PERMISSIONED BLOCKCHAIN AND EFFICIENT INTERNET OF THINGS

Sonali Solat[1], Sujay Awale[2], Sakshi Barkare[3], Kunal Gaikwad[4], Amita Toraskar[5]

[1] *Professor, Information Technology, Dhole Patil College Of Engineering, Maharashtra, India*
[2] *Student, Information Technology, Dhole Patil College Of Engineering, Maharashtra, India*
[3] *Student, Information Technology, Dhole Patil College Of Engineering, Maharashtra, India*
[4] *Student, Information Technology, Dhole Patil College Of Engineering, Maharashtra, India*
[5] *Student, Information Technology, Dhole Patil College Of Engineering, Maharashtra, India*

ABSTRACT

The maintenance and effective improvement in health is considered an essential part of human beings lifetime and in countries across the world it is a human right. The individual health of a person is highly critical aspect that can determine the person's productive output. A healthy person is happier and can perform with effective efficiency that can considerably impact the workplace and the company. There have been several advances in technology which have been useful in improving the healthcare sector significantly. The idea of remote medicine through the use of IoT sensors can be extremely effective in reducing the doctor's workload and also enable ubiquitous monitoring of the patients. But the incidences of increased utilizations of these types of sensors can leave the sensitive data at risk of theft or manipulation. Most of this sensor data is effectively being uploaded onto the cloud platforms which puts it at a greater risk. The increased convenience of the IoT devices and cloud platform in healthcare is highly coveted and there is a need for an alternate to secure this data with robustness. Therefore, this approach defines an effective search over encrypted cloud IoT data that utilizes, Arduino UNO, Encryption and Blockchain along with Bucket and trapdoor formation. This approach has been tested through in-depth experimentation that has resulted in highly effective results.

Keyword: - *Internet of Medical Things, Public Cloud, Medical Health Records, Cryptography, Search over encrypted data.*

1. INTRODUCTION

Humans have an inherent right to the care and treatment they need to be healthy throughout their lives. An individual's health is a crucial factor that may significantly impact the individual's level of productivity. A healthful employee is more likely to be happy in their job, which improves their productivity and results. Numerous technological developments have served to greatly enhance healthcare. With the use of Internet of Things (IoT) sensors, remote medical care may be provided, lowering doctors' burden while allowing for constant surveillance of patients.

More and more situations call for the use of such sensors, but this increases the possibility that confidential information may be lost or tampered with. There is an increased danger since much of this sensor information is essentially being transferred into cloud services. Stronger data security is required in medicine, where the improved accessibility of IoT equipment and the cloud-based platform is much sought after.

Due to advancements in computing power and the proliferation of online services, the volume of data is expanding exponentially. Consequently, more and more people and businesses are turning to cloud storage services in order to relieve the stress of data storage and to make their data available to others who may benefit from it. Meanwhile, the information is encrypted before even being uploaded to avoid content leakage. The last ten years have seen tremendous advancements in cloud technology, both in academia and industry. Furthermore, it has also been recognized as a novel model of modern infrastructure that can efficiently and effectively organize unrestricted

hard drive space as well as potent computation, allowing users to appreciate memberships, comfortable and characterized assistance from a common cloud computing is a framework.

Furthermore, the method may lessen the initial investment in hardware setup, software, and people upkeep. As a result of these benefits, businesses and people are increasingly turning to cloud servers to store their data. Contracting data, especially susceptible data, to cloud storage raises privacy issues, which limits the spread of this new paradigm despite its many benefits. Because data controllers no longer have personal control over their data, cloud service companies may utilize it in an illegal manner, even intentionally. The potential for financial loss or reputational harm due to cloud information leakage makes privacy and information security crucial factors that need to be well-addressed in addition to accomplish more productive use and wider implementation of cloud technology.

Encrypting information before outsourced is one of the many cryptographic methods that may be used to safeguard sensitive information. Such procedures, nevertheless, increase the complexity of data use even though many strategies used on original data, including such search term data acquisition, aren't any more appropriate for ciphertext information. It is impractical and impossible to retrieve and decrypt all data locally, particularly if there is a lot of data stored in the cloud. Many people have spent a lot of time and energy developing effective algorithms for querying through encrypted cloud-based information in an attempt to lessen the influence of cryptography on available information.

