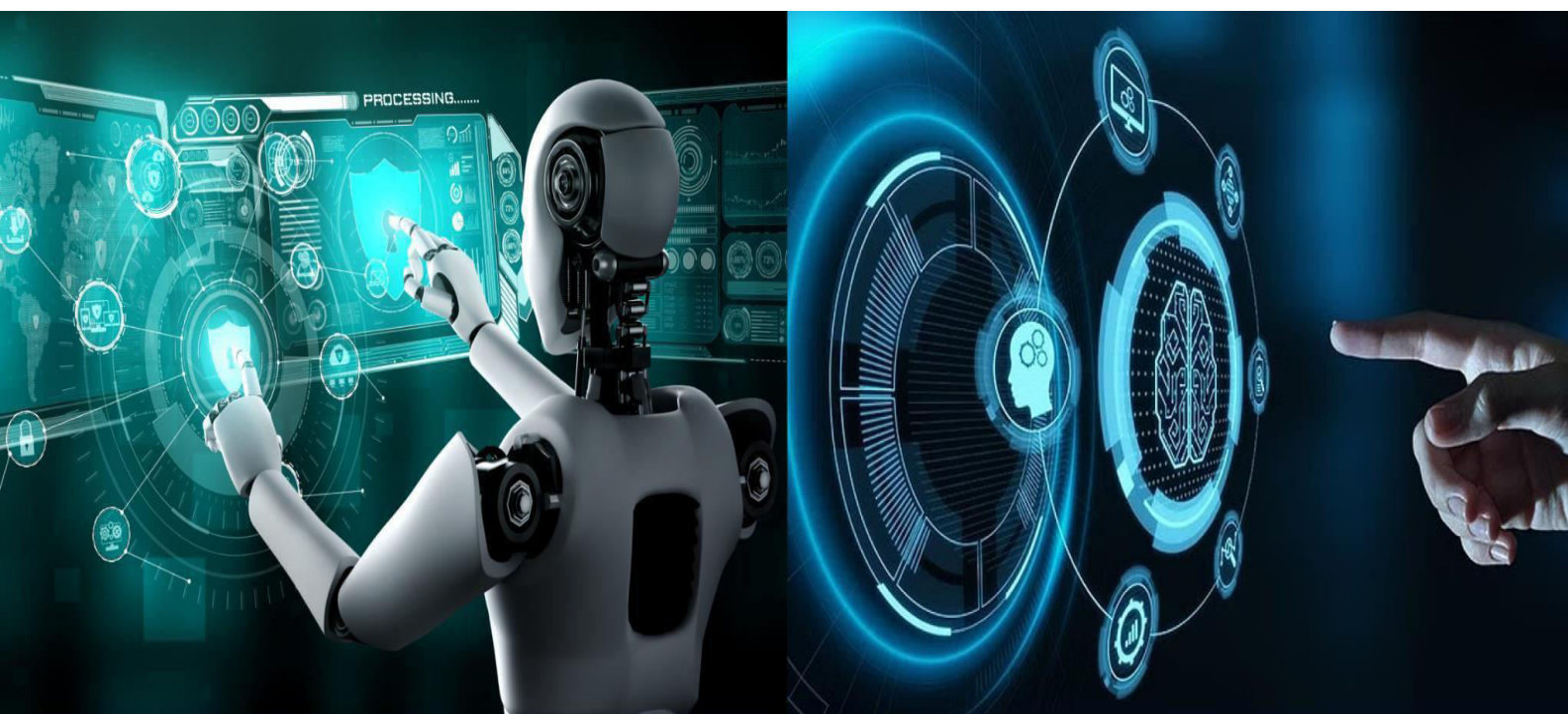


International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 11, November 2025



Secure and Efficient Encryption Image Retrieval Based on Additive Secret Sharing

B. Parimala, Prof. K. R Mohanapriya, K.N. Sivakumar

M.E Student, Department of Computer Science and Engineering, M.P. Nachimuthu M.Jaganathan Engineering College, Chennimalai, Erode, Tamilnadu, India

