FMDB *Transactions on Sustainable Computing Systems*

Transforming Medical Education: Multi-Keyword Ranked Search in Cloud Environment

Ritcha Saxena[1, *], Vikas Sharma[2], Ritwik Raj Saxena[3]

[1]Department of Biomedical Sciences, University of Minnesota School of Medicine, Duluth, Minnesota, USA.
[2]Department of Computer Science, Delhi Technological University, Delhi, India.
[3]Department of Computer Science, University of Minnesota, Duluth, USA.
rsaxena@d.umn.edu[1], vikassharma12387@gmail.com[2], saxen130@d.umn.edu[3]

Abstract: In the rapidly evolving medical education landscape, technology integration is synonymous with progress, and cloud computing emerges as a transformative force. This article discusses how cloud computing has transformed medical education for aspiring healthcare professionals. As we enter the digital age, cloud technology and medical education must work together to ensure connectivity, accessibility, and preparation for current healthcare concerns. The partnership between cloud computing and medical education shows how technology may mould the future generation of healthcare workers. As cloud storage becomes simpler and more capable, conventional systems are being replaced, making cloud resources more tempting. Data privacy is vital, so personal data must be encrypted before outsourcing. This requires a paradigm shift from keyword-based data use. To solve this problem, the essay provides an efficient encrypted cloud information search solution. The proposed system supports synonym queries to improve multi-keyword searches, a novel synonym-based search strategy. The report also stresses the necessity of ranked search for more relevant and thorough results. The proposed solution uses ranked searches to enable an effective searchable system, especially for terminology-based multi-keyword questions, unlike existing methods that only help with fuzzy keywords or correct queries over encrypted cloud data. In conclusion, cloud computing has the potential to alter medical education by tackling the difficulties of secure and efficient data retrieval.

Keywords: Transforming Medical Education; Multi-Keyword Ranked; Cloud Environment; Terminology-Based Multi-Keyword Questions; Efficient Encrypted Cloud Information; Conventional Systems; Healthcare Workers.

Received on: 21/02/2023, **Revised on:** 29/05/2023, **Accepted on:** 05/08/2023, **Published on:** 19/12/2023

Cite as: R. Saxena, V. Sharma, and R. Raj Saxena, "Transforming Medical Education: Multi-Keyword Ranked Search in Cloud Environment," *FMDB Transactions on Sustainable Computing Systems*., vol. 1, no. 3, pp. 135–146, 2023.

1. Introduction

In the rapidly advancing landscape of medical education, the integration of technology has become synonymous with progress. Among the transformative technologies making a significant impact, cloud computing stands out as a catalyst for change. This article explores the profound influence of cloud computing on medical education, revolutionizing the way students learn, collaborate, and prepare for the challenges of modern healthcare.

Firstly, cloud computing transcends traditional confines of brick-and-mortar classrooms. With cloud-based platforms, students gain access to a wealth of educational resources, lectures, and collaborative tools from anywhere in the world. This flexibility not only accommodates diverse learning styles but also ensures that geographical boundaries do not limit medical education. Secondly, collaboration lies at the heart of medicine, and cloud computing seamlessly fosters teamwork among students. Virtual collaboration tools [1], shared documents, and real-time communication platforms enable students to engage in collaborative

*Corresponding author.

learning experiences. This collaborative approach mirrors the interdisciplinary nature of healthcare, preparing students for the dynamic and interconnected world of modern medicine. This mirrors the collaborative ethos of healthcare, preparing students for interdisciplinary practice. Moreover, cloud computing grants students unprecedented access to a vast array of educational materials, spanning research articles, journals, and multimedia content. This democratization of information ensures that students, regardless of their location or institutional affiliations, have equal access to the latest advancements in medical knowledge.

In the realm of medical education, hands-on experience is invaluable. Cloud computing also facilitates the creation of virtual laboratories and simulations, allowing students to engage in realistic medical scenarios without the need for physical resources. This not only enhances practical skills but also provides a safe environment for students to learn from mistakes and refine their clinical decision-making abilities. Furthermore, cloud platforms prioritize security and confidentiality. Security and confidentiality are paramount in the healthcare sector, and cloud computing addresses these concerns in the realm of medical education. Cloud platforms incorporate robust security measures, ensuring the safe storage and transmission of sensitive educational materials. Additionally, the accessibility of cloud-based resources ensures that students can securely access learning materials anytime, fostering a continuous and uninterrupted learning experience. Finally, cloud computing supports seamless remote learning—an invaluable asset in times of global crises like the COVID-19 pandemic. It ensures that medical students can continue their education regardless of physical restrictions. This adaptability is crucial in preparing future healthcare professionals to navigate the evolving landscape of healthcare delivery.

At the vanguard of technological advancement, cloud computing cultivates collaboration, enhances resource accessibility, and facilitates remote learning, thereby forging a dynamic and future-proof medical education ecosystem.

Cloud computing is a transformative force in medical education, redefining how aspiring healthcare professionals learn and collaborate. As we embrace the digital era, the partnership between cloud technologies and medical education becomes increasingly essential. The future of medical education promises to be more connected, accessible, and equipped to meet the challenges of a rapidly evolving healthcare landscape with innovative cloud computing. The synergy between cloud computing and medical education is a powerful testament to the potential of technology in shaping the next generation of healthcare professionals.