Cloud data integrity audits predicated on the term with private data is a novel issue that Xiang Gao [1] tackles. In order to verify the connection that files include the searched keyword and to create the auditing evidence without revealing the identity of the file which contains the questioned keyword, the authors created a brand-new label termed RAL. Through extensive tests, the researchers demonstrate the safety of the suggested approach and assess its usefulness in practice.

In a multi-data-owner scenario, Sherif Abdelfattah [2] suggested a safe and efficient search technique across encrypted medical cloud data. This is known as economical and Privacy-preserving Searching over Medical cloud. The cloud server is unable to understand the semantic similarity of indexes and partitions, but it can calculate noisy values and communicate them to the doctor so that they may be de-noised, allowing for Economical and Confidentiality Searching over Medical cloud. Even more so, EPSM permits a novel function that lets physicians tailor their query results by specifying search requirements in the trapdoors. This comprehensive demonstration and sensitivity study shows that EPSM is safe versus renowned plaintext and known background modeling and may be used to protect patient privacy. In addition, EPSM guarantees that any indices/trapdoors with the same terms are not connected to one another. EPSM is optimized for a multi-data-owner situation, making it a little more appropriate for medical applications, and our comprehensive studies show that it needs minimal calculation and communication overhead expenses and a limited number of keys.

Using the work of Hyunsoo Kwon [3], we suggested a safe and effective similarity search technique for M/M environments. Regardless of whether no comparable data is provided, the proposed technique ensures asymptotically optimum comparison searching and query privacy. For the proposed approach, we first verified its security from the standpoint of request, indexing, and file confidentiality under conventional complexity considerations, and then demonstrated its adaptive semantic security. The first is figuring out how to provide support for advance and reverse privacy, both of which are critical for real-time data changes. The latter is to do away with the need for the central trusted component, such a key service in the suggested protocol.

Section 2 of this research article presents an analysis of the relevant literature; Section 3 explains the research approach; Section 4 discusses the experimental assessments; and Section 5 closes with suggestions for further study in the future

2. RELATED WORKS

In his recent article, Bin Wu [4] proposes a new route finding approach that uses searchable encryption to support the ranking order. We begin by outlining the big picture of our strategy, which involves three distinct phases: creating a chained list, making an index, and doing route finding. Next, we demonstrate that our method is secure and that it satisfies the requirements of adaptive translational security. Furthermore, empirical is used to evaluate our suggested system and confirms the scheme's superior speed and performance.

An effective search approach for encrypted cloud data is proposed by Lingbing Tao [5], which makes use of characteristics to identify joint words (FMJK). Joint keywords are generated by randomly selecting a subset of non-duplicated keywords taken from the data owner's documents; together, these keywords constitute a keyword dictionary with a significantly reduced dimensionality. This boosts search performance by decreasing the keys, indexes, and trapdoor's dimensions, which are all connected to the dictionaries. Every index and trapdoor is built with precision, matching document characteristics and query keywords against the joint terms in the words lexicon to provide a weighted score that guarantees the precision of the query.

As stated by Guoxiu Liu [6], the fuzzy searching of the term is ignored if the query keyword entered by the user does not match the specified keyword. This might happen due to input or spelling mistakes while entering the query phrase. It is common for a single term to have many interchangeable meanings in real-world contexts. As a consequence of the user's failure to take into account the broader meaning of the term, the search will provide misleading results. To address this issue, we present a cloud-friendly, multi-keyword searchable, fuzzy semantic encryption system. The fuzzy search is carried out by integrating the Distance measure with the fingerprints of the query keywords and the dictionary generated using a keyword fingerprint generating technique.

