2024 International Conference on Computational Intelligence and Network Systems (CINS) | 979-8-3315-0410-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/CINS63881.2024.10864435

Efficient and Lightweight Framework for Confidential Medical Image Search using Edge Computing

Arun Amaithi Rajan*, Vetriselvi V*, Aishwarya R* and Anitha Amaithi Rajan†
*Security Research Laboratory
Department of Computer Science and Engineering
College of Engineering Guindy, Anna University, Chennai, Tamil Nadu, India - 600025
Email: arunamaithirajan@gmail.com, kalvivetri@gmail.com, aishwarya.rsv@gmail.com
†Department of Computer Science and Business Systems
Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India - 627011
Email: anitharajan1804@gmail.com

***Abstract*—In healthcare, medical images are playing a major role in accurate diagnosis. Cloud storage for medical images creates security risks and latency due to some critical vulnerabilities and their distance from data sources. By bringing computation closer to the source, edge computing improves efficiency, still edge servers cannot be trusted blindly, requiring robust security measures. In this article, an efficient and lightweight framework for secure medical image search and retrieval that leverages edge computing is proposed. Here, Medical images are encrypted and similarity-preserving hashcodes are generated locally at the source, which are sent to a trusted master edge server. Before being stored, searchable hashcodes undergo homomorphic encryption, allowing for secure computations on encrypted data. The master edge server generates n shares of the encrypted images by applying a Learning With Errors (LWE) based image sharing scheme and distributing them across nearby edge devices. During retrieval, to ensure resilience against device compromise, m out of n shares are used to reconstruct the image. The master edge server retrieves and reconstructs the top k relevant images in response to the query image. This framework enhances security and efficiency by reducing reliance on cloud storage and enabling secure processing on edge servers, making it ideal for modern healthcare environments. The efficiency and security of the proposed framework are proved theoretically and experimentally. Hence, it proved that the framework is performing better than existing state-of-the-art models.**

***Index Terms*—Healthcare, Medical Image Search, Edge Computing, Trusted Computing, Searchable Encryption.**

I. Introduction

Medical imagery is crucial in healthcare as it allows for precise diagnostic, treatment, and continuous patient care. These essential images, such as X-rays, MRI, CT scans, and ultrasounds, are crucial for detecting and tracking different medical conditions [1]. In medical procedures, retrieving and analyzing images is a necessary step for researchers and healthcare professionals to make timely and informed decisions in clinical settings. The efficient storage, retrieval, and secure management of medical imaging data have become increasingly important due to the growing volume of data [2].

Typically, cloud computing has been employed to store and manage the massive amount of medical images produced by healthcare facilities. For handling large datasets, the cloud offers scalability and centralized management. However, cloud storage poses serious security threats, as sensitive medical data is vulnerable to breaches, and latency issues arise due to the physical distance between data sources and cloud servers [3]. By processing data closer to the source, edge computing has developed as a solution to these issues, lowering latency and increasing efficiency [4]. Edge servers are nevertheless vulnerable to different security risks, thus even with these benefits, they cannot be completely trusted.

To address the need for trusted computing in edge environments, this article proposes a lightweight and efficient framework for secure medical image search and retrieval that leverages confidential edge computing (TrustMedSearch). Figure 1 shows the general overview of the proposed work.

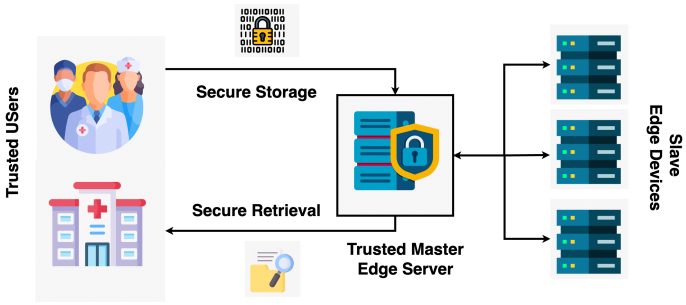


Fig. 1: Overview of the proposed system

The TrustMedSearch framework offers a trustworthy solution for traditional cloud-based systems, greatly improving the security and efficiency of medical image management in healthcare environments. The major contributions in this article are listed as follows,

1) Development of a lightweight framework that ensures the secure storage and retrieval of medical images using

edge computing.

