Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1 : 2024
ISSN : **1906-9685**

BLOCK-CHAIN-BASED SECURE REMOTE SENSING IMAGE RETRIEVAL IN CLOUD ENVIRONMENT

#1 Mr.P.NARASIMHARAO, #2 A.SAIKIRAN, #3 K.KAVITHA, #4 H.SUMANASA, #5 P.NAVYASRI

#1Assistant professor in Department of IT, DVR & Dr.HS MIC College of Technology,Kanchikacherla

#2#3#4#5 B.Tech with Specialization of Information Technology , DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180

ABSTRACT_

The safe extraction of remote sensing photos in a cloud environment that is outsourced attracts a lot of interest. It becomes a crucial difficulty to establish safe and verifiable remote sensing picture retrieval because the cloud service provider (CSP) is regarded as a semitrusted third party that can return false retrieval results to save computational resources or swindle retrieval payments for profit. A blockchain-assisted verified approach for secure retrieval of encrypted remote sensing photos in a cloud context is presented in this research. We build a remote sensing image retrieval approach to enable safe and effective retrieval in response to the feature that geographical objects in the images have distinct category attributes.Furthermore, we put forth a verifiable approach that combines blockchain technology with Merkle trees to verify the accuracy and integrity of the storage and retrieval services offered by CSP. This approach has the potential to supplant the conventional third-party auditor. The security analysis and experimental evaluation show that the suggested technique is secure, verifiable, and feasible; it achieves secure remote sensing picture retrieval while thwarting CSP's hostile behaviour.

1.INTRODUCTION

Nonetheless, as a semitrusted outsider, CSP may unlawfully assemble picture data from clients while giving recovery Original copy got 9 June 2022; reconsidered 21 November 2022; acknowledged 21 December 2022. Date of distribution 26 December 2022; date of current form 24 January 2023. This work was upheld by the Public Key Innovative work Program of China under Award 2021YFB2501103, to some degree by the Public Innate Science Groundwork of China under Award 42271431, and to a limited extent by the Hubei Common Key Program of the Inherent Science Underpinning of China under Award 2020CFA001. (Relating creator: Yanyan Xu.) Xue Ouyang, Yanyan Xu, Yangsu Mao, Zhiheng Wang, and Yuejing Yan are with the State Key Lab of Data Designing in Reviewing, Planning and Remote Detecting, Wuhan College, Wuhan 430072, China (email: ouyangxue602@whu.edu.cn; xuyy@whu.edu.cn; maoyangsu@whu.edu.cn; wangzhih@whu.edu.cn; yuejingyan@whu.edu.cn). Yunqi Liu is with the Vital Research center of Aviation Data Security and Confided in Processing, Service of Training, School of Digital Science and Designing, Wuhan College, Wuhan 430072, China (email: yunqi1028@whu.edu.cn). Computerized Article Identifier 10.1109/JSTARS.2022.3231890

administrations [5]. Since remote detecting pictures portray the dispersion examples and development examples of morphological data, they uncover profoundly delicate information, like assets and geographic areas. An information hole would cause different picture security concerns and immense financial misfortunes for clients. For information insurance, remote detecting pictures are scrambled prior to moving to keep CSP from social affair picture data [6]. There are now some safe picture recovery plans in the cloud climate, including randomized highlight assurance [7], homomorphic encryption [8], vigorous hash [9], pack of-scrambled words (BOEW) model [10], and secure multiparty processing [11], and so forth. Encryption makes a security worldview accessible for rethought information, however here is another central test: How might we guarantee that CSP can give right capacity and recovery administrations in the encoded climate? The essential driver of such an issue is that picture proprietor and recovery clients will fail to keep a grip on their information assuming pictures are moved to CSP, bringing about CSP returning inadequate or erroneous recovery results to save computational assets or swindle recovery expenses for benefit. CSP keeps specialized evidence from clients, leaving clients incapable to check whether CSP is genuinely offering types of assistance that measure up to their assumptions [12]. Because of the downsides of semitrusted CSP, a conventional and direct choice is to consolidate a thirdparty reviewer (TPA) to check that the CSP is offering types of assistance honestly. For instance, in the public auditable check plans [13], [14], it accepts that the TPA is fair-minded and designates it to assess the administrations of CSP. This might appear to be a proper technique, however provided that the TPA is trusted without uncertainty. In any case, truly TPA works in a black box, with clients not knowing its inner working strategies as a general rule [14],[15]. The TPA fills in as a concentrated outsider, and its trade off might bring about the end of the whole check administration. Besides, the TPA and CSP might conspire to give a deceptive confirmation report, i.e., no matter what the rightness of the administrations given by the CSP, the TPA will report exact check results to the clients.

