword searches, DSSE performs better than SPEKS. With a search duration of about 7 ms for individual keyword searches and 8.5 ms for multiple keyword searches, MKHE has search times that are lower than SPEKS but higher than DSSE. The proposed framework exhibits the fastest search times and greatest efficiency. For single keyword searches, it takes around 3.5 milliseconds, while for multiple keyword searches, it takes about 5.5 milliseconds. The SETBS model is a superior choice for quick and effective encrypted keyword searches than the other models, as this figure demonstrates. It performs better than the existing models in both single and multiple-keyword search cases.

B. Running Time of Proposed Model

The running time of the Proposed SETBS method depends on several factors including the size of the trie, complexity of the search queries, and efficiency of cryptographic operations. Typically, it involves constructing the encrypted trie, which may incur an initial setup cost, and then performing encrypted search operations, which are generally efficient due to trie's logarithmic search time relative to the size of the trie. Overall, SETBS aims for practical efficiency while ensuring secure keyword search capabilities in encrypted data environments.

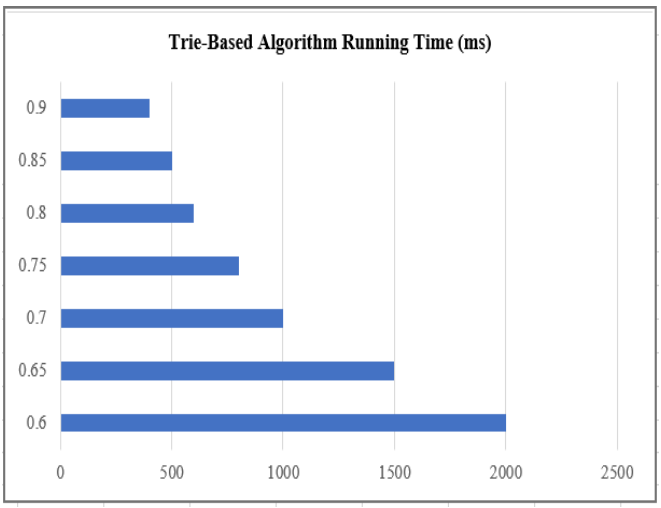

Fig. 5. Running time of the proposed model.

Fig. 5 demonstrates the given values denote the trie-based searchable encryption framework's running time for different values of (t). The duration of the run reduces with increasing (t), indicating that greater amounts of (t) optimize the search process and shorten the time needed to retrieve keywords. The trend of decreasing running time with increasing (t) presents the trie-based approach's efficiency in analysing encrypted search queries.

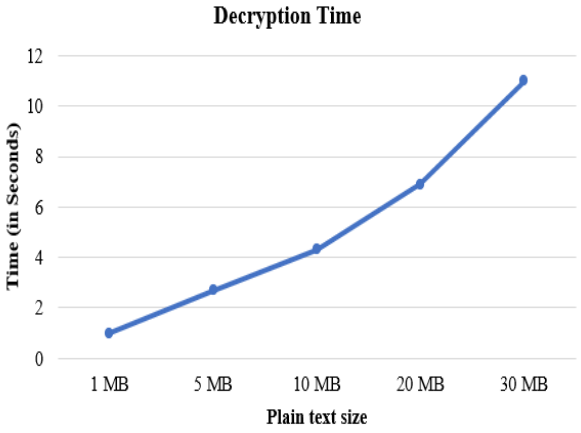

Fig. 6. Decryption time of AES.

The trie-based searchable decryption framework's processing time for varying data input sizes is depicted in Fig. 6. The framework takes one second for a one MB input, 2.7 seconds for a five MB input, and 4.3 seconds for a ten MB input. Processing 20 MB and 30 MB of bigger data inputs takes 6.9 and 11 seconds, respectively. This illustrates how the framework can be scaled and used effectively to handle different data quantities in encrypted cloud settings.