2) For secure medical image search homomorphically encrypted hashcodes are utilized.
3) To enhance data security and resilience Learning With Errors (LWE) based secret image-sharing scheme is employed.
4) Theoretical and Experimental analysis of the proposed TrustMedSearch framework is presented and compared with existing state-of-the-art models.

The rest of the article is structured as follows: section 2 discusses the related works done in this area. The technical background details are explained in section 3 followed by a detailed working of the proposed method in section 4. Section 5 is dedicated to formal security analysis and Section 6 shows the experimental results and comparison of the proposed retrieval framework. Finally, Section 7 concludes the paper.

II. Related Work

There are various approaches available for secure and privacy-enhanced content-based image retrieval, which can be broadly divided into two categories. The first category involves generating secure indexes from image features and encrypting the images before storing them in the cloud or edge. The second category offloads feature extraction and secure index computation to the cloud or edge. Xu et al. [5] introduced an image retrieval system for large-scale cloud environments by using Hamming embedding to generate binary signatures, followed by min-hash to improve retrieval accuracy. This system enhances accuracy by combining the image's frequency histogram with the binary signature to better represent its features. Yan et al. [6] incorporated Software Guard Extensions (SGX) enclaves for secure similarity search in IoT environments, relying on a simple encryption scheme within a trusted Intel SGX environment.

In 2020, Cheng et al. [7] improved the accuracy and speed of this system by employing a 4D hyperchaotic map and deep pairwise supervised hashing. Ma et al. [8] designed an image retrieval model based on searchable encryption. Xia et al. [9] proposed a method using the Local Binary Pattern (LBP) for image search, combined with a simple encryption scheme involving big block permutation, pixel permutation, and an order-preserving polyalphabetic cipher. Janani et al. [10] used a secure multiparty-based similarity matching function for efficient medical image retrieval, comparing it with existing similarity measurement techniques. However, there is still a need for faster and more secure medical image retrieval systems. The discussed approaches may increase query processing latency due to computation overhead on either the user or cloud side. This issue can be addressed by integrating edge computing, where edge servers can be utilized for feature extraction, storage, or both in content-based image retrieval (CBIR) systems [4]. The existing methods have an edge-cloud hybrid model, which still has increased latency. To overcome this security and performance issue, in this article TrustMedSearch framework has been proposed. Table I shows the comparative analysis of the related articles. Here IE refers to Image Encryption, HE refers to Homomorphic Encryption, SS refers to Secret Sharing, CC refers to Cloud Computing and EC refers to Edge Computing.

TABLE I: Methods: Comparative Analysis

Year	Reference	IE	HE	SS	Platform
2020	Ma et al. [8]	✔	✔		CC
2022	Janani et al. [10]			✔	CC
2024	Ajitesh et al. [4]	✔		✔	CC and EC
2024	TrustMedSearch	✔	✔	✔	EC

III. Preliminaries

This section details the basic technical concepts used in the proposed TrustMedSearch framework. This section includes concepts such as edge computing, trusted computations, and the image encryption model used.

A. Edge Computing

Edge computing is a distributed computing model that moves computing resources nearer to data sources and end-users [11]. It deals with the requirement for processing in real-time and minimal delay. Edge computing decreases dependence on centralized cloud infrastructure by analyzing and processing data at the network edge, improving performance, and supporting applications in healthcare, IoT, autonomous vehicles, and smart cities. Figure 2 shows the general collaboration of edge-cloud systems.

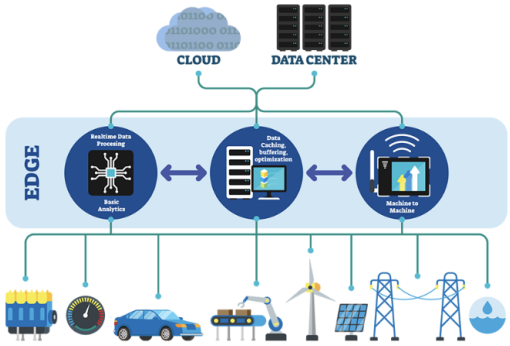


Fig. 2: General Architecture of Edge Computing

B. Secure Data Processing

Secure data processing is the method used to protect confidential information from unauthorized access, modification, or exposure while it is being processed. This includes making sure data is kept private and unaltered during processing, and transmission through encryption and secure environments. In the proposed searchable encryption of hashcodes threshold-based image-sharing schemes are used for secure medical image processing.