In order to allow the centralized data repository and access to information services or resources whenever appropriate, the cloud provides a wide group of remote servers in a network. Many IT companies and individuals are exporting their cloud server databases. Different users, regardless of location, can access and exchange information uploaded to the cloud. Outsourced data may contain very confidential information such as e-mails, financial information for companies, government documents, records of personal health care, and pictures of Facebook and business documents [2]-[3].

Cloud service providers (CSPs) can access confidential information from users without authorization. CSPs' general strategy is to maintain the confidentiality of data under which data is encrypted until it is outsourced to cloud storage, and this would affect the tremendous cost of data usability. In order to protect their privacy, data owners subcontracted their data to cloud servers in encrypted form in a secure quest for encrypted data. If a data user wants to search for a specific file, they send a keyword request to the cloud server. The cloud server then creates the most relevant data results for the data user. A safe keyword search over sensitive information not only reduces the cost of computation and storage but also allows for a ranked search for multi-keywords, fuzzy keyword searches, and searches for similarities. Both of these systems are based on a single-ownership model.

Previous work supports the single-owner model where the data owner needs to remain online in order to create data consumer trapdoors. Therefore, this paper suggests a multi-owner model to solve the limitations of earlier approaches, where multiple data owners store encrypted data and data owners remain online to create trapdoors at the same time. In order to encrypt their secret data with different secret keys, various data owners exchange different secret keys.

Safe search protocols are introduced in this paper in which cloud servers can conduct secure searches without knowing the true value of keywords and trapdoors. In this multi-user and multi-owner cloud model, there are 4 private servers involved. Apart from these private servers, there is one monitoring server which collects the index from all the servers and merges them into an integrated main index. There is one Key distribution server, which manages the key generation and distribution process. One service is for data users, which allows them to input the query for search and access the data from the cloud. The cloud server is there to store the data received from the private server. Cloud server also provides the data to the data user upon proper authentication from the private server. Figure 1 shows the architecture of the system consisting of all these entities.

Data owners create a stable, searchable index of the keyword set and extract keywords from files. The data owners submit a keyword index to the management server. Data owners encrypt files and outsource encrypted data to cloud servers. When the administration server sends an encrypted keyword index, the keyword index is re-encrypted by the administration server.

The administration sends the server out to an outside company for re-encryption, which in turn outsources the cloud-stored index. In order to see if any files from the cloud server are open, the data user must first check if any of the appropriate traps have been set, which send data to the administration. After the user has completed their logon process, the system verifies the user's identity and then stores it in the cloud as an encrypted secret key. If the cloud identifies the data owner (for example, the name and encryption key that was associated with the target file), it returns the top-K encrypted files. The data user downloads and decrypts the files from the cloud as a result of getting incredibly large amounts of K data from the server. When a user gets top-N files from a cloud server, they are given N times the amount of data in decrypted files to download, and then they have to decrypt and unpack them.

The data protection access file [4]-[6] and short-term data protection surveys and data exchange in the data organizations. The data protection agreements are applicants' agreements. PPI is a third-party catalogue advantage (e.g. open cloud) that gives users or searchers global knowledge. A requester is involved in a two-part method for seeking stories of plots: firstly, it includes a survey of the related phrases against the PPI server that summarises the applicant owners in the program (e.g. p0 and p1).

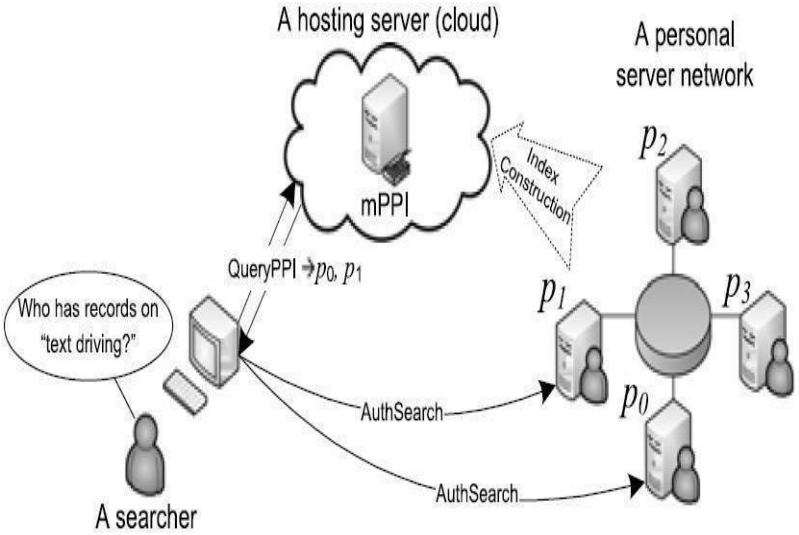

Figure 1: Architecture for Privacy-Preserving Indexing System

The search administrator must then contact the server and customer reviews and permission requests for any positive holders prior to local searches-At rundown. Rundown at detailed breakdown. Rundown. Rundown. It is important to mention that while the dataset has been validated and approved, it hasn't been uploaded to the PPI server. Furthermore, PPI contrasts with current safe information efforts [7]-[9] and is exemplary since 1) the data are straightforwardly placed on a PPI server (i.e. not encrypted), enabling the generation of valid, informed and scalable data. PPI jams consumer privacy by climbing to clouds that could only be used through encryption. 2) Rough-grained data is supplied on the PPI server, while the first private content is left on the servers and handled in accordance with customer laws.

