ISSN: 2366-1313

A BLOCKCHAIN BASED ENCRYPTED IMAGE RETRIEVAL SCHEME

[1]MR.V.V.RAMANJANEYULU, [2]M.TRIVENI, [3]K.VARUN KUMAR, [4]M.TIRUPATI RAO

[1](Assistant Professor) ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

[234]B,tech scholar ,**CSE.** Teegala Krishna Reddy Engineering College Hyderabad

ramu5b4@gmail.com, tmunnangi18@gmail.com, varunkalwa121@gmail.com, nanimodugu592@gmail.com

ABSTRACT

Encrypted image retrieval may return incorrect or incomplete results due to threats from malicious cloud servers. Most of the existing solutions focus on the efficiency and accuracy of retrieval, lack of verification of the completeness of search results, to achieve the reliability of search results and the transparency of the search process, we explore characteristic such as the decentralization and tamper-proof of blockchain, proposed a blockchain-based encrypted image retrieval scheme. This scheme stores the encrypted index on the blockchain (Ethereum), through the blockchain consensus mechanism and the function of searching on the smart contract, ensures the integrity and correctness of search results, then outsources the corresponding encrypted images to the cloud server to reduce storage cost, and designs a double-layer index structure using the bag of visual word model and simhash in the process of image similarity index. Experiments show that the reliability, high retrieval efficiency, and precision of the scheme also have a good privacy protection effect.

1. INTRODUCTION

More and more enterprises and individuals use cloud computing platform to outsource a large number of images to cloud service centres (such as Amazon EC2) to reduce local storage costs and computing resource consumption. However, the cloud service centre has lost user data due to internal

ISSN: 2366-1313

reasons and external attacks in recent years. Therefore, to ensure image security and prevent privacy leakage, users encrypt the data before outsourcing them to the cloud server. However, the encrypted images lose the plaintext feature, and the user cannot efficiently retrieve the images and affect the management of the images. Searchable encryption supports the simultaneous realization of image confidentiality and search of encrypted images, which ensures the security and availability of images, and realizes the search of encrypted data without disclosing the privacy of user data. However, most image retrieval schemes based on searchable encryption do not pay enough attention to the problem of the malicious cloud server, which may return error results. Although some related research work proposed verification schemes to let data owners verify the integrity of search results, these schemes were highly dependent on the unique index structure and did not support fine- grained access control for users' search rights. It is difficult to construct a general authentication structure to verify the similarity calculation process of images, the verification of encrypted image retrieval results is faced with great challenges. Besides, there is still a problem. When users need to query the information of a car, and the background is a desert environment, they hope to get more images of similar cars to understand their information, such as car brand and model. However, the results of similar images retrieved are only desert and mound images related to the background, which cannot well reflect the users' real goals and interests. So how to narrow the gap between image semantics and its feature descriptors, and better capture the user's interest is also a considerable challenge.

1.2 DESCRIPTION

To solve the above problems, we utilize blockchain to deal with threats brought by malicious cloud servers, realize the reliability of search results and the transparency of the search process, and support fine-grained access control of search permissions. At the same time, we introduce the blockchain fairness mechanism to realize the service payment fairness, which ensures that users can get correct and consistent with the users as long as they pay the service fees according to the agreement. In this paper, we propose a blockchain-based encrypted image retrieval service scheme BEIR. The main contributions are as follows:

• Solve the threat of malicious cloud server: using the inherent verification operation (consensus mechanism) in blockchain, we

use blockchain to store encrypted index and store encrypted images on the cloud server. Users can effectively retrieve the encrypted images on the blockchain, then download the encrypted images from the cloud server to decrypt and get the desired results finally. The search process and results are stored on the blockchain permanently and transparently. Each miner can verify the completeness without knowing the specific content, which protects the user's privacy.

• Double-layered index structure: We hope to construct the bag of visual word (bovw) model as the first layer index to determine image classification, to reduce the similarity calculation in the second layer, and then the Hamming distance of simhash is judged in a smaller range to perform image similarity search to improve the efficiency and accuracy of image retrieval and to realize image encryption by combining symmetric searchable encryption.