To combat duplicate data and ensure that search terms can be trusted, Xueyan Liu [7] proposes a keyword search method based on attributes. Sharing data is encrypted using the ABE method of concealed access policy, which not only ensures the privacy of the data but also allows for more granular control over who has access to it. First, a TPA is implemented to double-check search engine results for authenticity, and then the user does his own hash function checks on the secret cryptography and decryption to ensure their own data is undamaged. Outsourced decryption is also utilized to lessen the burden of computation brought on by ABE. Furthermore, data labels are employed to check the reproducibility of the submitted data with both the information in the cloud, in order to accomplish the cloud data minimization. This helps to decrease the multiplicity of information on the public cloud and the connection traffic consumption of users.

An ABMKS created by Yuanbo Cui [8] that uses just multiplication computations to generate encrypted keyword indices, allowing for safe multi-keyword searches with granular permissions. Index creation uses simply multiplication, which is a more efficient calculation procedure than arithmetic operations and pairing, since it requires fewer operations. Furthermore, regardless of how many keywords are hidden in a given file, the classified keyword indices are merged into a single data point. This approach has been shown to be secure by formal analysis. The study of performance shows that compared to existing works, the ABMKS-WM system has lower computational and network latency.

An effective ranked search strategy for encrypted cloud data was suggested by Lianggui Liu [9]. In order to decrease the dimensionality of encryption keys, they use a classification system to organize the documents and generate group vectors for each index, which is different from other encrypted search techniques. There is a net savings in terms of the amount of time required to generate the index. Moreover, the creation of grouped vectors within every entry makes it simpler for users to refresh their information. Users should simply rebuild the group vectors that correlate to the modified sets of category keywords when adding, modifying, or removing documents. Additionally, we recommend a focused search technique for use in the CGIM extraction of features. By using this technique, the cloud server may improve search performance and efficiency by just calculating the products of a subset of the group vectors that match to query terms in the dictionary and then each index, rather than of the entire combinations of those vectors.

To find every instance where the query text matches the gene sequences, Shiyue Qin [10] suggested a private information substring searching strategy for multi-source gene information in cloud technology. The system allows for several users to be set up at once while maintaining tight security. Authorized inquiries may use query strings of varying lengths to carry out the substring scan. Depending on the complex mathematical issue, this technique is safe and can preserve the confidentiality of both the genetic sequence information and the queries. In addition, researchers reach the optimum number of engagement sessions and communicative sophistication. This method's efficiency is sufficient for use in practical medical research settings.

Using extensive study, Huanglin Shen [11] proposes a safe and effective search technique for doing multi-keyword ranked searches over encrypted cloud data. In addition to the method provide precise multi-keyword ranked searching, but it can also reduce search time to a higher than logarithmic. Vector space modelling and term frequency-inverse document frequency (TF-IDF) modelling are used to efficiently get precise rankings in search

results. The technique is protected from two different types of threats by combining the secure kNN computation. Each page is indexed using a BC-tree framework, and a cluster of comparable documents is built for each one preceding encryption to boost search performance.

According to Hua Dai [12], even if we assume that the search queries would return accurate results, it remains difficult to guarantee the effectiveness of the query. In addition, the majority of the current solutions for multi-keyword prioritized searching over cipher text are only available in the public cloud. In this work, we present MRSE-HC, an authenticated Multi-Keyword Ranking Searching for use in hybrid clouds that protects user privacy. Based on a bisecting k-means segmentation, this method utilizes a keyword partition technique to evenly split an article's keyword vocabulary.

A new feature identifying prioritized search strategy for secure cloud data is suggested by Lianggui Liu [13]. Using a feature score technique, indexes are constructed in such a way that each of a document's retrieved keywords is only associated with a single dimensional of the ranking. This approach may lower the index dimension in comparison to constructing indexes with separate keywords. Additionally, FMRSM's trapdoor generator includes a custom-made matching score algorithm. The system may provide a score to the query depending on the kind of similarity as well as the amount of matching terms, making search results more relevant to users' intentions.