The PPI system must protect various search queries and owners separately. The information indicates that each server has a different data structure and data system with different words. Personal and confidential information should be protected under a PI if each party who may have possession of it has more than one record of having substantial ownership. This strategy has significance in several ways, firstly in the fact that it conceals the identity of all parties in private transactions, and secondly, it also hides the identity of individuals using the service.

There are no words in such (single sentences) that could be expanded. To take the point, for example, with an e-Health organization, the experience of a treatment associated with "preterm delivery" (e., undocumented instances of induction or even of difficult childbirth) is seen in an example) A language used to refer to a larger or smaller individual is more (or less) vulnerable than a word or phrase acting on its own. The respective appearances of content and motion are two things: "solo", for instance, and "cont." Motion and content can both be contained, for instance and "cont." can be perceived as being motion itself. When people are motivated by interest, they are less likely to form positions on divisive issues.

Presenting the idea [6], [9] provides expanded concepts about privacy concepts [expands ideas] it could use that to enable it to balance privacy and retention better. Data security measures of this good nature are too good to use just once or for a short period, so it is almost impossible to use these programs that offer to say something quantitatively that they won't break.

It's proposed that pi-MPPI, another PPI debate, regulates the spillage of data protection for a multi-watchword record look. This μ-MPPI framework paper describes the distinctive terms; value 0 is moderate in privacy security, while value 1 provides

absolute privacy protection (including overhead for further enquiries). In other words, a multi-stage μ-MPPI aggressor can only guarantee that successful attacks have been conducted according to the label's privacy.

It attempts to calculate the μ-MPPI in the data system's measuring points and frame contours. Č-development MPPIs requires a cautious plan to legally shield false-positive people (i.e. any owner who's going to claim falsely to be without word and conspiracy) in order to maintain their privacy by protecting a genuinely positive owner from false-positive people.

Contextually, a stable β-MPPI needs to be generated without exchanges in a true knowledge organization of experts requiring mutual trust between self-regulatory operating servers. If a secure output spread is assigned, it is highly testable. In order to comply with the most stringent data protection standards in various multi-specific looks, μ-MPPI can basically be constructed as an improvement issue in order to fix complex calculations.

In this paper, a multi-party system (MPC) is used [10]-[12] to maintain data protection and safeguard basic intelligence; existing MPCs are able to run virtually well in a restricted environment with a simple workload. For instance, FairplayMP is an effective MPC agent: it demands approximately 10 seconds to assess capacity [13], which is normally possible in milliseconds for reasonable non-safe calculations. Therefore, MPC procedures will lead to completely unbelievable and unsatisfactory costs if they are specifically applied to the β-MPPI problem with skewed calculations and a wide range of servers. Our main goal is to align the secure and unsafe parts of the calculation to address the challenges of accurate and stable μ- PPI development. However, as predicted, we restrict the safe calculation portion by evaluating various techniques.

In this context, perplexing MPC NLP measurement has been effectively isolated to the extent. Its design convention μ-MPPI needs only a simple method of computing that enables the system to be implemented globally. The reference can be translated from this paper as follows.

In order to address various needs, notably distinct privacy security concerns, we have created multi-term PPI. There is no question that financial planning is among the most significant topics of retirement planning. A model PI is instructed to look for non-existent pixels and control another to make sure that no infringement occurs simultaneously, guaranteeing privacy is protected quantitatively.

For the network of widely untrusted servers, we have also proposed a set of MPPI software agreements. In particular, when exploring how many security responsibilities could be reshaped without abandoning the nature of privacy protection, Single and multi-term, enhancing the safety of the MPPI in line with both the measurement model and the device configuration.

We followed a working model of the MPPI, in which a test study reaffirms that our convention is a beneficial place for list construction.

2. Literature Review

The new knowledge networks [5] have an economic search for the documents distributed. PPIs maintain data security tables or indexes for the owner's privacy. This topic is understood given the existence of multiple-key emerging information networks [6] and the security of privacy. Data-protection indexes or PPIs protect the owner's privacy. The known issue is the security of privacy when using PPI. Circumstances and phrases give them an inherited meaning. The author introduces the first e-PPI work for the quantitatively differentiated search for distributed records and the protection of their privacy.

A stable, fuzzy, multi-keyword search for encrypted cloud information was suggested in [14]. This scheme allows the search parameter for multiple keywords and gives the related results. Coordination is used to calculate similarity on the basis of safe internal measurement of the product.

In [15], the author proposed a new method of attack and a strategy to resolve the identity-shattering issues associated with PPIs by implementing an extended PPI. Without any trusted third party and/or trusted relationships between providers, the proposed e-PPI construction protocol is initiated. Through the use of a generic MPC technology, the PPI construction protocol is introduced, which secures multi-part computing and enhances performance to a realistic level by minimizing the costly MPC component.

The Low Weight Hash Tree is a low-maintenance query-efficient indexing technique, according to this research [16]. A new naming system and description technique are used in tree form for the layout of the index. LIGHT has been developed with nearly optimal performance over a generic DHT system that supports numerous complex questions.