Associate Professor, Department of CSE, M.P.Nachimuthu M.Jaganathan Engineering College, Chennimalai, Erode, Tamilnadu, India

Associate Professor, Department of Computer Engineering, M.P.Nachimuthu M.Jaganathan Engineering College, Chennimalai, Erode, Tamilnadu, India

ABSTRACT: With the increasing use of cloud-based image sharing, protecting sensitive data from unauthorized access has become an important challenge. This project presents a secure cloud image-sharing system that ensures both privacy and controlled accessibility through an encryption-based image management model. In the proposed system, users can register and log in securely to upload their images, which are then encrypted using the Advanced Encryption Standard (AES) algorithm with a unique secret key before being stored in the cloud. This process ensures that even if unauthorized users gain access, the actual image content remains protected and unreadable. When another user requests access to an image, the image owner can either approve or deny the request. Upon approval, the secret decryption key is securely sent to the requester's registered email, allowing them to decrypt and view the image safely. This process guarantees that only authorized users can access the image data. The system also features two separate cloud servers that help administrators securely monitor and manage uploaded images without exposing their original content. This dual-cloud-server setup improves data organization and ensures a clear overview of encrypted image storage. Each image access or download activity is recorded in the system to maintain accountability and traceability. Overall, this structured approach strengthens data confidentiality, prevents unauthorized access, and provides a secure, efficient, and user-friendly platform for cloud-based image sharing. In the future, an intrusion detection mechanism can be added to identify and prevent unauthorized access attempts, further enhancing the system's security.

I. INTRODUCTION

Cloud technology has become a vital part of today's digital world, offering easy and flexible ways to store and share data online. As more users store images and personal files on cloud platforms, the need to protect this information from unauthorized access and misuse has become increasingly important. Ensuring privacy and secure image sharing is therefore a key requirement in modern systems. This project introduces a secure cloud-based image-sharing system that focuses on privacy, controlled access, and data protection. In this system, users can register and log in to upload their images, which are automatically converted into encrypted form using a secret key before being stored. This process ensures that even if data is accessed without permission, the original image remains hidden and unreadable. When another user requests to view an image, the owner can either approve or deny the request. Upon approval, the secret key is securely sent to the requester's registered email, allowing them to decrypt and view the image safely. After successful login, each server displays the uploader's name, image filename, and the encrypted version of the image, enabling administrators to monitor and manage uploaded images without exposing the original content. All image access activities are recorded for transparency and accountability. Overall, this project provides a secure, efficient, and well-organized image-sharing system that uses encryption and controlled access to protect user data and ensure safe sharing in the cloud environment.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE SURVEY

Dandan Lin et.al has proposed in this paper Image retrieval keeps attracting a lot of attention from both academic and industry over past years due to its variety of useful applications. Due to the rapid growth of deep learning approaches, more better feature vectors of images could be discovered for improving image retrieval. However, most (if not all) existing deep learning approaches consider the similarity between two images locally without considering the similarity among a group of similar images globally, and thus could not return accurate results. In this article, we study the image retrieval with manifold ranking (MR) which considers both the local similarity and the global similarity, which could give more accurate results. However, existing best-known algorithms have one of the following issues: (1) they require to build a bulky index, (2) some of them do not have any theoretical bound on the output, and (3) some of them are time-consuming. Motivated by this, we propose two algorithms, namely Monte Carlo-based MR (MCMR) and MCMR+, for image retrieval, which do not have the above issues. We are the first one to propose an index-free manifold ranking image retrieval with the output theoretical bound. More importantly, our algorithms give the first best-known time complexity result of $O(n \log n)$ where n is the total number of images in the database compared with the existing best-known result of $O(n^2)$ in the literature of computing the exact top-k results with quality guarantee. Lastly, our experimental result shows that MCMR+ outperforms existing algorithms by up to four orders of magnitude in terms of query time. Image retrieval [5] keeps attracting a lot of attention from both academic and industry over past years due to its variety of useful applications. In academic, before the growth of deep learning studies, most researchers [5, 6, 67] studied how to “engineer” good image features (manually) such that any two given images should have a high “pre-defined” similarity measure if they look similar to human. Recently, due to the growth of deep learning approaches, researchers focused on how to use deep learning models [64] like convolutional neural networks (CNNs) to capture or find the “embedded” features to get rid of (manual) feature engineering. To efficiently address the top-k MRIR search, this article proposes two novel approaches by exploiting the basic idea of Random Walk Sampling. We theoretically proved the correctness of our new weighted Random Walk Sampling strategy used in MCMR and MCMR+ as well as their time complexity for answer the top-k MRIR search. Comprehensive experiments show that our proposed method MCMR+ dominates the state-of-the-arts in terms of query time, accuracy, and space cost.