1) Searchable Encryption: Searchable encryption enables searches to be done on encrypted data without the need to decrypt them [8]. This method ensures that data remains confidential while also allowing for secure search functionalities.

Homomorphic encryption as searchable encryption allows secure searches over encrypted data without decrypting [12]. Given an encrypted hashcodes $E(H) = \{E(h_1), E(h_2), \ldots, E(h_N)\}$ and an encrypted search query hashcode $E(h_q)$, the master edge server can compute a function $E(f(h_q, h_i))$ directly on the encrypted hashcodes. The user then decrypts the result to determine if the images similar to the query image's hashcode h_q exist in any image hashcode h_i without revealing the plaintext data:

$$E(f(h_q, h_i)) = \begin{cases} E(1) & \text{if } h_q \text{ is in } h_i, \\ E(0) & \text{otherwise.} \end{cases} \tag{1}$$

2) Threshold-based Secret Image Sharing: Threshold-based secret image sharing is a technique where an image is split into multiple shares (n) and a specified number of these shares (let's say threshold m) are required to reconstruct the original image. This ensures that the image remains secure and inaccessible if fewer than m shares are combined. The method distributes the image among different participants or locations, enhancing security by requiring collaboration to access the complete image.

LWE-based secret image sharing uses the Learning With Errors (LWE) problem to securely distribute an image into multiple shares [13]. The original image is transformed into shares using LWE-based encryption, where each share is generated so that the original image can be reconstructed only by combining a specific number of shares. Let $\mathbf{S}$ be the secret image, and $\mathbf{A}$ is the public matrix. Each share $\mathbf{Sh}_i$ is created as:

$$\mathbf{Sh}_i = \mathbf{A} \cdot \mathbf{S} + \mathbf{e}_i \tag{2}$$

where $\mathbf{e}_i$ is an error term. Equation 2 is the search LWE problem. Each (Sh_i, e_i) is shared by the master to n slave devices. To reconstruct the image, a threshold m number of shares is combined, solving:

$$\mathbf{S} = \text{Combine}(\mathbf{Sh}_{i_1}, \mathbf{Sh}_{i_2}, \ldots, \mathbf{Sh}_{i_m}) \tag{3}$$

where Combine denotes the process of reconstructing the original image from the shares.

3) Quantum based Image Encryption: A Quantum-based medical image encryption scheme called QMedShield has been proposed by Amaithi Rajan et al. recently [14]. This QMedShield is used in the framework. QMedShield comprises bit-plane scrambling, quantum logistic map, quantum operations in the diffusion phase and hybrid chaotic map, DNA encoding, and computations in the confusion phase to transform the plain medical image into a cipher medical image.

IV. Proposed Framework

The key challenges addressed in this work focus on securing medical image retrieval in edge computing environments while ensuring efficiency. Edge servers have risks of physical tampering while reducing latency for large datasets is another concern. Furthermore, balancing security with computational efficiency is important in resource-constrained edge setups. So, In this paper, the efficient and lightweight secure medical image search framework TrustMedSearch has been proposed. The detailed architecture is shown in Figure 3. Upcoming subsections detail the framework. Table II shows the notation used.

TABLE II: List of Notations

Notation	Description
M	Medical Image
Key	Encryption Key
E	Encrypted Medical Image
H	Hashcode
$E(H)$	Encrypted Hashcode
n	Total number of shares
E_i	i^{th} share of encrypted image
m	Required shared to reconstruct image
M_q	Medical query image
$E(H_q)$	Search Trapdoor
R_i	Retrieved i^{th} encrypted image out of top-k images
ER	Encrypted retrieved medical image

A. Framework Design

This subsection presents the detailed framework design proposed and entities with functionalities associated with it. The proposed framework assumes a trusted master edge server for managing encryption and retrieval, with secure communication channels between devices. Security is based on the LWE problem, and edge servers are assumed to have adequate resources for tasks such as encryption and reconstruction.