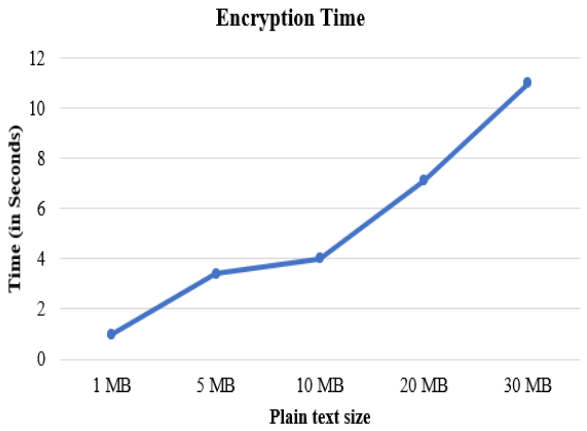

Fig. 7. Encryption time of AES.

Fig. 7 shows how long the trie-based searchable encryption system takes to handle different amounts of input data. The processing time is one second for an input of one MB. The timings grow to 3.4 seconds and 4 seconds, respectively, as the data input size increases to 5 MB and 10 MB. The processing speeds are 7.1 seconds and 11 seconds, respectively, for bigger inputs of 20 MB and 30 MB. These outcomes demonstrate how well the framework scales to accommodate varying data sizes.

C. SETBS Framework

Compared to conventional searchable encryption techniques, which frequently struggle to balance security and speed, the SETBS framework offers an important improvement in secure keyword searches for encrypted cloud databases. Its use of a trie data structure ensures efficient indexing and recovery of encrypted keywords; moreover, the hierarchical nature of the trie permits for rapid traversal, making both single and multiple-keyword searches practicable without sacrificing speed; additionally, the use of Advanced Encryption Standard (AES) ensures robust data protection against unauthorized access; finally, performance metrics reveal that SETBS achieves a single keyword search time of 3.456 milliseconds and a multiple keyword search time of 5.678 milliseconds, outperforming. For applications that need adequate safety and quick data retrieval, such as those in commercial cloud settings, this upgrade is essential. To further improve security, the framework's robust access control system makes sure that only authorized users may conduct searches. Overall, SETBS tackles the main issues with searchable encryption in multi-user cloud environments, providing a scalable and effective approach that satisfies strict security standards.

In evaluation to current searchable encryption techniques, SETBS extensively outperforms its friends in phrases of search performance and protection. For instance, whilst the SPEKS approach suggests seek instances of eight.123 milliseconds for unmarried key-word searches and 10.234 milliseconds for multiple key phrases, SETBS achieves a first rate three.456 milliseconds and 5.678 milliseconds, respectively. Similarly, other fashions like DSSE and MKHE display longer retrieval instances, with DSSE recording 5.789 milliseconds for unmarried keywords and seven.345 milliseconds for more than one key phrases, and MKHE at 6.912 milliseconds and 8.567 milliseconds. These metrics genuinely suggest that SETBS not best hurries up the search manner however additionally keeps robust security through its AES integration, making it a greater powerful alternative for applications in encrypted cloud environments. The better overall performance of SETBS positions it as a superior desire for customers desiring fast get right of entry to touchy data even as ensuring strict privacy and safety features.

To offer a greater complete and illustrative assessment, it's miles important to give no longer only the uncooked overall performance metrics but additionally contextualize them within actual international scenarios wherein every technique may be carried out. For instance, at the same time as SETBS boasts astonishing search times of three.456 milliseconds for single key phrases and five.678 milliseconds for multiple keywords, it's far important to spotlight that these rapid retrieval abilities enable users to speedy get admission to important statistics in time-touchy environments, which includes healthcare or economic offerings. In evaluation, SPEKS, with seek times exceeding 8 milliseconds, may additionally avert performance in programs requiring instant statistics retrieval, doubtlessly leading to delays in decision-making methods. Similarly, even as DSSE and MKHE display advanced overall performance over SPEKS, their retrieval times of 5.789 milliseconds and 6.912 milliseconds, respectively, nevertheless lag behind SETBS, which could be unfavourable in situations in which massive volumes of queries need to be processed quickly, consisting of in big statistics analytics. Moreover, incorporating qualitative components, together with personal experience and ease of integration into existing structures, similarly underscores SETBS's advantages, making it now not simplest a quicker choice but additionally a more sensible and consumer-pleasant solution in the realm of steady key-word searches in encrypted cloud databases.