Zheng Zhang et.al has proposed in this paper Semantic hashing enables computation and memory-efficient image retrieval through learning similarity preserving binary representations. Most existing hashing methods mainly focus on preserving the piecewise class information or pairwise correlations of samples into the learned binary codes while failing to capture the mutual triplet-level ordinal structure in similarity preservation. In this article, we propose a novel Probability Ordinal-preserving Semantic Hashing (POSH) framework, which for the first time defines the ordinal-preserving hashing concept under a non-parametric Bayesian theory. Specifically, we derive the whole learning framework of the ordinal similarity-preserving hashing based on the maximum posteriori estimation, where the probabilistic ordinal similarity preservation, probabilistic quantization function, and probabilistic semantic-preserving function are jointly considered into one unified learning framework. In particular, the proposed triplet-ordering correlation preservation scheme can effectively improve the interpretation of the learned hash codes under an economical anchor-induced asymmetric graph learning model. Moreover, the sparsity-guided selective quantization function is designed to minimize the loss of space transformation, and the regressive semantic function is explored to promote the flexibility of the formulated semantics in hash code learning. The final joint learning objective is formulated to concurrently preserve the ordinal locality of original data and explore potentials of semantics for producing discriminative hash codes. Importantly, an efficient alternating optimization algorithm with the strictly proof convergence guarantee is developed to solve the resulting objective problem. Extensive experiments on several large-scale datasets validate the superiority of the proposed method against state-of-the-art hashing-based retrieval methods. In this article, we presented a novel probability ordinal-preserving semantic hashing method, dubbed POSH, which was built on a general non-parametric Bayesian-induced framework, for scalable image retrieval. The proposed POSH method defined the ordinal-preserving hashing scheme under a maximum posteriori estimation, which includes three modules, i.e., probabilistic ordinal similarity preservation module, probabilistic quantization function, and probabilistic semantic-preserving function. Particularly, the triplet ordinal similarities and flexible semantics were simultaneously considered in a unified learning framework. An efficient learning algorithm was developed to address the resulting optimization problem. Some theoretic analyses on the optimization algorithm have demonstrated its fast convergence and reasonable computational complexity involved. Extensive experimental results conducted on three large-scale benchmark datasets demonstrated that the proposed POSH method could outperform several state-of-the-art hashing methods under different evaluation criteria.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Shu-Li Cheng et.al has proposed in this paper In recent years, information leakage incidents occur frequently. Cipher text domain search has become a hot spot in multimedia technology and software engineering. Therefore, how to mine valuable information safely and effectively is very important. In this paper, we present the CBIR solution and complete the relevant software development. The proposed method not only outsources CBIR services but also avoids privacy leaks. Our main contributions are reflected in two aspects: improving search efficiency and protecting user privacy. For one thing, we propose a novel privacy protection algorithm to encrypt images. For the other thing, we propose an integrated deep hash algorithm to extract the high-level features of images. In the index encryption process, we use secure KNN to encrypt the index. Through experimental analysis and argumentation, the proposed privacy protection algorithm has a lower correlation coefficient and a better information entropy. It is secure enough and can resist common types of attacks encountered during data transmission. The proposed secure image retrieval algorithm is tested on two datasets. Compared with the same type of algorithm, the proposed algorithm has better retrieval performance. In short, the privacy reservation scheme guarantees the security and effectiveness of the system. With the arrival of the wave of cloud computing and multimedia technology, the acquisition of personal data is becoming easier, but the privacy and security of the data has raised concerns [4, 11, 23]. At present, the issue of user privacy protection has not only attracted the attention of relevant departments of various countries, but also caused great repercussions among the majority of users. This has inspired many researchers to study privacy protection data processing for information security. Large-scale data is difficult to process by users with limited computing resources and storage capabilities. At the same time, the cloud server can meet the basic computing service needs of users, so it is concerned by researchers. In cloud computing, data owner can submit data to cloud server, and cloud server completes the storage and complex processing of data. Generally, there are security risks in the transmission of multimedia data, so it is very important to study cipher text domain retrieval. In this paper, we present the CBIR solution and complete the relevant software development. The proposed method not only outsources CBIR services but also avoids privacy leaks. Our main contributions are reflected in two aspects: improving search efficiency and protecting user privacy. Encouraged by privacy protection scheme proposed in recent works, we complys a up-to-date privacy protection algorithm using hyperchaotic system and DNA coding technology. Inspired by the deep hashing algorithm, this paper uses ADFSDH to extract high-level features of images.