2.LITERATURE SURVEY

The system of secure CBIR is by and large made out of two modules: include insurance and element likeness estimation. The advancement of these modules will be investigated explicitly. The objective of element insurance is to extricate the picture includes and scramble them with encryption strategies to guarantee the encoded picture highlight descriptors can be utilized for recovery computation. For the most part, the visual substance of remote detecting pictures is communicated by customary hand-created or profound organization highlights [25]. Specifically, profound learning networks have been shown to have major areas of strength for a to perceive fundamental highlights of pictures

[26]. Thus, it is practical and OK to utilize profound organization elements to recover remote detecting pictures, since they show a mind-boggling advantage over hand-made highlights [27], [28], [29]. In the wake of separating picture includes, the picture proprietor encodes them and sends them to the CSP for additional similitude estimation. In crafted by [7], three randomization-based techniques for secure picture recovery are presented, and afterward utilizing L1 distance and Hamming distance to ascertain the distances between encoded includes precisely. In spite of the fact that works[7] have low computational intricacy, the encoded includes still stay the first component data and the recovery execution is lacking, suggesting that the recovery security and execution of these works are deficient. To tackle the above issues, a solid picture recovery in light of homomorphic encryption is proposed in [8], in which picture highlights are safeguarded by homomorphic encryption and the main piece is utilized to accomplish distance estimation in the encoded space. Hence, the recovery execution of this plan is pretty much as precise as plain picture recovery, yet homomorphic encryption requires colossal calculation, which is a significant weight for clients with restricted assets and makes proficient recovery of enormous scope pictures troublesome. To work on the proficiency of secure picture recovery, an enormous scope picture recovery is introduced in [9], in which each picture creates a hearty hash-based unique mark and afterward looks at the fingerprints of the pictures by Hamming distance. Albeit this plan keeps CSP from surmising the picture content, the critical decrease of highlights prompts its low recovery execution. In crafted by [10], a clever BOEW model for separating picture highlights is intended to further develop recovery proficiency, yet the security of scrambled elements ought to be gotten to the next level. Besides, a solid multiparty computationbased picture recovery conspire is given to upgrade recovery security in [11], yet the gotten to the next level

Euclidean distance utilized in similitude estimation needs picture data, bringing about the penance of recovery exactness. In rundown, because of the colossal number and high-layered elements of remote detecting pictures, it is trying to strike a split the difference between recovery proficiency, security, and recovery execution in these examinations. Moreover, most secure picture recovery studies expect that CSP will do capacity and recovery work sincerely, however CSP is a semitrusted outsider that might return mistaken recovery results for benefit.

3.PROPOSED SYSTEM

Even while works [7] have a low computational complexity, the performance of the retrieval is insufficient and the encrypted features retain the original feature information, suggesting that the retrieval security and performance of these works are inadequate. A secure picture retrieval method based on homomorphic encryption is suggested as a solution to the aforementioned issues.

Below architecture diagram represents mainly flow of request from the users to database through servers. In this scenario overall system is designed in three tiers separately using three layers called presentation layer, business layer, data link layer. This project was developed using 3-tier architecture.

Fig 1:Architecture

3.1 IMPLEMENTATION

User:

Using this module mobile user can register with application and login with valid username and password. User will get key from key management to login upload image and encrypt data and send to cloud server with block chain for attribute. User can view data and send to cloud..

Cloud Server :

Using this module cloud server will login view data uploaded by user and view requests

from retravel user and respond to message by send request to block and verify block chain and then send decryption key to retravel user.

Block chain Server:

Using this module block chain server can login view requests from cloud server verify block chain and send confirmation to retravel user.