Using ABE, Persona masks user information and sends users fine-grained policies to see their information. The data is hidden in the paper [17]. It provides effective applications where, by using a given privacy policy, users are not the OSN. This new cryptographic mechanism improves the general application of ABE. It describes an application that reproduces Facebook applications and provides appropriate results even on mobile devices when browsing privacy-enhanced web pages, contrasting

both current and new and illustrating how Persona provides additional privacy benefits to the features of existing online social networks.

This paper [18] illustrates that both hospitals and patients can use the device to exchange medical information with a third-party server. When accessing records from anywhere via a shared device, this is beneficial. The mutual protection of the system is important. When medical records are encrypted with symmetrical encryption, authentication is applied, also known as private-key encryption; a sender sends encrypted data, and the recipient uses this form of encryption to decrypt the data.

A new data security index abstraction, SS-PPI, is proposed in [4] by the author, which provides theoretically guaranteed protection of confidentiality in combination with distributed access managed search protocols. In contrast with current plans, our approach highlights a variety of distinctive characteristics (for example, index flipping protection for data [14]). (a) Includes access control measures that improve both search effectiveness and attack resistance in the Privacy Security Index; and (b) utilizes the Rapid Index Construct Protocol in a fully distributed way through the modern use of secret sharing. We implement two methods, formal and SS-PPI analysis, and demonstrate the latest privacy security and execution efficiency solutions that are available.

In a place such confidence in [by making a proposal which involves eliminating the need for this kind of authority], in a hierarchical, multi-user control system, the approach maintains a centralized index of privacy preservation in line with the distributed access protocol. As the index has been made public, there are absolute protections for privacy in this new index. To begin with, there is a twofold allure of a solution:

We expect the service suppliers to monitor and ensure conformity with the ways groups are maintained in identifying and controlling who has access to the content. In order to compensate for their privacy and effectiveness issues, device developers minimize controls that can be manipulated. No feature in this block is transmitted, but the machine compiles it into a circuit specification [6] that is not revealed in any other blocks when calculating the Boolean result. Players are cooperating with Fairplay, which encourages two competing entities to make efficient use of resources and provide positive outcomes. Beaver's underlying FairplayMP protocol (and that's how they're usually described) is a constant number of touch counts (although, as can be noted, they're usually referred to as FairplayMP) (8 rounds in our implementation). As an ongoing collaboration project to modernize the BMR by means of meeting Ben-own Or's criteria, it has added new elements and made substantial improvements to the existing methods. We ought to use this approach, as it is well acknowledged that the number of rounds applied in the process is crucial to the protocol's ultimate success [19].

In order to conduct job assignments while protecting them from the eyes of others, smaller organizations frequently need to exchange documents with one another. In this case, users need a document indexing facility that allows them to access documents easily (1) without exposing other document information, (2) as users, groups and documentation change, and (3) without the need for users to settle on a single and fully trusted authority. In [5], the author proposes a concept of privacy that measures how much data is leaking from the index in relation to something like the conditions contained in the inaccessible content. In addition, the system provides re-confidential indexing facilities with sensitive materials that use secret divisions and term mergers to set tenable limits for the leakage of information, even in the event of statistical attacks.

The need for a confidential authority is removed in this document [6]. With a distributed search compliance access control protocol, the paper offers a solution through the development of a centralized PPI. This PPI, even when the index is written, guarantees strict confidentiality. This device has been tested in real-life experiments. The solution has two steps: firstly, service providers maintain full control when identifying access classes, and secondly, system implementers have control over the security and efficiency of their particular areas or document searches with PPI applications [20]. Circumstances and phrases give them an inherited meaning. The author introduces the first e-PPI work for the quantitatively differentiated search for distributed records and the protection of their privacy.

This pursuit was suggested in [21] with symmetrical searchable encryption (SSE). They form a fluffy watchword collection of data with the help of distance of transition. He scans for Tw when the customer looks at CS and returns scratch-coordinating Tw papers. By using a special case and a fluffy Multiway Tree searchable list that uses an image-based trial to navigate search, they compile the suitable fluffy phrase identified.

3. Modules and Methodology

An open cloud server, several specialized servers, and several clients are included in the architecture. The owners' records Is shared on the private servers. Information is scratched throughout the construction. AES Calculation is used for data encryption. Each private server has registered its information file. Observation is based on gathering and using all relevant material. this merged file from the free cloud must be deleted. A customer could place an order on the same day the order was sent or an "as-needed" order record in the cloud data warehouse.

On the contrary, however, the clear cloud records the phase of observation as a single log. Query-related data is now available on this latest consolidation list for customers with a private server. In order to obtain access to all information on the server, the client must request an acceptable inspection with the headquarters and the watchword at this stage (Figure 2).

