IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 8, August 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108065 |

Secret Image Sharing & Identifying Fake Images Using Blockchain Technology

Meghashree N [1], DR.M.V.Vijaya kumar [2]

P.G. Student, Department of Information Science and Engineering, DR.Ambedkar Institute of Technology, Bengaluru, India[1]

Vice Principal and Head of Department of Information Science and Engineering, DR.Ambedkar Institute of Technology, Bengaluru, India[2]

ABSTRACT: Blockchain is a recently evolved technique for the application & distribution of information. Encrypted data, timestamps, & shared agreement can be utilized for transmit of distributed data in networked platforms not requiring reciprocal confidence, enhancing the effectiveness of information exchange & usage. The massive information remotely sensed imaging system may completely exploit this technique, while the multi-system associated nodal storing platform can be controlled effectively & evenly to increase the service's economic viability. This solution suggests important development techniques and creates a common approach that relies on blockchain technologies. This method's primary goal is to find duplicated images & reduce the amount of memory they take up in the Blockchain.

KEYWORDS: Blockchain, Image Deduplication, Cloud Security, Cryptography.

I. INTRODUCTION

The amount of remotely sensed information produced is growing dramatically as our nation's aviation remote sensing systems & techniques are advancing quickly. Different manufacturing systems have indeed been set up for various purchasing grounds. Services for distributing remotely sensed pictures are being specifically designed. They all choose centrally controlled administration. The jobs remain difficult, as the technology is enormous. The relevant information is unalterable & identifiable. The answer is difficult, so it takes a while to respond. Methods to create & alter multi-media materials may now offer a really high sense of authenticity thanks to the latest, significant advancements. Cloud computing is currently utilized in data exchange & deployment. By using cryptographic techniques, it is possible to share data while not relying on one another. Due to improvement in hacking techniques, hacker can able to tamper the encrypted data in cloud, there is no way to identify whether the data is tampered or not. A recently developed technique for file transmission & usage is blockchain. Information in the blockchain systems are safe and unaltered. The potential of information exchange solutions is significantly hampered by this method of distributed development & individual assistance that is inconsistent with the emerging trends of information management & extensive application. Simultaneously, the implementation advantages of remotely sensed systems are also constrained. Information integrity, decontrol, & dispersion are attributes of distributed ledgers. It has enormous scope for employment in ensuring the safety, reliability, accountability, & non-modification of information transmission service processes.

II. RELATED WORK

For overall purpose of preventing unauthorised accessing of overall communications processes including exchanged information, these study suggests unique confidential sharing groups keys managing technique (SSGK). In contrast with earlier efforts, SSGK uses a groups key to encryption shareable information as well as a confidential distribution technique that transfer this groups key. According to thorough secure but also efficiency assessments, our approach significantly reduces all protection and confidentiality issues associated with exchanging information in cloud hosting also conserves around 12% of storing area [1]. To CECS, they suggest the brand-new protected information searching as well as distribution system. This method has significant edge over earlier works throughout terms both safeguarding overall security for IoT Connected systems & customers' secret credentials as well as attaining Minimal savings for construct phrase searching passageways. information exchange

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108065 |

with information seeking that is better secured as well as effective. With respect to privacy, this plan guarantees that privacy all information stored with that internet, protected information exchange among consumers as well as Internet of things, protected information searches among both access information centre with consumers, that permits for deployment of information facilities with a weaker level of confidence [2]. Researchers reviewed the threats on blockchain systems with permissions. Focusing upon these cyberattacks, they created indications that may be used whether strategically and responsively by such a specific organisation within a blockchain system can identify continuing threats. They suggested any viable computational framework that those parameters that was modelled after SIEM technologies [3]. This suggested method for privacy-preserving inspection on distributed information secures information kept on cloud servers that verifies its accuracy. Prior of saving all information within its clouds servers, its technology encrypts that information using using AES encryption algorithm. They employed the SHA1 technique that verifies the validity all the information so order that confirm storing accuracy [4]. Information from the authorized source is shared with your organization. This pairing key is generated by this file by utilizing DSS method. Every every block in that HARS system, a verified signatures is produced by utilizing publicly monitoring method. A Validation meta can always be generated by this team's member [5].