D. Discussion

The SETBS framework represents a tremendous advancement in steady keyword searches for encrypted cloud databases, efficiently addressing the common demanding situations of balancing safety and pace that conventional searchable encryption strategies frequently face. By utilizing a trie records structure, SETBS enables efficient indexing and retrieval of encrypted keywords, facilitating short single and a couple of keyword searches without compromising overall performance. The hierarchical nature of the trie allows for speedy traversal, while the combination of Advanced Encryption Standard (AES) ensures strong records safety in opposition to unauthorized access. Performance metrics display that SETBS achieves marvelous seek times of three.456 milliseconds for single key phrases and 5.678 milliseconds for more than one key phrases, surpassing current strategies. This enhancement is mainly important for packages requiring both excessive protection and rapid facts retrieval, together with those in commercial cloud environments. Additionally, the framework's stringent get entry to manipulate system ensures that handiest authorized users can carry out searches, in addition strengthening its security posture. Overall, SETBS successfully resolves key issues related to searchable encryption in multi-person cloud settings, offering a scalable and efficient answer that clings to rigorous protection requirements [3].

VI. Conclusion and Future Work

In this paper, we present the SETBS method, which extends the security, as well as improves the efficiency of the multi-user encrypted cloud databases. In SETBS, the Merkle hash tree is well employed to enable dynamic addition/subtraction of owners and self-verification of the owners together with secure and efficient multi-owner authentication, non-disclosure of data, and data tamper proofing. The above framework shows significant enhancements compared to the previous techniques as follows: the encryption and decryption time is less therefore the framework proves to be more effective and viable solution on the cloud for managing the encrypted data. Some important issues like resource constraint, task performance consequences of bottlenecks, and inadequate data management are well solved by SETBS by properly controlling the load and work distribution to the first level owners. But it does so in a way that optimizes the general operational efficiency of the system in question; it also addresses the system bottleneck problem. The fact that one can verify the data consistency with reasonably high security gives additional confidence in data protection. In addition, the scalability of SETBS also allows for large scale and multiple data owners in a cloud and parallel processing in case of large volume. There are several directions for the further development of the SETBS framework which need to be investigated in future research: Firstly, it is possible to enhance the security aspects and performance of the SETBS with the help of the further incorporation of innovative cryptographic approaches. Moreover, applying the framework to analytically more demanding forms of queries and data representations might expand the area of its utilization and relevance. It was seen that extending SETBS to various cloud environment as well as putting it through different loads could give valuable indication of its stability and versatility. However, when linked to other cloud-based services and platforms, SETBS could present a more global solution of storing and protecting data. Finally, user studies and real-world implementations may offer insights into further improvements of the proposed framework and deal with certain issues that may arise with other applications.

The future scope of this studies encompasses several avenues for enhancement and application. Firstly, the framework can be improved to aid more complicated question kinds beyond unmarried and multiple key-word searches, doubtlessly integrating herbal language processing techniques to enhance user interaction. Additionally, the incorporation of device mastering algorithms ought to decorate the framework's capacity to adaptively optimize seek efficiency based totally on user conduct and alternatives. Exploring the integration of blockchain technology could similarly bolster safety and transparency in multi-user environments. Furthermore, applying the framework to diverse domains, which include healthcare, finance, and e-commerce, can provide precious insights into its versatility and robustness in managing sensitive facts. Finally, carrying out good sized actual-international user studies will help validate the framework's overall performance and user satisfaction in diverse operational contexts.