• We implemented the model we designed and deployed it to a local private blockchain (Ganache). The security and practicability of the scheme were proved through the analysis and performance evaluation of the experiment.

Finally, an encrypted image retrieval scheme based on the blockchain was realized.

2. LITERATURE SURVEY

The related work of this paper can be divided into two parts: 1) Encrypted image retrieval: This paper mainly introduces the development of related technologies to protect image privacy in the process of image retrieval; 2) Symmetric searchable encryption and blockchain: This paper mainly introduces the current work on how to better solve the problem of image privacy.

• Encrypted Image Retrieval In 2015, Yuan et al. [6] proposed an encryption domain image retrieval algorithm with access control function, which can manage the user's access rights to the image, and realize the access of different user roles to the image. Xia et al.[7] propose a scheme that supports CBIR over encrypted images. They extracted feature vectors to represent the corresponding images, and the pre-filter tables are constructed by locality- sensitive hashing to increase search efficiency.

• In 2019, Qin et al.[8] improved Harris algorithm is used to extract the image features, and the Speeded Up Robust Features algorithm and the Bag of Words

ISSN: 2366-1313

model are applied to generate the feature vectors of each image. Then, the Local Sensitive Hash algorithm is applied to construct the searchable index for the feature vectors. To protect the privacy of images, encryption is often per- formed before outsourcing to the cloud server. Many encryption technologies can be used, such as AES or RSA. Although encryption ensures the security of data content, it often makes the process of index establishment more difficult. B.SSE and Blockchain Cryptologists have proposed symmetric searchable encryption (SSE) [9] to support the sublinear search of encrypted data. Wang et al. [3] designed an SSE scheme for image s by using local sensitive hashing (LSH), which does not rely on homomorphic encryption, but has the problem of linear search complexity on the dataset. Cui et al. [10] also designed a scheme based on LSH. However, due to the complex process of building search credentials, the overall efficiency of the scheme is still very low.

3. SYSTEM DESIGN

Next step is to bring down whole knowledge of requirements and analysis on the desk and design the software product. The inputs from users and information gathered in requirement gathering phase are the inputs of this step. The output of this step comes in the form of two designs; logical design and physical design. Engineers produce meta-data and data dictionaries, logical diagrams, data-flow diagrams and in some cases pseudo codes.