On the user side, they take care of hashcode and encrypted image generation from the original medical image

1) $E \leftarrow \mathsf{EncMedImage}(M, Key)$: The QMedShield image encryption algorithm takes medical images M, and encryption key Key as input, and outputs encrypted medical image E.
2) $H \leftarrow \mathsf{HCodeGeneration}(M)$: The medical image M has been given as input to the hashcode generation algorithm and returns the similarity preserving hashcodes H.

The edge layer is designed as a master-slave, where the master edge server is trusted and other edge devices are not trusted. At the master edge server, hashcode encryption, Secret image share generation, and TrustMedSearch happen. The slave edge devices store the shares with image reference.

1) $E(H) \leftarrow \mathsf{EncryptHCode}(H, Key)$: All hashcodes are homomorphically encrypted and returned the encrypted hashcodes $E(H)$. This will be stored in the meta DB at the master edge server.
2) $\{E_i\}_{i=1}^{n} \leftarrow \mathsf{ShareGeneration}(E)$: Encrypted images E is given as input and generates n shares based on search-LWE problem. All these n shares will be sent to slave edge devices for storage.

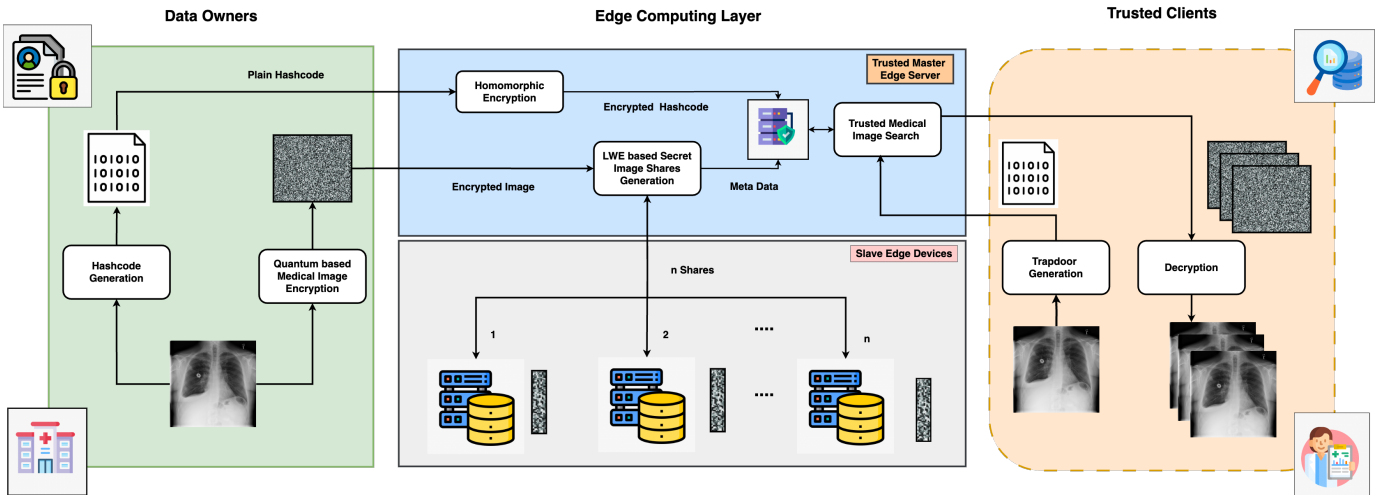


Fig. 3: Architecture diagram of the proposed TrustMedSearch Framework

3) $\{R_i\}_{i=1}^{k} \leftarrow \mathsf{TrustMedSearch}(E(H_q))$: This algorithm takes encrypted query hashcode $E(H_q)$ as input and searches in the meta DB and returns the top-k similar medical images and their shares locations. Each R_i has m shares.
4) $\{ER_i\}_{i=1}^{k} \leftarrow \mathsf{ReconstuctImages}(\{R_i\}_{i=1}^{k})$: This module fetches shares from the edge device locations and reconstructs the encrypted image.

In the end, the trusted clients request the master edge server to retrieve similar images by giving the query image. After the results are retrieved from the edge server, decrypt at the user end.