References

[1] Xu and Shiyuan, "Lattice-based Public Key Encryption with Authorized Keyword Search: Construction, Implementation, and Applications," 2023.

[2] Y. Wang and D. Papadopoulos, "Multi-user Collusion-Resistant Searchable Encryption for Cloud Storage Yun Wang, and Dimitrios Papadopoulos," 2023.

[3] J. Han, "Attribute-Based Access Control Meets Blockchain-Enabled Searchable Encryption: A Flexible and Privacy-Preserving Framework for Multi-User Search Jiujiang," 2022.

[4] N. Cui, "Towards Multi-User, Secure, and Verifiable kNN Query in Cloud Database," 2023.

[5] H. Yoon, "SPEKS: Forward Private SGX-Based Public Key Encryption with Keyword Search," Nov. 2020.

[6] Z.-Y. Liu, "Cryptanalysis of 'FS-PEKS: Lattice-based Forward Secure Public-key Encryption with Keyword Search for Cloud-assisted Industrial Internet of Things,'" Jun. 2021.

[7] S. S. Bulbul, "Fast Multi-User Searchable Encryption with Forward and Backward Private Access Control Fast Multi-User Searchable Encryption with Forward and Backward Private Access Control," 2024.

[8] X. Li, "Privacy preserving via multi-key homomorphicencryptionincloud computing," 2023.

[9] X. Liu and Y. Guomin, "Privacy-Preserving Multi-Keyword Searchable Encryption for Distributed Systems," 2020.

[10] L. Jia, "A Trie Based Set Similarity Query Algorithm." 2023.

[11] M. N. Ramachandra, "An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard," 2022.

[12] M. Azhari, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," 2022.

[13] A. Kumar and C. Shantala, "An extensive research survey on data integrity and deduplication towards privacy in cloud storage," Int. J. Electr. Comput. Eng., vol. 10, no. 2, p. 2011, 2020.

[14] F. S. Abas and R. Arulmurugan, "Radix Trie improved Nahrain chaotic map-based image encryption model for effective image encryption process," Int. J. Intell. Netw., vol. 3, pp. 102–108, 2022.

[15] Y. WANG, "A Trie-Based Authentication Scheme for Approximate String Queries," 2024.

[16] J. S. Jayaprakash, "Cloud Data Encryption and Authentication Based on Enhanced Merkle Hash Tree Method," 2022.

[17] V. Melnyk, "Data Structures and Lookup Algorithms Investigation for the IEEE 802.15. 4 Security Procedures Implementation.," in IntelITSIS, 2021, pp. 494–513.

[18] R. Subrahmanyam, N. R. Rekha, and Y. S. Rao, "Authenticated distributed group key agreement protocol using elliptic curve secret sharing scheme," IEEE Access, vol. 11, pp. 45243–45254, 2023.

[19] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology," IEEE Access, vol. 8, pp. 45468–45476, 2020, doi: 10.1109/ACCESS.2020.2976894.

[20] L. Jia, "ATrie Based Set Similarity Query Algorithm," 2023.

[21] C. Ghasemi, "Content Distribution over Named-Data Networks," 2020.

[22] H. Zhong, Z. Li, J. Cui, Y. Sun, and L. Liu, "Efficient dynamic multi-keyword fuzzy search over encrypted cloud data," J. Netw. Comput. Appl., vol. 149, p. 102469, 2020.

[23] S. Syväniemi, "Evaluating the fabrication and performance of sulfonated biochar composite membranes for copper redox flow battery," 2024.

[24] M. R. Ahmed, J. M. Cano, P. Arboleya, L. S. Ramón, and A. Y. Abdelaziz, "DSSE in European-type networks using PLC-based advanced metering infrastructure," IEEE Trans. Power Syst., vol. 37, no. 5, pp. 3875–3888, 2022.

[25] J. Park, "Homomorphic encryption for multiple users with less communications," Ieee Access, vol. 9, pp. 135915–135926, 2021.