3. PROPOSED METHODOLOGY

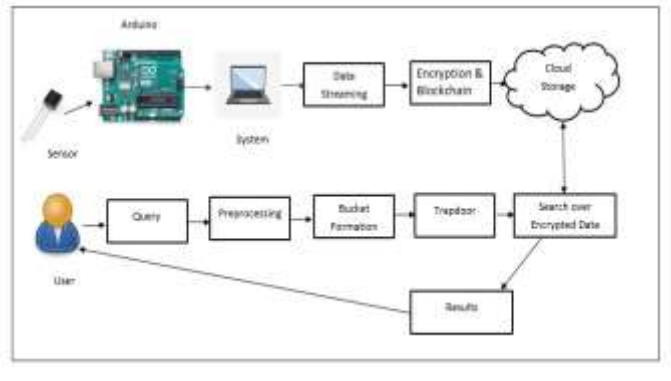

Figure 1: Proposed Methodology

The proposed approach for enabling search over the medical IoT data on the cloud platform through the use of Blockchain has been depicted in the figure 1 above and the steps taken to achieve this system are elaborated below.

Step 1: User Registration and System Initialization – The suggested system was created using Java as its programming language and the Swings platform. The user registers using the Interactive Interface by entering accurate information including name, sex, email address, cell number, user ID, and passcode. The user is able to log into the the software by entering the username and password that they chose when registering after proper verification and authentication.

When a user first logs into the system, they are met with an operation window that looks like a menu and offers them a number of choices. Edit, storage of data, preferences, and logout are some of these choices. By means of the edit choice, the user may modify the details of their registration-generated profile. The data streaming alternative enables the initial configuration of the information streaming generated by the sensors, and the view previous option displays the data gathered for a specific date. These are two submenus under the data storage selection. After the user starts streaming, the technique's next stage demonstrates how to gather information from sensors.

Step 2: Sensor Data Collection – The procedure is initiated by connecting the Arduino UNO microcontroller to the development system. The utilization of the Arduino UNO device is currently being implemented to facilitate the

integration of sensors and the collection of their respective data. The present setup employs a range of sensors, encompassing ultrasonic, skin warmth, pulse rate, and temperature measurement sensors. The aforementioned sensors are connected to a microcontroller board, which is subsequently programmed to gather and transmit sensor data to a laptop. Figure 2 depicts the electrical connections between the sensor and the Arduino UNO embedded system.

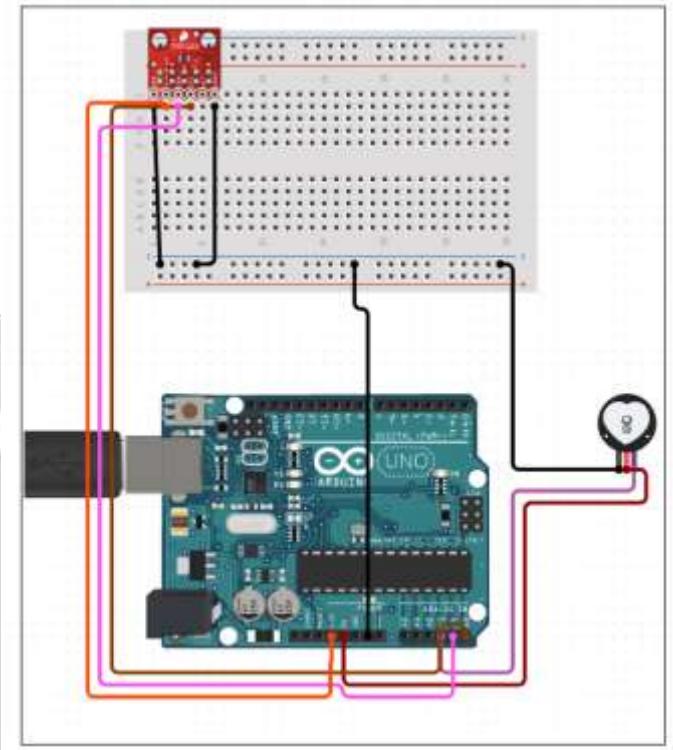

Figure 2: Circuit Diagram

The code written in Java is initiated to collect sensor data through the microcontroller. A graphical user interface with a high level of intuitiveness has been developed to facilitate the activation of the sensor data collection mechanism for this purpose. Upon activation, a thread is initiated to oversee the transmission of readings from sensors through the COM27 port. The aforementioned process involves the accumulation of sensory data from various sources, namely the ultrasonic, temperature of the skin, pulse, and general temperature sensors. This information is subsequently recorded in the database, along with the present time and date. To the extent as the sensor is collecting the values this process remains ongoing, it will persist indefinitely. The cessation of sensor data collection can be achieved through the user interface by activating the stop switch, which promptly halts the thread's execution.