Yingying Li et.al has proposed in this paper The increasing awareness in privacy has partly contributed to the renewed interest in privacy-preserving encrypted image retrieval, and designing for outsourced images stored on cloud servers, etc. However, there are some limitations in these existing schemes such as low retrieval accuracy, low retrieval efficiency, and less efficient result verification in the dynamic setting. Therefore, in this paper we present a novel Dynamic Verifiable Retrieval over Encrypted Images (DVREI) scheme. First, a pre-trained Convolutional Neural Network (CNN) model is utilized to extract image features to improve retrieval accuracy. Then, an encrypted index based on the K-means clustering algorithm is designed to improve retrieval efficiency. Finally, a dynamic verification tree based on the chameleon hash is used to verify the correctness of the retrieval results and support dynamic updates. We theoretically and experimentally evaluate the security and performance of DVREI to demonstrate its practicability. WITH the ever-creasing devices and applications that produce massive images, it is vital and urgent to explore encrypted image retrieval solutions for security and performance considerations as images are typically found in a broad range of applications such as medical diagnosis, social networks, and e-commerce. The cryptographically strong encryption helps ensure images confidentiality, but complicates images processing such as image retrieval. Hence, the Searchable Encryption (SE) that facilitates secure retrieval on encrypted images has been extensively studied. Although many encrypted images retrieval schemes have been proposed, there are some limitations such as low retrieval accuracy, low retrieval efficiency, and unsuitable for dynamic scenarios. In this paper, we designed a dynamic verifiable encrypted image retrieval scheme that provides both image update and result verification. Specifically, we presented a method for building the dynamic index and hash tree. Based on these two data structures, DVREI facilitates efficient retrieval and result verification services. In addition, the application of enhanced secure KNN method based on the LWE difficult problem improves the security of DVREI. Finally, using both theoretical and experimental analyses, we demonstrated that DVREI is secure and efficient.

Zhen Wang et.al has proposed in this paper To solve the problem that the existing cipher text domain image retrieval system is challenging to balance security, retrieval efficiency, and retrieval accuracy. This research suggests a searchable encryption and deep hashing-based secure image retrieval technique that extracts more expressive image features and constructs a secure, searchable encryption scheme. First, a deep learning framework based on residual network and transfer learning model is designed to extract more representative image deep features. Secondly, the central similarity is used to quantify and construct the deep hash sequence of features. The Paillier homomorphic



