International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

A Secure Multi-Modal Encrypted Retrieval Methodf for Iomt

Rakshitha H R[1], Meenakshi S[2], Ananya F K[3], Dr Wahida Banu[4], Akshaya Sai A[5]

[1,2,3,5]Department of Information Science and Engineering, Don Bosco Institute of Technology, Bengaluru, India
[4]Associate Professor, Department of Information Science and Engineering, Don Bosco Institute of Technology, Bengaluru, India

Abstract
The rapid development of the Internet of Medical Things (IoMT) has resulted in the generation of large amounts of healthcare information from medical devices, hospital systems, wearable sensors, and imaging technologies. This information includes medical records, diagnostic reports, images, and sensor readings, making secure and efficient retrieval increasingly important. Conventional retrieval techniques mainly depend on keywords and often focus on a single type of data, which limits their ability to understand the actual meaning of a medical query. At the same time, storing healthcare information on cloud platforms creates privacy concerns because sensitive patient information may be exposed to unauthorized parties. This literature review studies twelve approaches related to encrypted search, cloud security, semantic retrieval, multimodal processing, and IoMT data protection. The reviewed works demonstrate the use of searchable encryption, multi-keyword retrieval, artificial intelligence, deep learning, cross-modal learning, and secure indexing. Based on these studies, a secure multimodal retrieval framework is proposed that combines semantic feature extraction, multimodal feature fusion, encryption, and cloud-based retrieval. The proposed approach aims to improve the relevance of medical search results while maintaining the confidentiality of sensitive healthcare information.

Keywords: IoMT, Multimodal Retrieval, Semantic Feature Fusion, Encrypted Retrieval, Cloud Security, Artificial Intelligence, Healthcare Data Security.

INTRODUCTION

The Internet of Medical Things (IoMT) has changed the way healthcare information is collected, stored, and accessed. Connected medical devices, wearable sensors, hospital systems, and medical imaging equipment continuously generate healthcare information. This information can include patient records, diagnostic reports, prescriptions, physiological measurements, and medical images. When properly managed, such data can assist healthcare professionals in diagnosis, patient monitoring, treatment planning, and medical research. However, the increasing size and variety of healthcare data also make efficient retrieval and secure management more difficult.

Cloud computing has become an important solution for storing IoMT data because many medical devices have limited storage and processing capabilities. Although cloud platforms provide scalability

and convenient access, healthcare information stored on external servers contains highly sensitive patient details. Unauthorized access, data leakage, and misuse of medical information can therefore create serious privacy risks. Encryption can protect the stored information, but it also creates a retrieval problem because conventional encrypted data cannot be directly searched like ordinary plaintext data. Searchable encryption has consequently become an important technique for allowing searches to be performed while keeping sensitive information protected.

Another limitation of conventional healthcare retrieval systems is their dependence on exact keywords. Medical concepts can be described using different words while referring to the same condition. Therefore, a system that only compares keywords may fail to identify relevant information. Recent studies have investigated multi-keyword ranked retrieval, semantic representations, machine learning, and deep learning to improve the relevance of search results. These approaches demonstrate that understanding the meaning of healthcare information is important for improving retrieval quality.

Medical information is also inherently multimodal. A patient's textual record may describe symptoms and diagnosis, while a corresponding medical image may provide visual evidence of the condition. Considering these sources together can provide a more complete representation of the patient's condition. The base paper addresses this problem by combining medical text and image features into a unified representation and performing encrypted retrieval in an edge-cloud environment.

Recent research has also moved toward stronger security mechanisms. For example, privacy-preserving cross-modal retrieval uses techniques such as CCA, LSH, Bloom filters, and SHVE to protect multimodal information while improving search efficiency. Other IoMT research has considered verifiable searchable encryption, blockchain, and explainable artificial intelligence to strengthen security, integrity, and trust.

This review therefore examines twelve relevant research works and studies how different techniques address the challenges of secure healthcare retrieval. The findings are used to formulate a multimodal encrypted retrieval system that combines semantic understanding with privacy-preserving search.