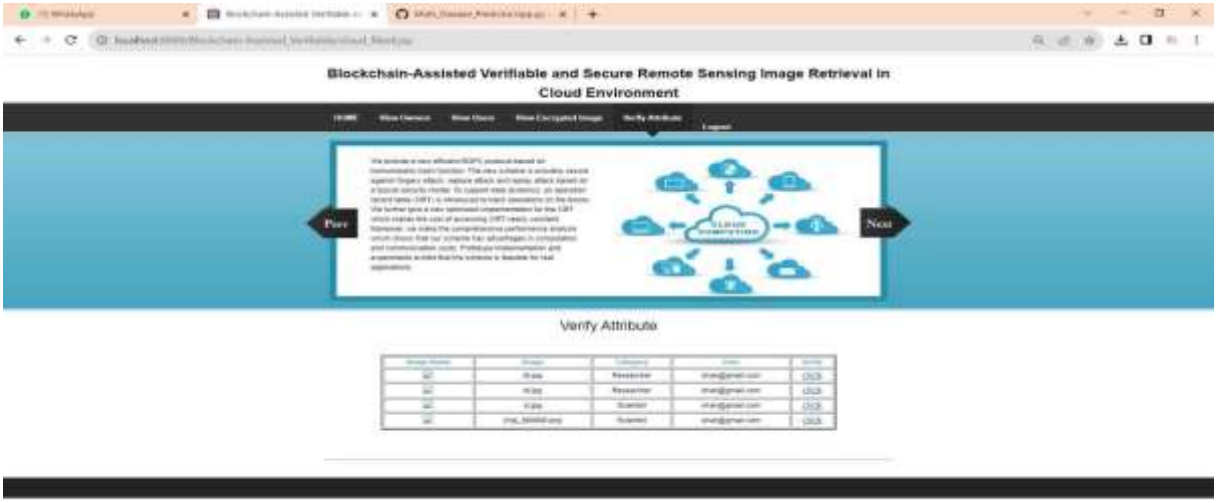
Key management:

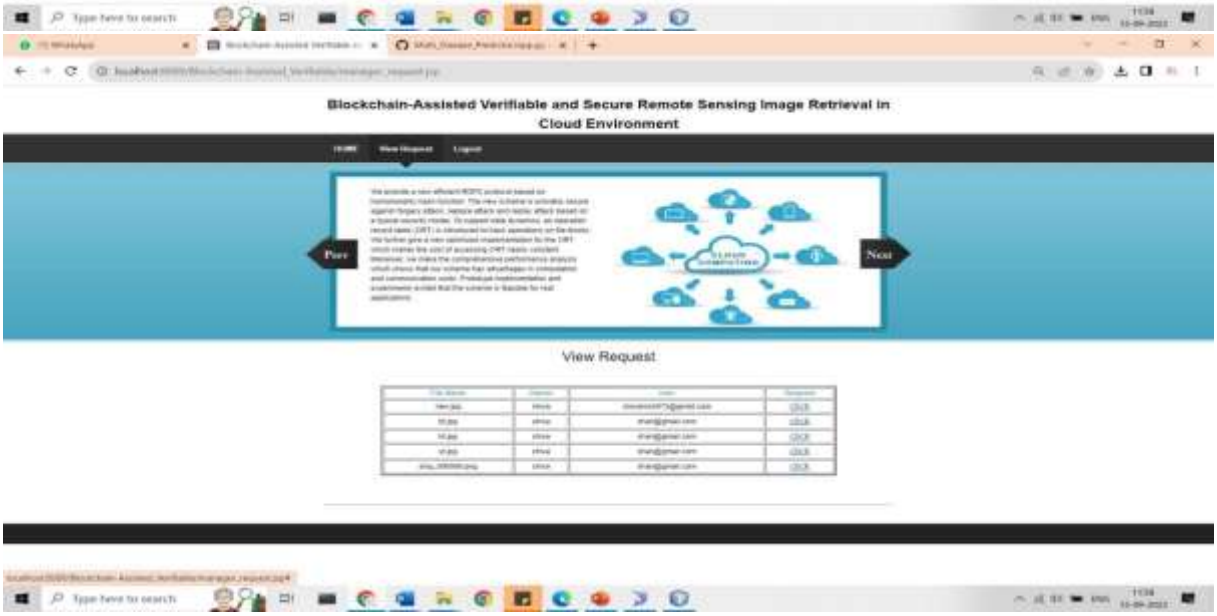
Using this module key management will login and view users authorize and send security key for login.