III. METHODOLOGY

RSA algorithm:

The best efficient method of encrypting data is the RSA scheme, which uses public keys. The RSA method was developed in 1978 by Rivest, Shamir, and Adleman. The cryptography or collection of cryptographic methods utilized for particular safety solutions or activities, is built on the RSA method (Rivest-Shamir-Adleman), that also facilitates public-key encrypting which is frequently utilized to safeguard delicate information, especially when something is dispatched along an unprotected system like the world wide web. One public-key & a private-key are used in public-key cryptography, commonly referred to as asymmetrical cryptographic method. While the private-key needs to be preserved as a secret, the public-key could be distributed with anybody.

DES algorithm:

Utilizing keys of 48 bits, the Data Encryption Standard (DES) block-cypher technique which transforms plain-text stored in block of 64 bits into cipher - text. Because it uses a symmetrical encryption technique, the very same key is utilized to both encrypt & decode information. Employing the DES method for both encrypting & decrypting of information is done.

Hashing Algorithm:

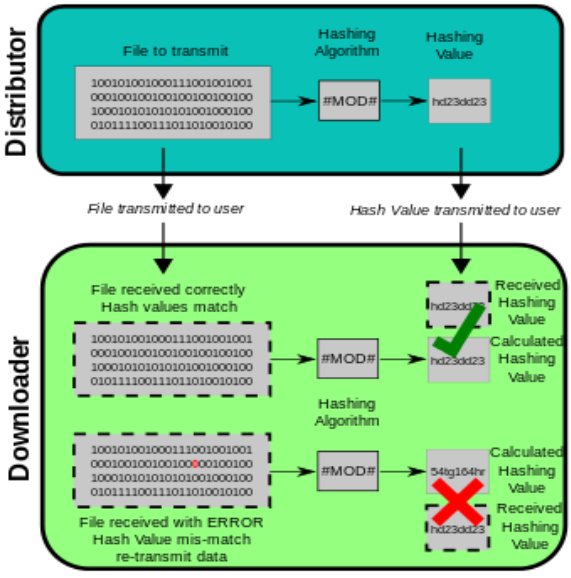

Fig 1: MD5 Algorithm Process

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108065 |

Fig 1 displays the Message Digest Method 5 (MD5). It comprises of a string, of any length which could be generated into a 128-bit hash using MD5's cryptosystems hashing technique. The digests are shown as 32-bit hexa-decimal values.

Block chain Technology

A blockchain is a continuous collection of documents, known as blocks or chunks that are connected together via encryption. Every chunk includes transactional information (often displayed as a root hash), a secure hash of the preceding chunk, plus the time-stamp. The data owner can register the data user, new data user registering time new user get the private key, this private key is used to decrypt the data owner uploaded the image file. In this system data owner uploaded time uploaded images are blockchain storage, for block creation below Algorithm 1 is used.

Algorithm 1: Block Creation Process

```
Input  : Electronic Health Record
Output : Block chain Block
User   : Data Owner
1 if N transactions are added in upload queue
2   Generate the Root-Hash-code from data
3   Fetch Pervious Block Hash code (PBV)
4   Form Header PBV-RH-TimeStamp-Nonce
5   Encrypt data and create Block Body
6   Merge Header and Body to create block
7 else
8   wait and check
```

Algorithm 2: Block Verification Process

```
Input  : Block ID
Output : Status of the Block
User   : Auditor
1 if number of Block (N) > 0 then
2   List the Block details
3   Fetch block to be tested & Extract data
4   From the transaction generate Hash Code(1)
5   Fetch Previous Block Hash Code
6   Compare both Hash Code and show result
7 else
8   Display no block the verify
```

Data users are created by Data owner, while creation of data users' information will be assigned by the data owner and decryption key will send to the data users. Data owner has to set the key information after uploading the images.