LITERATURE SURVEY

Several research works have focused on secure healthcare data retrieval and encrypted cloud-based systems in IoMT environments. Puning Zhang et al. (2024) proposed a multimodal encrypted retrieval method using semantic feature fusion techniques for IoMT applications. Their approach combined medical text and image features to improve retrieval accuracy and semantic understanding while ensuring data privacy through encryption methods. Although the system improved secure multimodal retrieval, it introduced high computational complexity and increased processing overhead.

Narendra Shyam Joshi et al. (2024) developed a ranked search mechanism for encrypted cloud data using multi-keyword synonym techniques. The proposed method enhanced search relevance by expanding user queries with synonym matching and performing ranked retrieval over encrypted data. While the system improved retrieval efficiency and security, it mainly supported text-based retrieval and lacked multimodal capabilities.

Similarly, Zhangchen Li et al. (2020) proposed a dictionary partition-based multi-keyword ranked search scheme for cloud environments. Their system improved retrieval speed and ranking efficiency by partitioning keyword dictionaries into smaller sections. However, the approach did not provide semantic understanding or support image-based healthcare retrieval.

M. Saradha et al. (2023) focused on enhancing cloud data security and access control through efficient auditing mechanisms. Their approach improved data confidentiality and reduced unauthorized access in cloud-based healthcare systems. However, the system mainly concentrated on security aspects and did not address semantic retrieval or multimodal data processing.

Dong Li et al. (2024) introduced a privacy-preserving ranked multi-keyword retrieval system for multiple data owners in outsourced cloud environments. The system used encrypted indexing and secure ranking mechanisms to maintain data privacy during retrieval operations. Although the approach improved cloud security, it suffered from high computational overhead and limited support for multimodal healthcare data.

Dhanraj V et al. (2023) proposed an AI-powered dual-server public-key encryption model for secure cloud search operations. Their system integrated artificial intelligence with encryption techniques to improve retrieval performance and security in cloud environments. Despite enhancing secure retrieval, the approach required high computational resources and involved complex implementation.

Haiyong Bao et al. (2022) developed a privacy-preserving multi-keyword ranked query system with ciphertext access control mechanisms. The proposed method improved secure query processing and data privacy in cloud-based retrieval systems. However, the approach mainly relied on keyword-based retrieval and lacked semantic understanding and cross-modal search support.

Y. Liu et al. (2022) proposed a deep learning-based cross-modal retrieval system for medical data. Their system extracted semantic features from both medical text and image data to improve retrieval accuracy and contextual understanding. Although the method supported efficient cross-modal retrieval, it required large training datasets and high computational power.

J. Wang et al. proposed a secure cloud-based healthcare retrieval framework using machine learning and encryption techniques. The system focused on protecting sensitive healthcare information while improving retrieval efficiency in IoMT environments. However, retrieval performance decreased when handling large-scale multimodal datasets.

X. Chen et al. introduced a semantic-aware healthcare retrieval system using artificial intelligence and cloud computing technologies. The proposed system applied semantic analysis techniques to improve contextual understanding and retrieval performance for healthcare data. Despite improving semantic retrieval accuracy, the system increased processing complexity and storage requirements.

S. Liu et al. proposed a privacy-preserving cross-modal retrieval scheme using CCA, LSH, Bloom filters, and SHVE to connect different types of medical data while keeping them protected. The approach improves retrieval efficiency for large datasets, but its main focus is efficient cross-modal searching rather than the complete semantic feature-fusion approach used in our proposed system.

Soleymani et al. introduced MI3SE, a searchable symmetric encryption scheme designed for secure retrieval in connected devices. It provides mechanisms for confidentiality, authentication, and access control, but it mainly focuses on secure keyword retrieval and does not combine medical text and image features for semantic multimodal search.

PROPOSED SYSTEM

The proposed system is designed as a secure multimodal retrieval framework for IoMT that brings together the useful ideas identified from the reviewed studies. The main objective is to allow healthcare professionals to retrieve relevant medical information while protecting sensitive patient data.