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

encryption encrypts the deep hash sequence to build a high-security and low-complexity searchable index. Finally, according to the additive homomorphic property of Paillier homomorphic encryption, a similarity measurement method suitable for computing in the retrieval system's security is ensured by the encrypted domain. The experimental results, which were obtained on Web Image Database from the National University of Singapore (NUS-WIDE), Microsoft Common Objects in Context (MS COCO), and ImageNet data sets, demonstrate the system's robust security and precise retrieval, the proposed scheme can achieve efficient image retrieval without revealing user privacy. The retrieval accuracy is improved by at least 37% compared to traditional hashing schemes. At the same time, the retrieval time is saved by at least 9.7% compared to the latest deep hashing schemes. This research proposes a secure image retrieval technique based on deep hashing and searchable encryption. This approach enhances the search ability of enormous image data on the cloud while maintaining privacy. The suggested technique enhances the significance of image features, retrieval accuracy, and retrieval efficiency by generating hash codes using a transfer learning model and central similarity quantization (CSQ). The following are the key contributions: 1) Transfer learning and ResNet50 are used to create a deep neural network model that has a greater beginning performance, a quicker rate of model improvement, and better model convergence, which lowers the complexity of feature extraction. 2) The CSQ and Paillier homomorphic encryption creates a safe, searchable index with a deeper meaning to improve retrieval precision. 3) A similarity measure approach appropriate for Paillier homomorphic encryption is developed to increase the security of picture retrieval in the encrypted domain. Experimental results show that the proposed cipher text domain image retrieval method has a higher mAP value, more extensive P-R curve coverage, and shorter retrieval time than other content based image retrieval schemes. It is proved that this method has higher security, retrieval precision, and retrieval efficiency.

III. PROBLEM STATEMENT

With the rapid growth of cloud computing and online data sharing, ensuring the privacy and security of sensitive information—especially multimedia files such as images—has become a major concern. Existing cloud-based image retrieval systems often lack robust mechanisms for protecting stored image data from unauthorized access or tampering. In many cases, encryption techniques or storage structures are either weakly implemented or overly complex, leading to performance degradation and management difficulties. The main problem arises when confidential images stored in the cloud are accessed, modified, or shared without the owner's permission. Existing methods like Additive Secret Sharing (ASS) in twin-cloud architectures add unnecessary complexity and slow down the system due to inter-server communication, while still not guaranteeing strong protection against data breaches. Furthermore, there is limited control for users over who can access their uploaded data, and administrators have minimal visibility into user activities and file access logs. Therefore, there is a need for a secure, efficient, and user-controlled cloud data sharing system that ensures complete data confidentiality, controlled accessibility, and effective monitoring. The proposed system addresses these challenges by implementing AES encryption for strong data protection, key-based access control for selective sharing, and a dual-server monitoring mechanism for transparency and accountability. This approach effectively eliminates unauthorized access risks, enhances system performance, and provides a simplified yet highly secure cloud environment for image storage and sharing.

IV. PROPOSED METHODS

1. USER AUTHENTICATION AND ACCESS MANAGEMENT MODULE

This module handles user registration and secure login within the system. Every user must register with valid credentials before accessing the platform. After successful login, users can upload images securely. The authentication process ensures that only authorized users can upload, view, or request images. This controlled entry point helps protect stored image data and prevents unauthorized access, forming the foundation for the system's security and controlled sharing features.

2. SECURE IMAGE UPLOAD WITH ENCRYPTION MODULE

Once authentication is complete, users can upload images that are automatically converted into an encrypted form using the AES (Advanced Encryption Standard) algorithm. The encryption process transforms the original image into an unreadable format, ensuring that it cannot be viewed or copied by unauthorized users. The encrypted image is then stored securely in the cloud. This process protects image privacy, maintains data integrity, and ensures safe image handling during both storage and transfer.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3. CONTROLLED IMAGE SHARING MODULE

This module manages the safe and authorized sharing of encrypted images. When a user requests access to a specific image, the image owner has the right to approve or reject the request. If the request is approved, a secret decryption key is sent to the requester’s registered email, which allows them to open and view the image securely. This approach ensures that image sharing occurs only between trusted users. The controlled access process maintains image confidentiality and prevents unauthorized use or sharing of protected data.