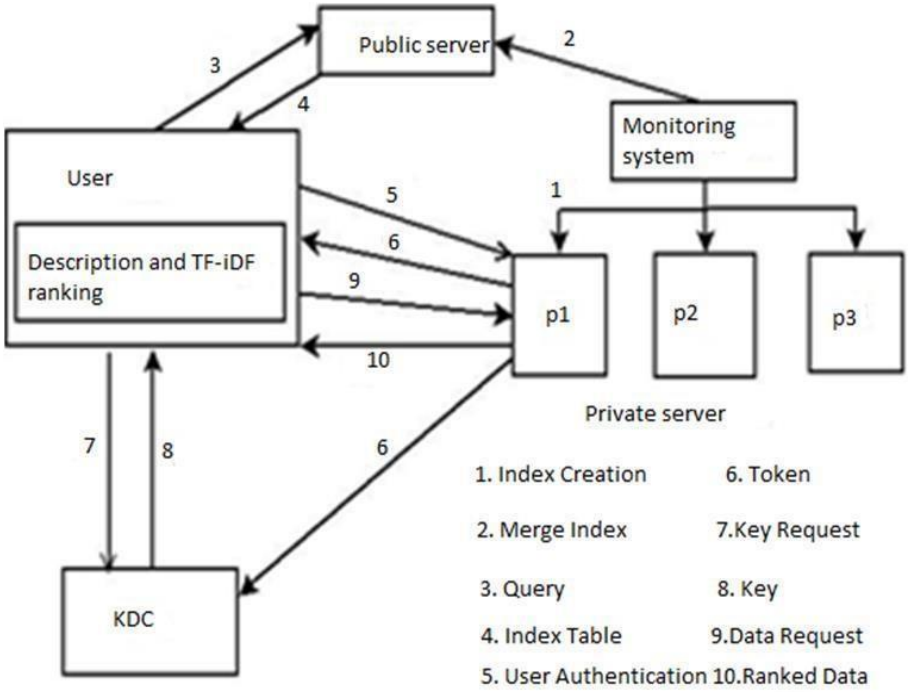

Figure 2: System Architecture

A private server is checking this subtle object inventory in their database. After validating the current capacity, the personal server delivers the token to the Key Distribution Center (Key Distribution Center). When customers order keys, it should be done such that an update is applied. As KDC determines that this token is a private key from a public key, the search returns true. Once the KDC [Kerberosdale Database Server] has issued the customer an authentication key, it will expand the user's secret key. The customer has sent the request to a private server that holds all of the scrambled documents in place and then compresses them into one stream. In theory, using the main consumer confuses the details; however, it is questionable whether it's a method that can yield an adequate result. In the end, to obtain the effects of your positioning setup, use the TF-IDF positioning equation. The system consists of the following modules:

Deployment of System: AES Client-Side Interface Encryption and Decryption Register and log in to the link programming and data exchange database, client, and server.

Creation algorithm for MPPI Index: When the MPPI formula is used to collect a list of all personal servers, you've created a global infrastructure. Since there is no way to make this list more complete and no risk of keeping user data confidential, the full list requires a review of all their data.

Uploading the combined index over the Public Server: When the control system has finished assigning each server a private cloud with the consolidated version of the latest update file, it is the responsibility of that private cloud to pass the whole file to the rest of the others.

Receiving response based on input query From Public Server: This is a cloud service request which can handle only one single piece of data, a cloud file that was created on the private server for use on only this user.

Token Generation and Authentication of Client: In order to access the private server after which the data has been obtained, the client must establish a connection to retrieve the data. Suppose the user's identity has been authenticated. In that case, the client makes a connection to the server and distributes tokens to designated Key Distribution Center (KDC) nodes, and the Key Distribution Service starts.

Distribution of Keys and Decrypting File: KDC does the work for the client, whoops, handing it the private servers' values in the form of tokens so that they can be decoded.

Ranking Results based on TF-IDF: Following confirmation, the customer receives private server scrambling reports. These shattered performances are then unbundled using the KDC key that was obtained. Finally, by using TF IDF, the positioning is created.

4. Mathematical Formulation

Consider the System be represented by S. S= {Ω, P, O}

where,

- Input Ω: The system takes a multi-keyword Query as an input
- Output (O): Ranking.
- Process (P)

Publication of single-term index

$$\in_j = \frac{(1-\sigma j).\ \beta j(tj)(1-\sigma j).}{\beta j + \sigma j}$$

$$\beta_j = [(\sigma_j^{-1} - 1)(\epsilon_j^{-1} - 1)]^{-1}$$

Where βj stands for all the possible values which are derived from source analysis.

Rate of False Positive: FP (0; 1) = F (0; 1)

$$FP(0,1) = \frac{F(0,1)}{F(0,1) + \sigma_0\ \sigma_1}$$

The most pertinent probability of an owner who is non-positive but publishes the details as a positive owner is β0; β1 When FP (0,1) is the false positive value.

Index Production

Ω = {Ω1, Ω2... Ωn}

Where Ω represents the set of indexes collected from all the server

Merging the index of all the Private Servers and uploading.

M = {M1, M2... Mn}

Where M is the collection of all the merge indices that the monitoring system has obtained.

User Query to the public server

θ= {θ1, θ2... θn}

Where θ represents the set of cloud queries from the public server.

Authentication of User at private server

μ= {μ1, μ2... μn}

U here refers to authenticated users on a private server.

Distribution and Generation of Tokens

δ= {δ1, δ2... δn}

Where δ is the collection of tokens for authenticated users created by a private server.

KDC for Key Generation

K= {K1, K2... Kn}

Where K is the set of KDC keys used for user-side decryption of data.

Data decryption and TF IDF ranking

Φ= {Φ1, Φ2... Φn}

Where Φ is the collection of all outcomes for the particular input query.