1) $E(H_q) \leftarrow \mathsf{TrapdoorGen}(M_q)$: Takes query image as input and returns the homomorphically encrypted hashcode.
2) $E \leftarrow \mathsf{DecMedImage}(ER, Key)$: The QMedShield image encryption algorithm takes medical images ER, and encryption key Key as input, and outputs decrypted retrieved medical image MR.

B. Detailed Flow

As shown in Figure 4, the proposed framework has two phases. In the secure storage phase, data owners who generate medical images encrypt them using QMedShield. Similarity-preserving hashcodes are generated using ConvNeXt-based indexing [15]. After these operations, encrypted images and hashcodes are sent to the trusted master server. Here, the hashcodes are encrypted using a homomorphic encryption technique. Furthermore, encrypted images are split into n shares using an LWE-based secret image-sharing algorithm. This enhances the privacy and security of the medical images. These n shares are stored in n slave edge devices near a trusted edge server. During the secure image retrieval phase, the client requests similar images by giving the query medical image. This query image is converted into a homomorphically encrypted hashcode and sent to the trusted edge server for the similarity search. The TrustMedSearch algorithm takes

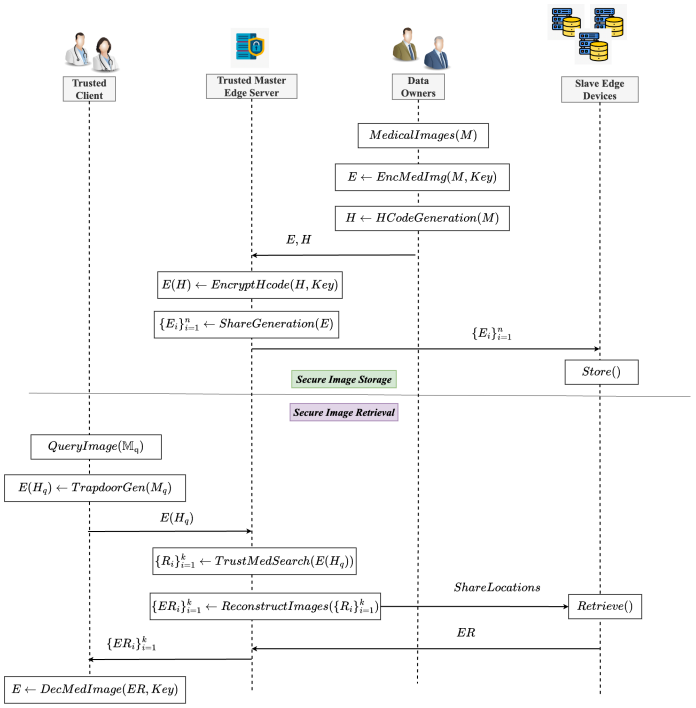


Fig. 4: Interaction diagram of the proposed TrustMedSearch Framework

place on the master edge server. After retrieving top-k images from the DB, reconstruction of those images takes place. While reconstructing, only m shares are enough. The retrieved results are sent to the client to decrypt the search results. The proposed framework is efficient, secure, and lightweight. The security analysis is shown in section 5.

V. Formal Analysis on TrustMedSearch

A. Theorem on Threshold-based Secret Image Sharing Scheme

Theorem 1: Given an image M encrypted into E using an IND-CPA secure encryption algorithm, and E is subsequently

split into n shares via a secret sharing scheme based on the search-LWE problem, the scheme is secure. Specifically, m shares are required to reconstruct E, and the probability of gaining any information about M or E with fewer than m shares is negligible.

Proof: Let $E = \text{Enc}(M, Key)$ be the ciphertext produced from the image M under an IND-CPA secure encryption scheme. IND-CPA security implies that for any two plaintexts M_0 and M_1, an adversary cannot distinguish $E_0 = \text{Enc}(key, M_0)$ from $E_1 = \text{Enc}(key, M_1)$ with probability better than $\frac{1}{2} + \text{negl}(\lambda)$, where $\text{negl}(\lambda)$ is a negligible function. The ciphertext E is split into n shares using a secret sharing scheme based on the search-LWE problem. The LWE problem is defined by:

$$\text{Given } (A, b = A \cdot E + e \mod q), \text{ find } E, \tag{4}$$

Where $A \in \mathbb{Z}_q^{m \times n}$ is a public matrix, $E \in \mathbb{Z}_q^n$ is the secret image and $e \in \mathbb{Z}_q^m$ is an error vector drawn from a discrete Gaussian distribution. Each share E_i is a pair $(b_i = A_i \cdot E + e_i \mod q, e_i)$. To reconstruct E_i, one must solve the system:

$$E_i = A^{-1} \cdot (b_i - e_i) \tag{5}$$

Given m or more shares, the system can be solved to recover E. However, with fewer than m shares, the system is underdetermined, and the LWE problem's hardness implies that finding E is computationally infeasible with given A, b. The probability of successfully reconstructing E without m shares is, therefore, $\text{negl}(\lambda)$.