4. DUAL SERVER MONITORING AND MANAGEMENT MODULE

This module provides administrative control and monitoring through two separate servers. After logging in, each server displays the uploader’s name, image filename, and the encrypted version of the uploaded image. This setup allows administrators to manage and verify uploads securely without revealing the original image content. The dual-server structure increases reliability, supports redundancy, and enhances transparency by allowing both servers to track activities, record access details, and maintain system accountability.

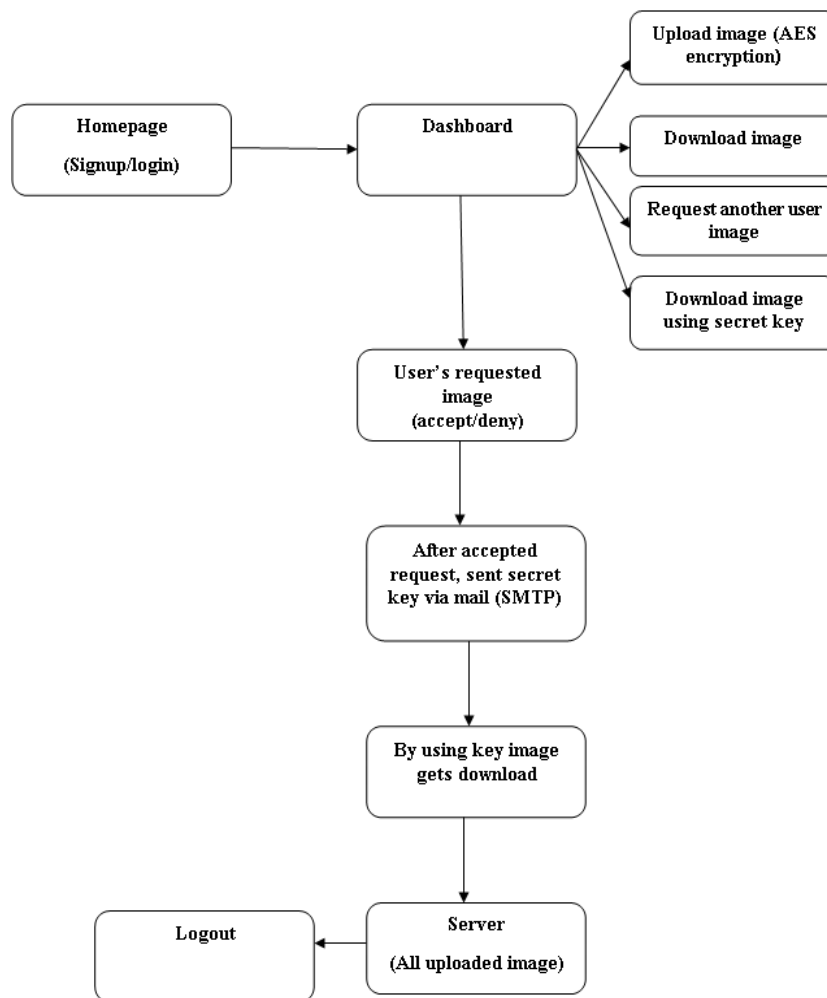


Figure.1 System Architecture

V. RESULTS AND DISCUSSION

The proposed Secure Cloud Data Sharing System using AES Encryption and Key-Based Access Control was successfully implemented and tested to evaluate its effectiveness in providing data confidentiality, controlled access, and administrative transparency. The system achieved secure image uploading, encryption, cloud storage, and selective sharing functionalities as designed. During testing, the AES encryption algorithm efficiently converted uploaded