5. Algorithms

AES Algorithm: The AES is a two-encrypted substitution cypher of 128 bits. Separate 3 Expansion three AES keys in either with 128, 192-bit, or 256-bit lengths. In addition to using square keys, a specific configuration, called round keys, is employed by the encryption method. AES is more of an iterative process as opposed to a stream cipher like Feistel. Increasing the number of keys by 12 bits requires 16 additional pieces and expanding the number of pieces by 24 bits uses 18 additional key positions. In general, only 128-bit components are used in computer memory expansions. On each turn, each player can trade one or more bytes and add one-line commentary and one new character/characters of one or more lines, as well as make an addition and removal. These four measures are handled differently depending on whether the size needs to be expanded or reduced. The encryption and decryption contain the following steps:

Steps for Encryption:

- Substitution of Bytes
- Shift rows
- Mix Columns
- Add round key

Steps for Decryption:

- Add round key
- Mix columns
- Shift rows
- Byte substitution

TF-IDF: This method is used to calculate how central a word is to a collection of text by figuring out how many times it appears in a certain type frequency section. Expansion: TF-IDF refers to the number of words and occurrences of each one of those words in the document but getting information about the documents that exhibit TF is very closely correlated with these is nearly the same as discovering words in context. Because every document is different in length, there are far more words in documents that appear far longer than those that appear in short ones.

$$tf(t,d) = \frac{f_d(t)}{\max f_d(w)}$$

After the calculation of the TF values for all terms is chosen, the index is extended with the 5 highest scoring terms, which produces the top 5 terms in the index. For index creation and table construction, a table is needed to both build a table and add the keyword(s). As will be "filename" and the size of the index "keyword" as a metadata field, so the table will contain when it is formed. This table is sent to the reporting server for further processing and then sent to the final results server.

$$idf(t,D) = In\left(\frac{|D|}{|\{d \in D: t \in d\}|}\right)$$

IDF: Frequency of the inverse text, measuring the importance of a term. During TF computing, all words are considered equally essential. However, it is understood that such terms, such as 'is' and 'of' and 'that,' may often occur but are of little value. Therefore, by measuring the following, we can measure down the periodic terms while analyzing the uncommon ones:

Iterative-Publish (Owner Pi, set β0 (rk))

for all k ϵ [0; l -1] do β' (rk) is topologically sorted if match (cur-mem_{vec}, getStartingState(rk))

then β_{cur}<mem_{vec}

where the current membership vector cur-mem_{vec} publish (cur-mem_{vec}, β' (rk)) ends if

end for

We advocate for using the Iβ method to merge phrases to provide a wider range of probabilities in our production. The Index Method Shows how iteratively, sentence by sentence, page by page, the indexing method functions.

6. Results

In the proposed method, a two-way encryption model is applied for data queries so the data remains complete and undistributed. With the help of two-way encryption, it would protect user privacy. When we are measuring time, we have to consider some additional things such as (a) file upload time, (b) search time, (c) time of encryption, (d) and the time to generate tokens (Figure 3).

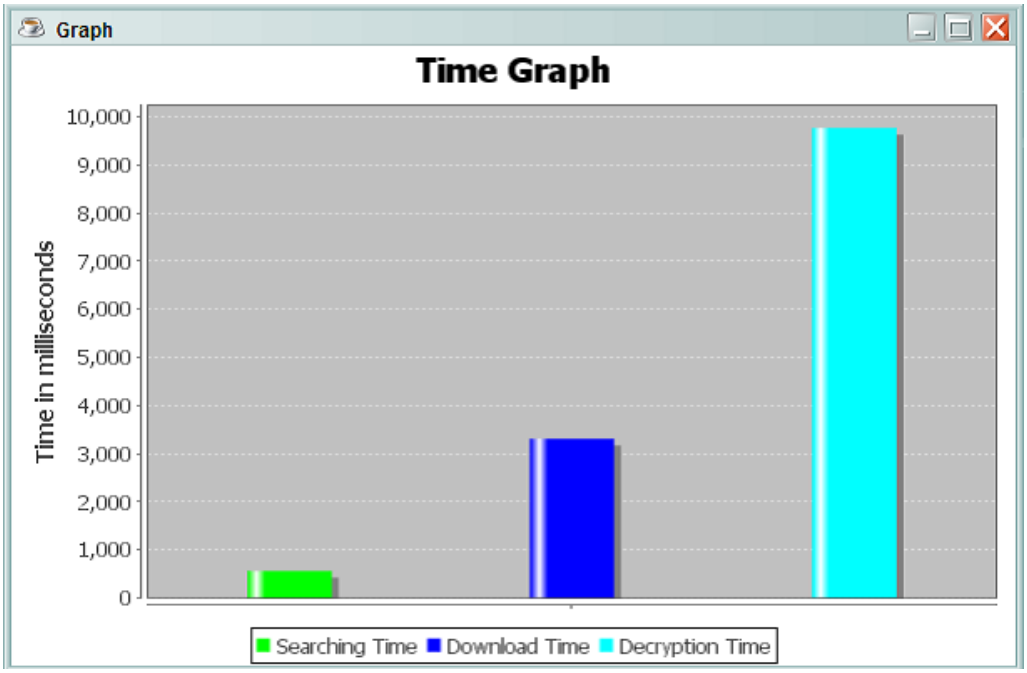

Figure 3: Time Graph at User Side

Similarity Measurement: There are two different systems demonstrated in this table 1: the first column shows the existing and the second, shows the proposed, which can be created with the help of similarity indexes. This model implemented four iterations successfully, and every iteration gave a different result, which was greater than the previous one.