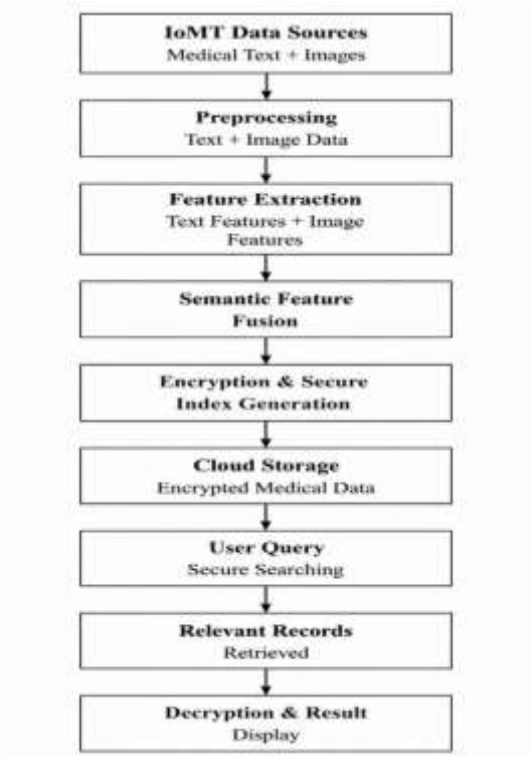
The system begins with the collection of healthcare information from IoMT devices, hospital databases, medical imaging systems, and other healthcare sources. The collected information can contain both medical text and medical images. Since these two modalities contain different types of information, they are processed separately before being combined. The base paper similarly considers image-text pairs and generates unified feature representations before constructing the encrypted index.

In the next stage, preprocessing is performed to remove unnecessary information and prepare the data for feature extraction. AI-based models are then used to obtain meaningful representations from the two modalities. Text features capture the contextual information contained in medical descriptions, while image features represent important visual characteristics. These representations are combined to form a unified semantic representation of the medical record.

The resulting representation is then protected using encryption before being outsourced to cloud storage. An encrypted index is created so that the cloud can participate in the retrieval process without directly accessing the original medical information. This follows the general principle of searchable encryption, where data remains protected while still allowing useful search operations. The base paper uses an edge-cloud architecture in which the edge server assists with query processing and the cloud handles encrypted storage and retrieval.

When a healthcare professional submits a query, the query is processed to obtain its corresponding representation. Depending on the query, the system can support text-based, image-based, or multimodal retrieval. The protected query is then used to search the encrypted index. Relevant records are ranked according to their similarity to the query, and the authorized user receives the selected results.

The proposed framework therefore combines multimodal processing, semantic understanding, encryption, searchable indexing, and secure cloud retrieval**.** Compared with systems that focus only on keywords or a single modality, the proposed approach is intended to provide a more complete understanding of healthcare information while maintaining patient privacy.



A. Equations

The feature extraction process is represented as:

$$F = \{f1, f2, f3, \ldots, fn\} \quad (1)$$

where F denotes the extracted feature vector.

The semantic feature fusion process is defined as:

$$SF = \alpha T + \beta I \quad (2)$$

where T and I represent text and image feature vectors, while α and β denote weighting parameters.

The encryption function is expressed as:

$$C = E(K, M) \quad (3)$$

where C represents encrypted data, K is the encryption key, and M is the original medical data.

The decryption function is represented as:

$$M = D(K, C) \quad (4)$$

where D denotes the decryption function.