If fake images detected whether all the blocks in block chain are intact or not and uploading and downloading hashing are not matching. For verification following Algorithm 2 is used.

IV. PROPOSED SYSTEM

The introduction of blockchain is seen as a recent technical revolution. It uses peer-to-peer decentralized network system to track purchases, contracts, & payments. Distributed operation, information storage in a block and then chain format, safe information transfer & accessibility, as well as tamper-evident & unquestionable information protection are all advantages of distributed ledger system. Fig. 2 illustrates how the proposed system stores image data on a blockchain. Select image to and upload to cloud in blockchain format. Before storing in cloud uploading images are encrypted with RSA algorithm. If user want to download the particular image file first user want to select private key file to download the particular selected image file if selected private key was wrong user can't download the selected image. A genuine picture can be swapped out for a counterfeit one by a hacker. When the users' try to download a picture, they are informed whether or not the picture has been altered, which indicates whether or not downloaded picture is real. The picture will only be downloaded if it is authentic. The introduction of blockchain is seen as a recent technical revolution. It uses peer-to-peer decentralized network system to track purchases, contracts, & payments. Distributed operation, information storage in a block and then chain format, safe information transfer & accessibility, as well as tamper-evident & unquestionable information protection are all advantages of distributed ledger system. Fig. 2 illustrates how the proposed system stores image data on a blockchain. Select image to and upload to cloud in blockchain format. Before storing in cloud uploading images are encrypted with RSA algorithm. If user want to download the particular image file first user want to select private key file to download the particular selected image file if selected private key was wrong user can't download the selected image. A genuine picture can be swapped out

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108065 |

for a counterfeit one by a hacker. When the users' try to download a picture, they are informed whether or not the picture has been altered, which indicates whether or not downloaded picture is real. The picture will only be downloaded if it is authentic.

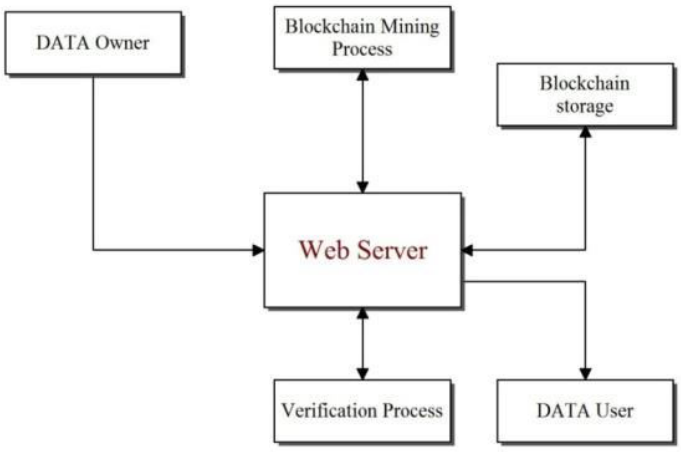

Fig2: System Architecture

V. EVALUATION

This system is deployed and tested in hybrid cloud formation and tested, it meets all the requirements specifications. All the four user functionalities are working correctly. Fig 3 & 4 shows the Block Uploading and Downloading Time comparison and Fig 3 shows the time requirements for block verification.