Table 1: Similarity

	Existing	**Proposed**
D1	0.47	0.93
D2	0.78	0.95
D3	0.38	0.98
D4	0.47	0.97

Now, the proposed method can be easily analyzed, which gives a better degree of similarity as compared to the reference system (Graph) for 4 texts in Figure 4.

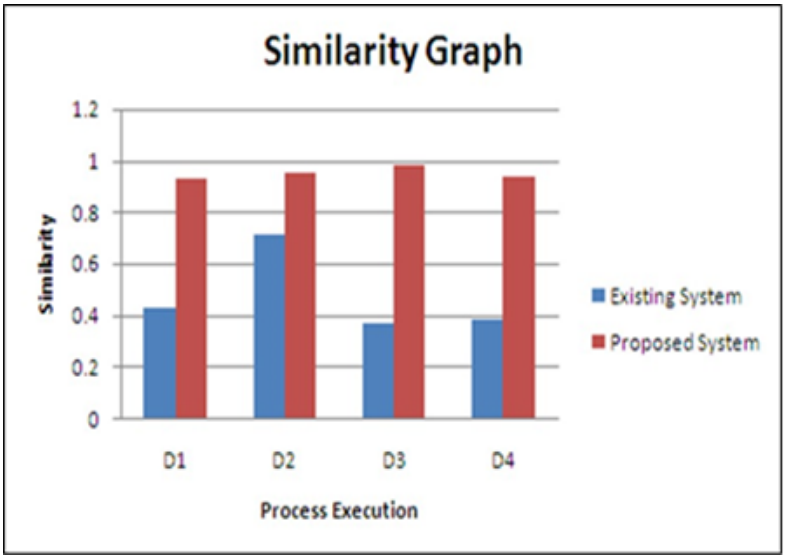

Figure 4: Time Graph for Process Execution

Time Measurement: It can be seen that each operation generally takes the same amount of time if you extend the chart to show time vs different activities like uploading, indexing, querying, and token generation. Work on the project twice, gather your data and plot your findings (Table 2).

Table 2: Time Measurement

	File Upload	SearchQuery	Time for Encryption	Time for Token Generation	Ranking
D1	3.08	0.92	3.40	0.37	0.88
D2	5.84	0.47	2.60	0.48	0.78

It is demonstrated by analyzing the data in Figure 5 that the suggested system would follow the trajectory over time. Find the table cell B2 from the chart and add its value to the graph.

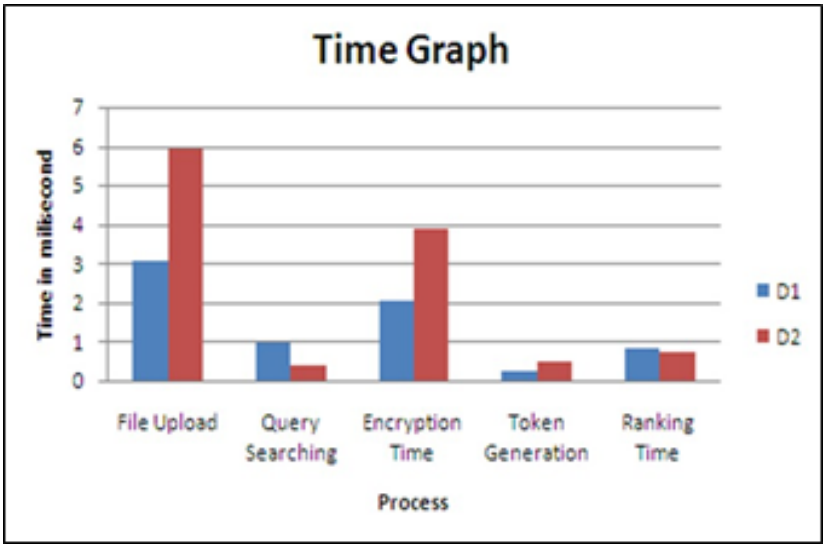

Figure 5: Time Graph

Figure 5 illustrates that the proposed system uses less memory since it distributes the Key Distribution Center (KDC). The x-axis shows the quantity of main requests made, and the y-axis shows the amount of memory used.

7. Conclusions

In conclusion, this paper has delved into the transformative impact of cloud computing on medical education, emphasizing its pivotal role in reshaping learning experiences for aspiring healthcare professionals. The integration of cloud technologies promises a future characterized by enhanced connectivity, accessibility, and preparedness to tackle the evolving challenges of modern healthcare. Moreover, as the complexity of cloud storage diminishes and its capacity expands, a paradigm shift is observed, with cloud resources becoming increasingly appealing. However, the critical aspect of ensuring data privacy is addressed through the proposed encryption system, which requires access to sensitive information or data for thorough validation. The paper also recommends the utilization of more settled figures and implementing a secure way for participating students to increase the percentage of available caution in the MPC nursing course. To facilitate this, the platform aims to establish a link between the neighbourhood and cloud servers, allowing seamless information sharing among customers. The encryption system plays a crucial role in handling validation and ensuring the security of sensitive data. As a concrete step, the paper encourages interested parties to initiate the process in a dedicated section, providing their details through a form and selecting the proposed system for implementation. This comprehensive exploration and offered solutions underscore the potential of technology, particularly cloud computing, in shaping the future of medical education, fostering innovation, and preparing the next generation of healthcare professionals for success in an ever-evolving healthcare landscape.