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

images into unreadable cipher data, ensuring that no unauthorized user could view or modify the original content without the correct decryption key. The decryption process restored the original image accurately when the valid secret key was provided, demonstrating the reliability and precision of the encryption-decryption workflow. The key-based access control mechanism proved effective in managing user permissions. When an access request was made, the image owner had full control to approve or deny it. Once approved, the secret decryption key was securely sent to the requester's registered email. This ensured that only trusted and authenticated users could decrypt and view the image, thus maintaining strict privacy and data integrity. The dual-server monitoring module enhanced transparency by allowing administrators to track every upload, access, and sharing activity. Both servers displayed details such as the uploader's name, file name, and encrypted image version, without ever exposing the original content. This dual-layered structure improved accountability and minimized risks of data leakage. Performance evaluation showed that the proposed system required minimal processing time for encryption and decryption, making it suitable for real-time usage. Compared to existing CNN-based twin-cloud systems, the proposed framework offered better security, reduced complexity, and faster response time since it minimized inter-server communication. Overall, the results confirmed that the system provides a robust, efficient, and user-friendly solution for secure cloud-based data sharing. It successfully integrates encryption, controlled access, and monitoring features to ensure complete data confidentiality and operational transparency. In future enhancements, the integration of intrusion detection and anomaly monitoring mechanisms could further strengthen the system's ability to detect and prevent unauthorized access attempts in real time.

VI. CONCLUSION

In conclusion, this system provides a secure and efficient way to upload, encrypt, and share images while maintaining privacy and controlled access. It ensures that every uploaded image is protected through encryption, preventing unauthorized users from viewing or modifying the content. The dual-server setup enhances security by allowing safe monitoring and management of encrypted images without revealing the original data. The controlled sharing feature ensures that only approved users can access specific images using a secret key. Overall, the system achieves strong data protection, reliability, and organized image management through a combination of encryption, authentication, and dual-server monitoring.

REFERENCES

- [1] D. Lin, V. J. Wei, and R. C.-W. Wong, "Effective and scalable manifold ranking-based image retrieval with output bound," *ACM Trans. Knowl. Discov. Data*, vol. 17, no. 5, pp. 1–31, 2023.
- [2] Z. Zhang, X. Zhu, G. Lu, and Y. Zhang, "Probability ordinal-preserving semantic hashing for large-scale image retrieval," *ACM Trans. Knowl. Discov. Data*, vol. 15, no. 3, pp. 1–22, 2021.
- [3] D. Gupta, R. Loane, S. Gayen, and D. Demner-Fushman, "Medical image retrieval via nearest neighbor search on pre-trained image features," *Knowl.-Based Syst.*, vol. 278, 2023, Art. no. 110907.
- [4] 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 Appl.*, vol. 80, pp. 22733–22755, 2021.
- [5] Y. Li et al., "DVREI: Dynamic verifiable retrieval over encrypted images," *IEEE Trans. Comput.*, vol. 71, no. 8, pp. 1755–1769, Aug. 2022.
- [6] Y. Duan, Y. Li, L. Lu, and Y. Ding, "A faster outsourced medical image retrieval scheme with privacy preservation," *J. Syst. Archit.*, vol. 122, 2022, Art. no. 102356.
- [7] Z. Wang, Q.-y. Zhang, L.-t. Meng, and Y.-l. Liu, "Secure content based image retrieval scheme based on deep hashing and searchable encryption," *Comput., Mater. Continua*, vol. 75, no. 3, pp. 6161–6184, 2023.
- [8] C. Guo, J. Jia, K.-K. R. Choo, and Y. Jie, "Privacy-preserving image search (PPIS): Secure classification and searching using convolutional neural network over large-scale encrypted medical images," *Comput. Secur.*, vol. 99, 2020, Art. no. 102021.
- [9] Z. Xia, Q. Gu, L. Xiong, and W. Zhou, "Privacy-preserving image retrieval based on additive secret sharing," *Int. J. Auton. Adaptive Commun. Syst.*, vol. 17, no. 2, pp. 99–126, 2024.
- [10] Y. Zhang, H. Geng, Y. Xu, L. Su, and F. Liu, "A privacy-preserving image retrieval scheme in edge computing environment," *KSII Trans. Internet Inf. Syst.*, vol. 17, no. 2, pp. 450–470, 2023.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details