Retravel User:

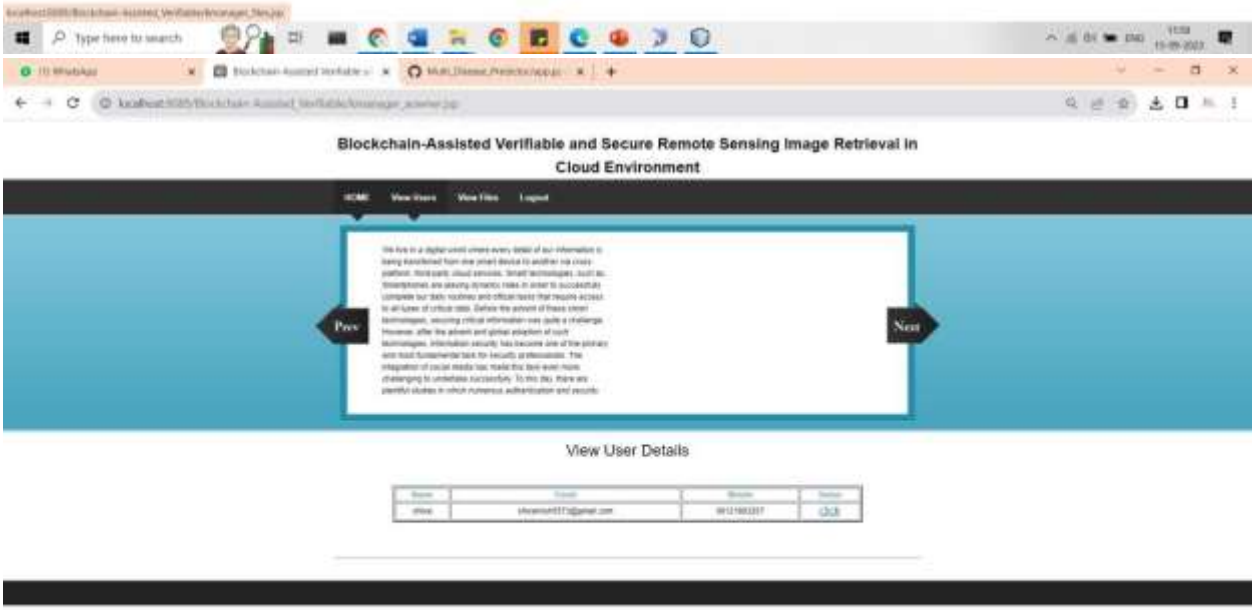
Using this module retravel user will register get key to login view encrypted data and send request to cloud server who will verify block chain for attribute if successful user will download data with key sent by cloud server.