Acknowledgement: N/A

Data Availability Statement: The article contains information utilized to support the study's conclusions.

Funding Statement: No funding was used to write this manuscript and research paper.

Conflicts of Interest Statement: No conflicts of interest exist, according to the authors, with the publishing of this article.

Ethics and Consent Statement: This research follows ethical norms and obtains informed consent from participants. Confidentiality safeguards protected privacy.

References

1. V. Sharma, K. Sharma, and A. Kumar, “From Theory to Practice: A Systematic Review of Digital Twin Implementations Across Industry 4.0,” in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, pp. 1–7, 2023.
2. V. Sharma and S. Ramamoorthy, “A Review on Secure Data access through Multi-Keyword Searching in Cloud Storage,” in 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), IEEE, pp. 70–73, 2021.
3. Y. Tang and L. Liu, “Multi-keyword privacy-preserving search in information networks,” Technical Report 2014, http://tristartom. GitHub. io/docs/tr-mppi. pdf, 2014. [Accessed by 14 March, 2023]
4. H. Löhr, A.-R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” in Proceedings of the 1st ACM International Health Informatics Symposium, pp. 220–229, 2010.
5. Y. Tang, T. Wang, L. Liu, S. Meng, and B. Palanisamy, “Privacy-preserving indexing for E-health information networks,” in Proceedings of the 20th ACM international conference on Information and knowledge management, pp. 905–914, 2011.
6. M. Bawa, R. J. Bayardo Jr, R. Agrawal, and J. Vaidya, “Privacy-preserving indexing of documents on the network,” VLDB J., vol. 18, no. 4, pp. 837–856, 2009.
7. R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, “CryptDB: Protecting confidentiality with encrypted query processing,” in Proceedings of the twenty-third ACM symposium on operating systems principles, pp. 85–100, 2011.
8. C. Gentry, “Fully homomorphic encryption using ideal lattices,” in Proceedings of the forty-first annual ACM symposium on Theory of computing, pp. 169–178, 2009.
9. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” IEEE Trans. parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, 2013.
10. A. Ben-David, N. Nisan, and B. Pinkas, “FairplayMP: a system for secure multi-party computation,” in Proceedings of the 15th ACM conference on Computer and communications security, pp. 257–266, 2008.

11. W. Henecka, S. Kögl, A. R. Sadeghi, T. Schneider, and I. Wehrenberg, “TASTY: tool for automating secure two-party computations,” in Proceedings of the 17th ACM conference on Computer and communications security, pp. 451–462, 2010.
12. I. Damgård, M. Geisler, M. Krøigaard, and J. B. Nielsen, “Asynchronous multi-party computation: Theory and implementation,” in International workshop on public key cryptography, Springer, pp. 160–179, 2009.
13. A. Narayan and A. Haeberlen, “{DJoin}: Differentially private join queries over distributed databases,” in 10th USENIX Symposium on Operating Systems Design and Implementation (OSDI 12), pp. 149–162, 2012.
14. R. J. Bayardo Jr, R. Agrawal, D. Gruhl, and A. Somani, “YouServ: a web-hosting and content sharing tool for the masses,” in Proceedings of the 11th international conference on World Wide Web, pp. 345–354, 2002.
15. M. Bawa, R. J. Bayardo Jr, S. Rajagopalan, and E. J. Shekita, “Make it fresh, make it quick: searching a network of personal webservers,” in Proceedings of the 12th International Conference on World Wide Web, pp. 577–586, 2003.
16. G. Lin, C. Shen, Q. Shi, A. Van den Hengel, and D. Suter, “Fast supervised hashing with decision trees for high-dimensional data,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1963–1970, 2014.
17. T. P. Ezhilarasi, N. Sudheer Kumar, T. P. Latchoumi, and N. Balayesu, “A secure data sharing using IDSS CP-ABE in cloud storage,” in Advances in Industrial Automation and Smart Manufacturing: Select Proceedings of ICAIASM 2019, Springer, pp. 1073–1085, 2021.
18. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, “Persona: an online social network with user-defined privacy,” in Proceedings of the ACM SIGCOMM 2009 conference on Data communication, pp. 135–146, 2009.
19. R. Geambasu, M. Balazinska, S. D. Gribble, and H. M. Levy, “Homeviews: peer-to-peer middleware for personal data sharing applications,” in Proceedings of the 2007 ACM SIGMOD international conference on Management of data, pp. 235–246, 2007.
20. Y. Tang, L. Liu, A. Iyengar, K. Lee, and Q. Zhang, “e-ppi: Locator service in information networks with personalized privacy preservation,” in 2014 IEEE 34th International Conference on Distributed Computing Systems, IEEE, pp. 186–197, 2014.
21. D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, “Fairplay-Secure Two-Party Computation System.,” in USENIX security symposium, San Diego, CA, USA, p. 9, 2004.