B. Algorithm

Algorithm 1 Secure Multimodal Encrypted Retrieval: Training Phase

TRAIN(X) — Multimodal Medical Dataset
Select medical text and image data A ⊂ Dataset
Nf ← {i : datai = medical_data}
for i = 1, ..., N do
T ← EXTRACT_TEXT_FEATURES(texti)
I ← EXTRACT_IMAGE_FEATURES(imagei)
SF ← SEMANTIC_FUSION(T, I)
EF ← ENCRYPT(SF, AES_RSA)
STORE(EF, Cloud)
end for
Build AI Model : CNN → ReLU → Dense
W ← train(X, y)
return W

Algorithm 2 Secure Multimodal Encrypted Retrieval: Retrieval Phase

PREDICT(T) — User Query
Q ← RECEIVE(User_Query)
QF ← EXTRACT_FEATURES(Q)
QSF ← SEMANTIC_FUSION(QF)
R ← SEARCH(Encrypted_Cloud_Data)
D ← DECRYPT(R, AES_RSA)
if D = Relevant_Data then
DISPLAY(Results)
else
DISPLAY(No Relevant Data Found)
end if
return D

References

1. P. Zhang, J. Wang, Y. Wang, and Z. Zhang, "Multi-Modal Encrypted Retrieval Method with Semantic Feature Fusion towards Internet of Medical Things," IEEE Conference Proceedings, 2024.
2. N. S. Joshi, K. P. Sambarekar, S. Sannaki, and A. Patankar, "Ranked Search of Encrypted Cloud Data Using Multi-Keyword Synonyms and Greedy Depth-First Search," 2024 Asian Conference on Intelligent Technologies (ACIT), IEEE, 2024.
3. Z. Li, H. Dai, Y. Deng, Q. Zhou, G. Yang, and X. Yi, "Efficient and Accurate Dictionary Partition-Based Multi-Keyword Ranked Search Scheme in Cloud," IEEE Transactions on Cloud Computing, vol. 14, no. 1, pp. 1–12, 2020.
4. M. Saradha, D. G, and K. S, "Enhancing Cloud Data Security and Access Control: An Efficient Auditing Scheme," 2023 International Conference on Evolutionary Computing and Mobile Sustainable Networks, IEEE, 2023.
5. D. Li, J. Wang, Q. Liu, X. Liao, and T. Xiang, "Privacy-Preserving Ranked Multi-Keyword Retrieval for Multiple Data Owners in Outsourced Cloud," IEEE Transactions on Services Computing, vol. 17, no. 2, pp. 1–13, 2024.
6. D. V, V. J, S. B. K, and P. P, "AI-Powered Dual Server Public-Key Encryption for Secure Cloud Search," International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics, IEEE, 2023.
7. H. Bao, L. Xing, H. Wu, M. Guang, N. Ruan, and C. Dai, "MKAC: Efficient and Privacy-Preserving Multi-Keyword Ranked Query with Ciphertext Access Control in Cloud Environments," IEEE Transactions on Cloud Computing, vol. 13, no. 3, pp. 1–10, 2022.
8. Y. Liu, X. Wang, and D. Zhu, "Cross-Modal Retrieval for Medical Data Using Deep Learning," IEEE Access, vol. 10, pp. 1–11, 2022.
9. J. Wang, Y. Tan, and X. Li, "Secure Cloud-Based Healthcare Retrieval Framework Using Machine Learning Techniques," IEEE Internet of Things Journal, vol. 9, no. 5, pp. 1–10, 2023.
10. X. Chen, Y. Zhao, and H. Lin, "Semantic-Aware Healthcare Retrieval System Using Artificial Intelligence and Cloud Computing," IEEE Access, vol. 11, pp. 1–12, 2023.
11. S. Liu, G. Wang, Y. Miao, Z. Liu, J. Peng, Y. Zou, and K.-K. R. Choo, "Secure and Efficient Cross-Modal Data Retrieval in Internet of Things," IEEE Internet of Things Journal, vol. 12, no. 20, 2025.
12. S. A. Soleymani, S. Goudarzi, M. H. Anisi, P. Xiao, L. Mihaylova, and W. Wang, "MI3SE: A Multi-User Index-Based Searchable Symmetric Encryption Scheme for Improving Security of Data in Connected Electronic Devices," IEEE Transactions on Consumer Electronics, vol. 71, no. 1, 2025.