- **IND-CPA Security:** Ensures that E is indistinguishable from a random ciphertext, so no information about M can be inferred from E alone.
- **LWE-Based Secret Sharing:** Ensures that reconstructing E from fewer than m shares is infeasible due to the hardness of the LWE problem. The probability of breaking the scheme is $\text{negl}(\lambda)$.

Thus, the scheme is secure, with the probability of an adversary successfully gaining any information about M or reconstructing E without the required n shares being negligible.

B. Theorem on Secure Search

Throrem 2: Given homomorphically encrypted binary hashcodes $E(h_i)$ where $h_i \in \{0, 1\}$ of length l, and a query hashcode h_q of length l, it is possible to securely search for matches between $E(h_q)$ and the encrypted hashcodes c_j without revealing any information about the underlying hashcodes. This ensures both searchability and security.

Proof: For each bit of the stored hashcode h_i and the query hashcode h_q, the XOR operation can be expressed as:

$$h_i \oplus h_q = h_i + h_q - 2 \cdot (h_i \cdot h_q) \tag{6}$$

This allows the XOR computation in the encrypted domain. Using the homomorphic properties, the XOR operation becomes:

$$E(h_i \oplus h_q) = E(h_i) + E(h_q) - 2 \cdot E(h_i \cdot h_q) \tag{7}$$

The Hamming distance between the encrypted query hashcode h_q and a stored hashcode h_i is the sum of XORs:

$$d(h_i, h_q) = \sum_{j=1}^{l} (h_i^j \oplus h_q^j) \tag{8}$$

In the encrypted domain, this is computed as:

$$E(d(h_i, h_q)) = \sum_{j=1}^{l} \left(E(h_i^j) + E(h_q^j) - 2 \cdot E(h_i^j \cdot h_q^j) \right) \tag{9}$$

- **Homomorphic Encryption**: The encryption scheme supports homomorphic addition and multiplication, ensuring that the encrypted XOR and sum can be computed without decryption during the distance calculation.
- **Semantic Security**: The encryption scheme is semantically secure, meaning that the ciphertexts $E(h_i)$ and $E(h_q)$ reveal no information about h_i and h_q to any adversary.

The homomorphically computed distance $E(d(h_i, h_q))$ remains encrypted, ensuring that the search operation is secure. Neither the server nor any adversary can gain information about the plaintext query or stored hashcodes, while the search remains fully functional and secure.

C. Theorem on Edge Computing Latency

Theorem 3: Secure image search and retrieval from nearby edge devices is more efficient than from a centralized cloud server in terms of latency.

Proof: Let ϕ_{edge} and ϕ_{cloud} denote the latency for edge devices and the cloud server, respectively. The latency for edge devices is given by:

$$\phi_{\text{edge}} = \min_x \left(\frac{d_x}{y} + \tau_{edge\_trans} + \tau_{\text{edge}} \right) \tag{10}$$

where d_x is the distance from the edge device x to the client, y is the speed of light, $\tau_{\text{edge\_trans}}$ is the transmission delay and τ_{edge} is the processing time at the edge. For a centralized cloud server, the latency is:

$$\phi_{\text{cloud}} = \frac{d_{\text{cloud}}}{y} + \tau_{\text{cloud\_trans}} + \tau_{\text{cloud}} \tag{11}$$

where d_{cloud} is the distance to the cloud server and τ_{cloud} is the server's processing time. Since $d_x < d_{\text{cloud}}$, it implies $\phi_{\text{edge}} \leq \phi_{\text{cloud}}$.

Thus, edge-based secure image search and retrieval result in lower latency compared to centralized cloud-based systems.