Step 3: Sensor Data Encryption and Cloud Storage – The information received from the sensors during the previous phase is utilized as an input within this point in the process, consisting of time and date information that is to be subjected to encryption. The utilization of the RCC (Reverse Circle Cipher) Encryption procedure and the generation of encryption keys are implemented for this purpose.

A symmetric key that is predefined has been supplied for a particular objective of encryption. The aforementioned key is utilized in the RCC methodology to generate the requisite keys that subsequently serve the purpose of anonymizing the sensor data.

Reverse Circle Cipher – The Reverse Circle Cipher is an exemplar of an exceptionally successful encryption method that has the potential to be utilized on a cloud-based infrastructure. The methodology of RCC operates through the systematic rotation of input characters in either a clockwise or anti-clockwise orientation,

subsequently resulting in the replacement of characters. The proposed methodology involves partitioning the sensor observations into distinct clusters and performing rotations on each cluster to encode relevant details. The Reverse Circle Cipher is an effective cryptographic technique that ensures secure transmission of cryptographic data to the cloud. The Reverse Circle Cipher is considered to be a highly important and cost-effective encryption technique that serves to safeguard the private nature of data. Algorithm 1 outlines the complete procedure for implementing Reverse Circle Cipher Encryption.

ALGORITHM 1: Reverse Circle Cipher

```
// Input: Sensor Data S_DATA
// Output: Sensor Cipher Data S_CDATA
Function reverseCircleCipher (S_DATA, KEY)
1:  Start
2:  Initialize list Block LST_BLK =∅, DIV_STR="", addupval=0
3:          for i = 0 to size of KEY
4:                  addupval= addupval+ASCII (KEY_[i])
5:      end for

6:          addupval= addupval MOD 20

7:          for i = 0 to size of S_DATA
8:                  char c= S_DATA [i]
9:                  D_STR = D_STR +c
10:             if (D_STR size =10), then
11:                 LST_BLK = LST_BLK + D_STR
12:                 D_STR =""
13:             end if
14:     end for

15:                 LST_BLK = LST_BLK + D_STR
16:

17:         For i = 0 to size of LST_BLK

18:             STR= LST_BLK [i]

19:             STR=rotate (STR, i)

20:                 For j = 0 to size of STR

21:                     char ch= STR [j]

22:                     newchar=ASCII(ch) + addupval

23:                     S_CDATA = S_CDATA +newchar

24:                 end for
25:         end for
26: return S_CDATA
27: STOP
```

Upon encryption, the information is subsequently transferred to the Amazon cloud service via integration with AWS (Amazon Web Services). The user can accomplish this task by opting for establishing a table in the database created by the MySQL instance upon the Amazon cloud through the "build table in cloud" feature. The aforementioned table is subsequently filled with secured sensor measurements, which are accessible by using the "view history" option located within the data storage menu options. The information can be accessed for a specific date, and subsequently deciphered and presented to the user following the prescribed procedures.

Step 5: Searching secure sensor data on cloud – The first step in facilitating the search process involves maximizing the potential of a trap door. A Trapdoor refers to a collection of encrypted queries that are utilized for the purpose of searching secured entities, for instance information from sensors that has been offloaded onto a cloud database. The potential trapdoor in this methodology pertains to the specific date on which the sensor data was gathered.

The aforementioned date is safely maintained in an encrypted format within the cloud-based database. The user's preferred date for accessing sensor information is initially encrypted, serving as a searchable trapdoor, and subsequently matched against the encrypted values stored in a cloud-based database. Upon successful matching of the secured trapdoor with the corresponding database entries for the given date, the associated data can be obtained and subsequently decrypted for the purpose of user presentation.