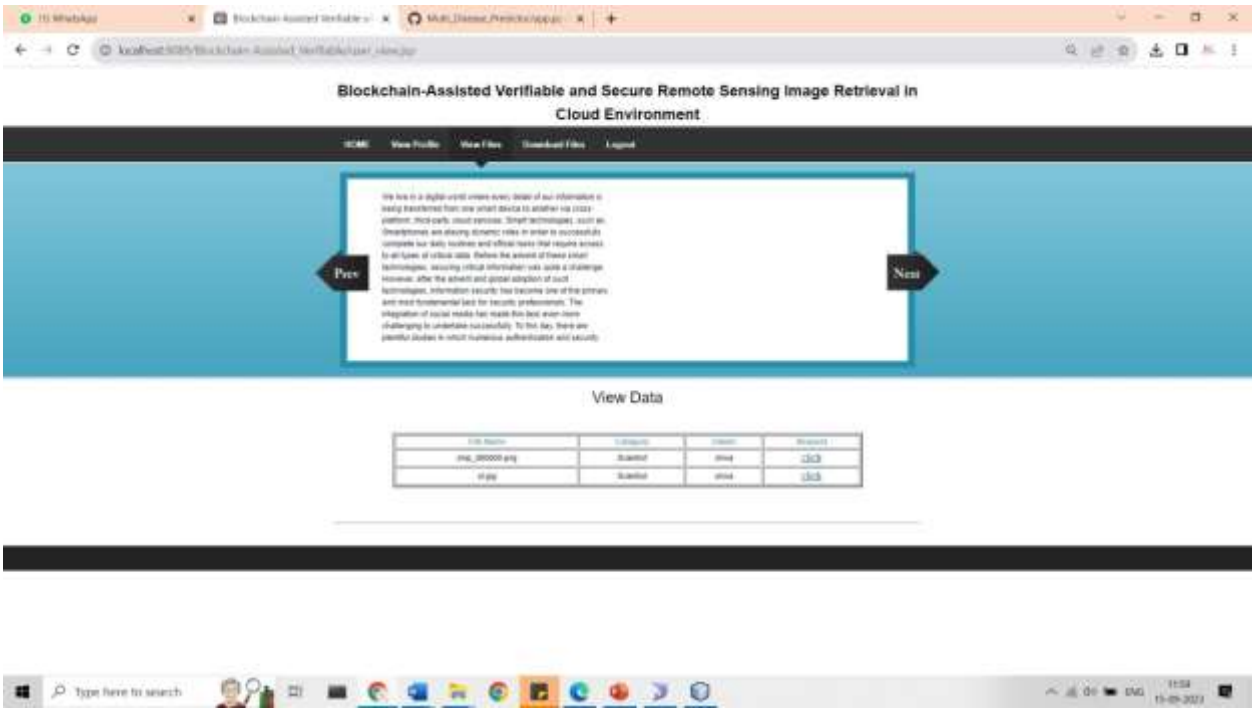
4.RESULTS AND DISCUSSION

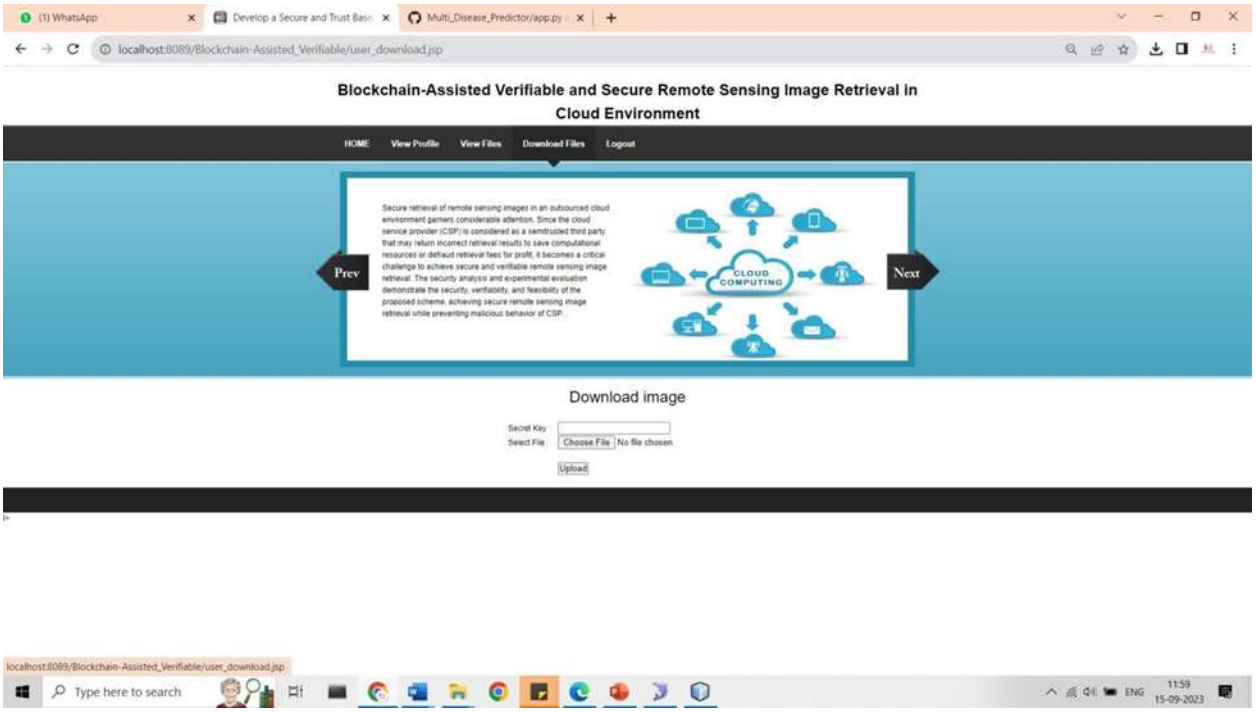





Blockchain-Assisted Verifiable and Secure Remote Sensing Image Retrieval in Cloud Environment
HOME
View Request
View Request
Logout
Prev
Next
View Files


Blockchain-Assisted Verifiable and Secure Remote Sensing Image Retrieval in Cloud Environment
HOME
View Users
View Files
Logout
Prev
Next
View User Details


Blockchain-Assisted Verifiable and Secure Remote Sensing Image Retrieval in Cloud Environment
HOME
View Profile
View Files
Download Files
Logout
Prev
Next
View Data



5.CONCLUSION

In this work, we offer a cloud-based, verifiable, secure, and blockchain-assisted remote sensing image retrieval technique that ensures accuracy of retrieval results while achieving secure and efficient picture retrieval. Because remote sensing photos are unique, we specifically designate the geographical objects in these images as attributes. The efficiency of image retrieval can be greatly increased by using the CSP to only measure images that have the same properties as the query image during the retrieval phase.Furthermore, we develop a verifiable mechanism aided by blockchain technology to allow consumers to efficiently confirm the accuracy and integrity of retrieval results. This allows the blockchain to record any dishonest behaviour on the part of CSP during the retrieval services process. We have carried out the experiment evaluation and demonstrated the security and viability of the suggested strategy.

REFERENCES

[1] H. Tamiminia, B. Salehi, M. Mahdianpari, L. Quackenbush, S. Adeli,and B. Brisco, "Google earth engine for geo-big data applications: Ameta-analysis and systematic review," ISPRS Journal of Photogram-metry and Remote Sensing, vol. 164, pp. 152–170, 2020.