VI. Experimental Results and Discussion

This section is dedicated to briefly explaining the experiments conducted to show the performance of the proposed framework, the setup and dataset used with analysis.

A. Experimental Setup and Dataset

The structured framework runs on a machine featuring an Intel Xeon CPU, 64 GB RAM, 16 GB memory with an NVIDIA Quadro P5000 GPU, and a 64-bit Windows OS. The complete plan was created using Python OpenCV libraries. To experiment with the study the following medical dataset has been used. The Chest X-ray [16] dataset, which is currently the largest chest radiograph data set, contains 112,120 frontal X-ray images from 30,805 special patients. Each image was attached to the associated text disease label. To build the database, four common and numerous thoracic disease labels, including Atelectasis, Infiltration, Cardiomegaly, and Effusion have been selected.

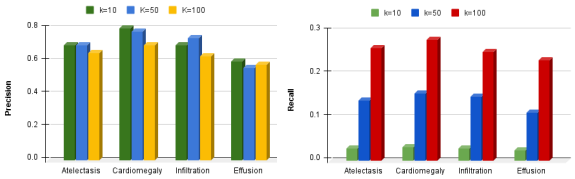
B. Retrieval Performance Analysis

To evaluate the TrustMedSearch framework, two metrics precision and recall @ Top-k results are chosen. The proposed method has been experimented with chest X-ray medical dataset and compared with 2 previous state-of-the-art secure image retrieval models SLBP [9], EdgeShield [4] as baseline models. Top-k retrieved images are used to estimate the accuracy of the retrieval. Image retrieval accuracy can be measured using Precision (P@k) and Recall (R@k) metrics. Precision refers to the ratio of relevant retrieved images to the total number of retrieved images in relation to the query image.

$$P@k = \frac{|\text{relevant images in k} \cap \text{retrieved image (k)}|}{|\text{retrieved images (k)}|} \quad (12)$$

Recall denotes the proportion of relevant retrieved images to the query image, considering the number of identical images in the entire dataset.

$$R@k = \frac{|\text{relevant images in k} \cap \text{retrieved images (k)}|}{|\text{total relevant images in the dataset}|} \quad (13)$$



(a) P@k (b) R@k

Fig. 5: Performance @ Top-k retrieved images

1) Top-k Vs (Precision and Recall): Figure 5 shows the results of precision and recall at various k values for the 4 different classes of Chest X-ray image dataset. It is observed that while k increases precision decreases and recall increases for all classes. On average when k=50, the model performs well. With this analysis, it can be concluded that TrustMedSearch works well with medical images.

2) Comparative Analysis: In this subsection, the proposed framework is compared with two baseline models chosen. The LBP-BOW model is fully cloud-based and the hashcode is extracted from the LBP features of an image. In the EdgeShield, it is an Edge-cloud hybrid model. Features are extracted and images are encrypted at the edge. When comparing the proposed model with theirs, encrypted indexes work well with chest X-ray images in TrustMedSearch. A constant medical dataset (Infiltration) and a k=50 value have been taken for comparative study. Table III shows the comparative analysis. The proposed model performs 7.9% better than EdgeSield and 16.5% better than the SLBP model.

TABLE III: Comparative Analysis

Method	Platform	P@k	R@k	F1-Score
SLBP [9]	Cloud	0.581	0.232	0.332
EdgeShield [4]	Cloud and Edge	0.642	0.256	0.365
TrustMedSearch	Edge	0.695	0.139	0.233

VII. Conclusion and Future Works

In this article, a framework has been proposed for secure and efficient medical image retrieval that effectively tackles the challenges of security, latency, and trust in edge computing. By integrating similarity-preserving hashcode generation, homomorphic encryption, and an LWE-based image-sharing scheme, it ensures secure storage and retrieval with minimal reliance on vulnerable cloud infrastructures. The proposed framework is not limited to medical images and could be extended to any image retrieval system requiring secure and efficient processing. The framework is demonstrated in a healthcare context due to the sensitive nature of medical images and the high demand for privacy and security in this field. The dynamic, verifiable threshold-based reconstruction further boosts resilience against potential edge server compromises. The proposed framework not only outperforms existing models in security and performance but also provides a scalable solution for modern healthcare. Future work includes extending support to multi-modal medical data and developing practical deployment strategies for diverse healthcare settings.