The trap door has been designed to facilitate searching operations on cloud-based systems. This is because the encrypted date provided is analogous to the date utilized for storing sensor information on the database stored in the cloud. Enhancing the precision of the search module leads to the generation of thorough and efficient search outcomes that cater to the particular inquiry.

4. RESULT AND DISCUSSIONS

The technique proposed for facilitating search functionality on secured sensor data stored on public cloud infrastructure has been established utilizing the programming language Java and the NetBeans IDE (Integrated Development Environment). The device utilized for the implementation of this strategy operates on the operating system Microsoft Windows and is equipped with an Intel Core i5 Processor, 8 GB of RAM, and a total of 1 TB of internal storage capacity. The utilization of the Arduino UNO microcontroller is facilitating the interfacing of diverse sensors along with their corresponding measurements. The cloud-based database is utilized for the storage of sensor values through the Amazon Web Services.

The feasibility of the suggested methodology has been meticulously assessed across a broad spectrum of variables. The results of the experimental inquiry have been outlined as follows.

4.1 Encryption and Decryption Time performance

The proposed methodology utilizes both decryption and encryption procedures to ensure sufficient anonymity of the data collected by the sensors being transmitted to the cloud database. The evaluation of the efficacy of this approach necessitates the implementation of the approach that is clarified hereafter. Table 1 illustrates the duration of the procedures for decryption and encryption as a function of the number of characters employed.

Number of Characters	Encryption Time in Milliseconds	Decryption Time in Milliseconds
15	3	3
1808	15	17
2808	33	32
3012	46	54
5003	52	56
5789	64	62
6342	67	64
8426	77	78
9210	82	81
9991	96	99

Table 1 : Encryption and Decryption time performance

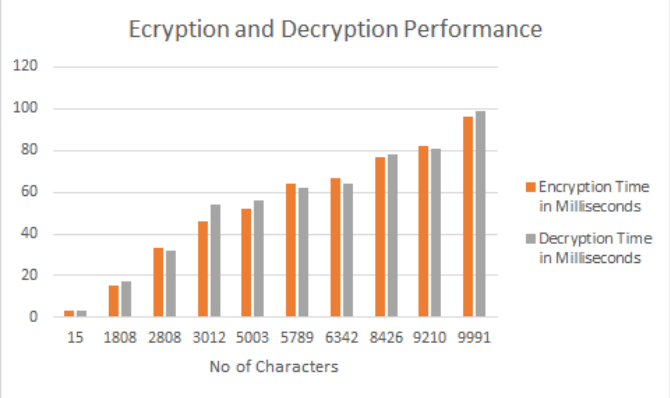

Figure 3: Encryption and Decryption Time

The results presented in the aforementioned bar graph, depicted in Figure 3, had been suitably obtained for the purpose of visual examination. It is evident that the duration required for encryption and decryption is not directly proportional to the quantity of input digits. The reason behind this phenomenon is attributed to the meticulous examination and implementation of the cryptographic technique employed in this approach, namely the reverse circle cipher. The effectiveness of this approach is supported by the performance metrics that have achieved a highly satisfactory conclusion in this section.

5. CONCLUSION AND FUTURE SCOPE

The proposed approach for enabling search over the medical IoT data on the cloud platform through the use of Blockchain has been elaborated in this research article. The approach initiates with the medical sensors being connected to the Arduino Uno microcontroller. This Arduino Uno microcontroller is then connected to the system that collects the data from these sensors and streams it to the proposed approach. The approach effectively encrypts the data and then converts it into a blockchain. This encrypted blockchain is then stored on the public cloud storage. The user then accesses the system and wishes to search the uploaded medical IoT data on the cloud. For this purpose the user then passes a query to the system that is first preprocessed to remove the redundant text and the passed to the nest step for bucket formation. The bucket formation process then transforms to the trapdoor creation that is then utilized to perform search over the encrypted data. The search results are then provided to the user. The approach has been quantified through the utilization of effective experimentations that has resulted in highly lucrative outcomes.