[2] P. Gao, H. Zhang, J. Yu, J. Lin, X. Wang, M. Yang, and F. Kong, "Se-cure cloudaided object recognition on hyperspectral remote sensingimages," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3287–3299, 2021.

[3] Q. Zhao, S. Chen, Z. Liu, T. Baker, and Y. Zhang, "Blockchain-based privacypreserving remote data integrity checking scheme foriot information systems," Information Processing & Management,vol. 57, no. 6, p. 102355, 2020.

[4] K. N. Sukhia, M. M. Riaz, A. Ghafoor, and S. S. Ali, "Content-basedremote sensing image retrieval using multi-scale local ternary pattern,"Digital Signal Processing, vol. 104, p. 102765, 2020.

[5] J. Zhu, Q. Li, C. Wang, X. Yuan, Q. Wang, and K. Ren, "Enablinggeneric, verifiable, and secure data search in cloud services," IEEETransactions on Parallel and Distributed Systems, vol. 29, no. 8, pp.1721–1735, 2018

[6] A. Knight and N. Dai, ``Objects and the web," IEEE Softw., vol. 19, no. 2, pp. 51_59, Mar. 2002.

[7] (2018). Quorum. [Online]. Available: https://github.com/jpmorganchase/ quorum

Author's Profiles

#1:-Mr.P.NARASIMHARAO working as Assistant Professor in the Department of IT in DVR & Dr, HS MIC College of Technology, Kanchikacherla-521180

#2:-A.SAIKIRAN(20H71A1233) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180

#3:- K.KAVITHA(20H71A1215) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180

#4:H.SUMANASA(20H71A1244) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla- 521180

#5: -P.NAVYASRI(21H75A1205) B.Tech with Specialization of Information Technology in DVR & Dr.HS MIC College of Technology,Kanchikacherla-521180