3.1 System Architecture

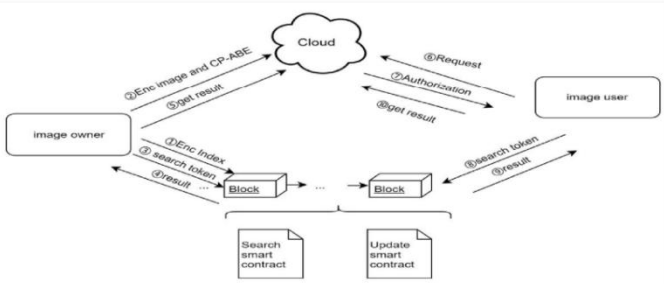

Fig 3.1 System Architecture

3.2 ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

ISSN: 2366-1313

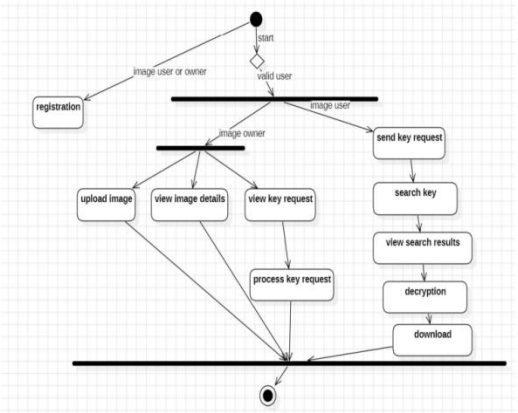

Fig 3.2 Activity Diagram

4. OUTPUT SCREENS

➢ This page helps owner to register their account

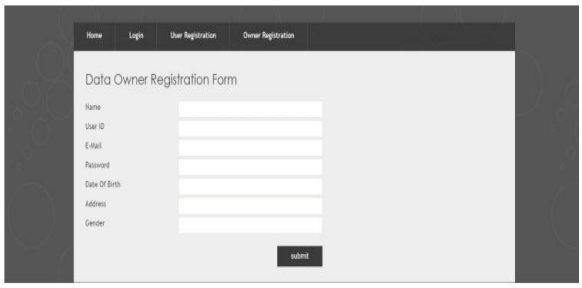

Fig 4.1 Owner registration

➢ This page helps user to register their account

Fig 4.2 User registration

➢ This page helps both user and owner to login into their accounts

Fig 4.3 Login page

➢ This page is used to enter the key which is sent through their mail

Fig 4.4 Key page

➢ This page helps to send request to owner to send the key

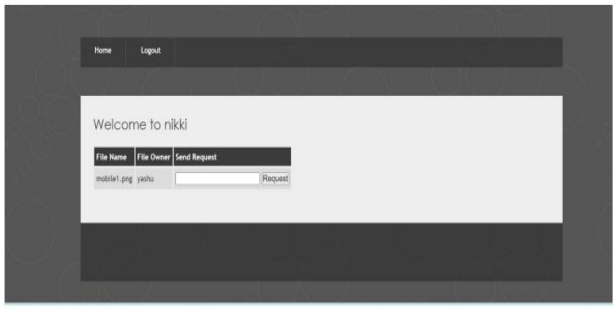

Fig 4.5 Request page

ISSN: 2366-1313

➢ In this page owner gives the details of image

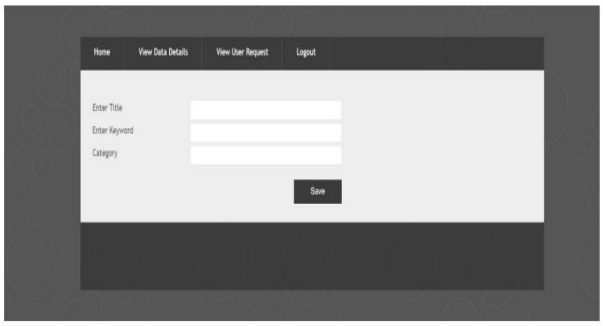

Fig 4.6 Details of image

➢ In this page Owner can view the details of the image uploaded

Fig 8.7 View data page

➢ In this page owner can view the details of the users who had sent the requests

Fig 4.8 User requests page

➢ In this page owner can upload the image

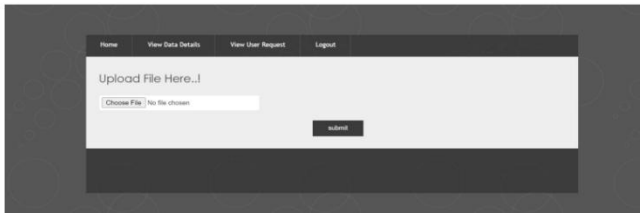

Fig 4.9 Image upload page

5. CONCLUSION

In this paper, we propose an encrypted image retrieval scheme based on blockchain, which can solve the problem that the malicious cloud server returns wrong or incomplete search results by searching on the smart contract. Besides, we also design an index structure using bag of visual word(BOVW) model and simhash to improve the efficiency and accuracy of image retrieval, and the index generation process of this scheme can also be modularized into other searchable encryption schemes. We just hope that more researchers can use blockchain to solve the trust problems encountered in the process of encrypted image search, and spend more energy exploring faster and more accurate encrypted image retrieval schemes, and finally realize encrypted image retrieval on the blockchain. At present, the cost of our privacy protection work on blockchain, such as the retrieval of the encrypted index, is still not very ideal compared with the traditional cloud server. In our future work, we will

ISSN: 2366-1313

also try to include trusted execution environment tee, homomorphic encryption, secure multiparty computing(SMC), and zero-knowledge proof, to further reduce the cost without disclosing image privacy. At the same time, we explore the feature fusion based on convolutional neural network and principal component analysis in the process of index establishment, which has achieved better similarity matching effect.