For the future scope the proposed model can be deploy in the real time hospital scenario to store the proper data of the each patients.

6. REFERENCES

[1] X. Gao, J. Yu, Y. Chang, H. Wang and J. Fan, "Checking Only When It Is Necessary: Enabling Integrity Auditing Based on the Keyword With Sensitive Information Privacy for Encrypted Cloud Data," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 6, pp. 3774-3789, 1 Nov.-Dec. 2022, doi: 10.1109/TDSC.2021.3106780.

[2] S. Abdelfattah et al., "Efficient Search Over Encrypted Medical Data With Known-Plaintext/Background Models and Unlinkability," in IEEE Access, vol. 9, pp. 151129-151141, 2021, doi: 10.1109/ACCESS.2021.3126200.

[3] H. Kwon and C. Hahn, "Asymptotically Optimal and Secure Multiwriter/Multireader Similarity Search," in IEEE Access, vol. 10, pp. 101957-101971, 2022, doi: 10.1109/ACCESS.2022.3208962.

[4] B. Wu et al., "Privacy-Protection Path Finding Supporting the Ranked Order on Encrypted Graph in Big Data Environment," in IEEE Access, vol. 8, pp. 214596-214604, 2020, doi: 10.1109/ACCESS.2020.3040781.

[5] L. Tao, H. Xu, Y. Shu and Z. Tie, "An Efficient Search Method Using Features to Match Joint Keywords on Encrypted Cloud Data," in IEEE Access, vol. 10, pp. 42836-42843, 2022, doi: 10.1109/ACCESS.2022.3168730.

[6] G. Liu, G. Yang, S. Bai, Q. Zhou and H. Dai, "FSSE: An Effective Fuzzy Semantic Searchable Encryption Scheme Over Encrypted Cloud Data," in IEEE Access, vol. 8, pp. 71893-71906, 2020, doi: 10.1109/ACCESS.2020.2966367.

[7] X. Liu, T. Lu, X. He, X. Yang and S. Niu, "Verifiable Attribute-Based Keyword Search Over Encrypted Cloud Data Supporting Data Deduplication," in IEEE Access, vol. 8, pp. 52062-52074, 2020, doi: 10.1109/ACCESS.2020.2980627.

[8] Y. Cui, F. Gao, Y. Shi, W. Yin, E. Panaousis and K. Liang, "An Efficient Attribute-Based Multi-Keyword Search Scheme in Encrypted Keyword Generation," in IEEE Access, vol. 8, pp. 99024-99036, 2020, doi: 10.1109/ACCESS.2020.2996940.

[9] L. Liu and Q. Chen, "A Novel Category Group Index Mechanism for Efficient Ranked Search of Encrypted Cloud Data," in IEEE Access, vol. 8, pp. 54601-54610, 2020, doi: 10.1109/ACCESS.2020.2977430.

[10] S. Qin, F. Zhou, Z. Zhang and Z. Xu, "Privacy-Preserving Substring Search on Multi-Source Encrypted Gene Data," in IEEE Access, vol. 8, pp. 50472-50484, 2020, doi: 10.1109/ACCESS.2020.2980375.

[11] H. Shen, L. Xue, H. Wang, L. Zhang and J. Zhang, "B+-Tree Based Multi-Keyword Ranked Similarity Search Scheme Over Encrypted Cloud Data," in IEEE Access, vol. 9, pp. 150865-150877, 2021, doi: 10.1109/ACCESS.2021.3125729.

[12] H. Dai, Y. Ji, G. Yang, H. Huang and X. Yi, "A Privacy-Preserving Multi-Keyword Ranked Search Over Encrypted Data in Hybrid Clouds," in IEEE Access, vol. 8, pp. 4895-4907, 2020, doi: 10.1109/ACCESS.2019.2963096.

[13] L. Liu and Q. Chen, "A Novel Feature Matching Ranked Search Mechanism Over Encrypted Cloud Data," in IEEE Access, vol. 8, pp. 114057-114065, 2020, doi: 10.1109/ACCESS.2020.3002236.