References

[1] S. Ma, T. Huang, Y. Qu, X. Chen, Y. Zhang, and Z. Zhen, "An fMRI dataset for whole-body somatotopic mapping in humans," *Scientific Data*, vol. 9, no. 1, 12 2022.

[2] A. Du, L. Wang, S. Cheng, and N. Ao, "A privacy-protected image retrieval scheme for fast and secure image search," *Symmetry*, vol. 12, no. 2, p. 282, Feb. 2020. [Online]. Available: http://dx.doi.org/10.3390/sym12020282

[3] R. Lovrenčić and D. Škvorc, "Multi-cloud applications: data and code fragmentation for improved security," *International Journal of Information Security*, 2023.

[4] A. M, D. M, A. Amaithi Rajan, V. V, and H. D, "EdgeShield: Attack resistant secure and privacy-aware remote sensing image retrieval system for military and geological applications using edge computing," *Earth Science Informatics*, 2024.

[5] Y. Xu, X. Zhao, and J. Gong, "A Large-Scale Secure Image Retrieval Method in Cloud Environment," *IEEE Access*, vol. 7, pp. 160 082–160 090, 2019.

[6] H. Yan, Z. Chen, and C. Jia, "SSIR: Secure similarity image retrieval in IoT," *Information Sciences*, vol. 479, pp. 153–163, 4 2019.

[7] S. L. Cheng, L. J. Wang, G. Huang, and A. Y. Du, "A privacy-preserving image retrieval scheme based secure kNN, DNA coding and deep hashing," *Multimedia Tools and Applications*, vol. 80, no. 15, pp. 22 733–22 755, 6 2021.

[8] W. Ma, J. Qin, X. Xiang, Y. Tan, and Z. He, "Searchable encrypted image retrieval based on multi-feature adaptive late-fusion," *Mathematics*, vol. 8, no. 6, 6 2020.

[9] Z. Xia, L. Wang, J. Tang, N. N. Xiong, and J. Weng, "A Privacy-Preserving Image Retrieval Scheme Using Secure Local Binary Pattern in Cloud Computing," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 318–330, 2021.

[10] T. Janani and M. Brindha, "SEcure Similar Image Matching (SESIM): An Improved Privacy Preserving Image Retrieval Protocol over Encrypted Cloud Database," *IEEE Transactions on Multimedia*, vol. 24, pp. 3794–3806, 2022.

[11] Y. Y. Ghadi, S. F. A. Shah, T. Mazhar, T. Shahzad, K. Ouahada, and H. Hamam, "Enhancing patient healthcare with mobile edge computing and 5g: challenges and solutions for secure online health tools," *Journal of Cloud Computing*, vol. 13, no. 1, May 2024. [Online]. Available: http://dx.doi.org/10.1186/s13677-024-00654-4

[12] M. Wang, W. Zhao, K. Cheng, Z. Wu, and J. Liu, "Homomorphic Encryption Based Privacy Preservation Scheme for DBSCAN Clustering," *Electronics (Switzerland)*, vol. 11, no. 7, 4 2022.

[13] M. H. Dehkordi, S. T. Farahi, and S. Mashhadi, "LWE-based verifiable essential secret image sharing scheme ((t,s,k,n) - VESIS)," *IET Image Processing*, vol. 18, no. 4, pp. 1053–1072, 3 2024.

[14] A. A. Rajan and V. V, "Qmedshield: A novel quantum chaos-based image encryption scheme for secure medical image storage in the cloud," 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2405.09191

[15] A. Amaithi Rajan, V. V, M. Raikwar, and R. Balaraman, "Smedir: secure medical image retrieval framework with convnext-based indexing and searchable encryption in the cloud," *Journal of Cloud Computing*, vol. 13, no. 1, Sep. 2024. [Online]. Available: http://dx.doi.org/10.1186/s13677-024-00702-z

[16] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri, and R. M. Summers, "ChestX-ray8: Hospital-scale Chest X-ray Database and Benchmarks on Weakly-Supervised Classification and Localization of Common Thorax Diseases," Tech. Rep., 2017. [Online]. Available: https://uts.nlm.nih.gov/metathesaurus.html