6. FUTURE ENHANCEMENT

Blockchain-based image retrieval schemes have the potential for significant enhancements in the future. Here are some potential future enhancements for such systems:

➢ Improved Decentralization: Enhancements can be made to increase the decentralization of the system. This could involve using more distributed storage solutions, such as decentralized file storage systems like IPFS (InterPlanetary File System), to store images. This would further reduce the reliance on centralized servers and improve the resilience of the system.

➢ Enhanced Privacy: Future enhancements could focus on improving the privacy of users when retrieving images. Techniques such as zero-knowledge proofs or homomorphic encryption could be employed to allow users to retrieve images without revealing sensitive information about the images they are searching for.

➢ Scalability: As blockchain-based systems grow, scalability becomes a crucial concern. Future enhancements could focus on improving the scalability of the image retrieval scheme to handle a larger number of users and a larger volume of images. This could involve implementing techniques such as sharding or layer 2 solutions to improve throughput and reduce congestion on the blockchain network.

➢ Integration with AI and Machine Learning: Integrating AI and machine learning algorithms could enhance the accuracy and efficiency of image retrieval. Advanced image recognition algorithms could be used to automatically tag and categorize images, making them easier to search for and retrieve.

➢ Incentive Mechanisms: Introducing incentive mechanisms could encourage users to contribute their images to the blockchain-based image retrieval system. This could involve rewarding users with tokens or other

incentives for uploading high-quality images or for helping to validate and curate the image database.

➢ Interoperability: Future enhancements could focus on improving interoperability with other blockchain-based systems and platforms. This would allow for seamless integration with other applications and services, making it easier for developers to build on top of the image retrieval system and for users to access images from a variety of sources.

➢ Cross-Platform Compatibility: Enhancements could also focus on improving crossplatform compatibility, allowing users to access and retrieve images from the blockchain-based system using a wide range of devices and applications. By focusing on these areas for future enhancement, blockchain-based image retrieval schemes can become more robust, scalable, and user-friendly, opening up new possibilities for image search and retrieval in various domains.

7. REFERENCES

[1] Rittinghouse, John, and James Ransome. Cloud Computing: Implemen- tation, Management, and Security. 2009.

[2] Li, Minghui, et al. "InstantCryptoGram: Secure Image Retrieval Ser- vice." IEEE INFOCOM 2018 - IEEE Conference on Computer Com- munications, 2018, pp. 2222–2230.

[3] Wang, Qian, et al. "Searchable Encryption over Feature-Rich Data." IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, 2018, pp. 496–510.

[4] Jarecki, Stanislaw, et al. "Outsourced Symmetric Private Information Retrieval." IACR Cryptology EPrint Archive, vol. 2013, 2013, p. 720.

[5] Wang, Qian, et al. "SecGDB: Graph Encryption for Exact Shortest Distance Queries with Efficient Updates." International Conference on Financial Cryptography and Data Security, 2017, pp. 79–97.

[6] Yuan, Jiawei, et al. "SEISA: Secure and Efficient Encrypted Image Search with Access Control." 2015 IEEE Conference on Computer Communications (INFOCOM), 2015, pp. 2083– 2091.

ISSN: 2366-1313

[7] Xia, Zhihua, et al. “A Privacy-Preserving and Copy-Deterrence ContentBasedImageRetrievalSchemeinCloudComputing.”IEEETransactions on Information Forensics and Security, vol. 11, no. 11, 2016, pp. 2594–2608.

[8] Qin, Jiaohua, et al. “An Encrypted Image Retrieval Method Based on Harris Corner Optimization and LSH in Cloud Computing.” IEEE Access, vol. 7, 2019, pp. 24626–24633.

[9] Kamara, Seny, et al. “Dynamic Searchable Symmetric Encryption.” IACR Cryptology EPrint Archive, vol. 2012, 2012, p. 530.

[10] Cui, Helei, et al. “Harnessing Encrypted Data in Cloud for Secure and Efficient Mobile Image Sharing.” IEEE Transactions on Mobile Computing, vol. 16, no. 5, 2017, pp. 1315– 1329.