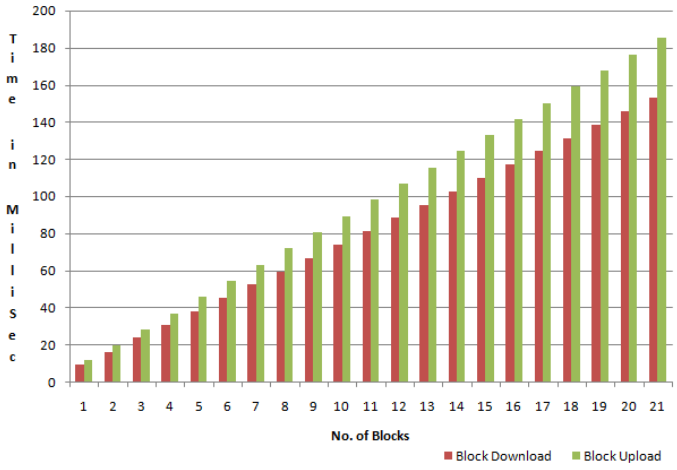

Fig 3: Block Uploading & Downloading

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108065 |

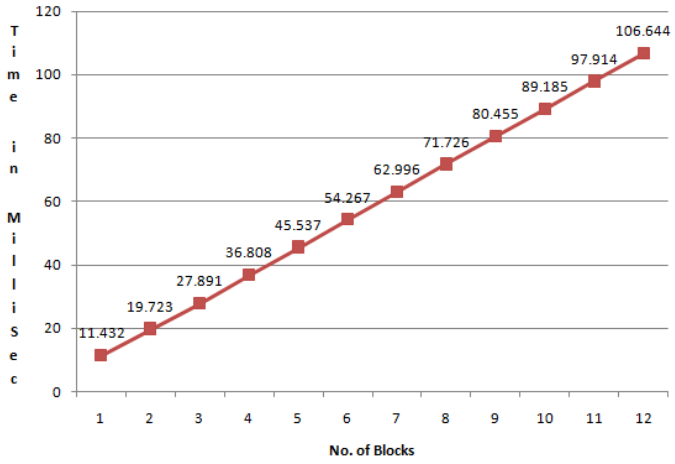

Fig 4: Block Verification Time Graph

VI. CONCLUSION

In this research, we firstly presented a revolutionary fake-image detecting approach using blockchain and hash function. A strong ledger with a hashed technique suggested technique is applied to various photos, despite the fact that several resilient hash functions have already been presented to obtain identical pictures to a search one. The suggested approach was shown to be resistant to a variety of picture modifications in the test, in addition to outperforming the state-of-the-art systems.

REFERENCES

1. Han, S., Han, K. and Zhang, S., 2019. A data sharing protocol to minimize security and privacy risks of cloud storage in big data era. IEEE Access, 7, pp.60290-60298.
2. Tao, Y., Xu, P. and Jin, H., 2019. Secure data sharing and search for cloud-edge-collaborative storage. IEEE Access, 8, pp.15963-15972.
3. Putz, B. and Pernul, G., 2020, November. Detecting blockchain security threats. In 2020 IEEE International Conference on Blockchain (Blockchain) (pp. 313-320). IEEE.
4. Ghutugade, K.B. and Patil, G.A., 2016, December. Privacy preserving auditing for shared data in cloud. In 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 300-305). IEEE.
5. Trueman, T.E. and Narayanasamy, P., 2015, November. Ensuring privacy and data freshness for public auditing of shared data in cloud. In 2015 IEEE International
6. Hsu, C.C., Zhuang, Y.X. and Lee, C.Y., 2020. Deep fake image detection based on pairwise learning. Applied Sciences, 10(1), p.370.
7. Guo, Y., Cao, X., Zhang, W. and Wang, R., 2018. Fake colorized image detection. IEEE Transactions on Information Forensics and Security, 13(8), pp.1932-1944.
8. Liao, Q., Li, Y., Wang, X., Kong, B., Zhu, B., Lyu, S., Yin, Y., Song, Q. and Wu, X., 2021, September. Imperceptible adversarial examples for fake image detection. In 2021 IEEE International Conference on Image Processing (ICIP) (pp. 3912-3916). IEEE.
9. Tanaka, M. and Kiya, H., 2021, March. Fake-image detection with Robust Hashing. In 2021 IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech) (pp. 40-43). IEEE.
10. El Abbadi, N., Hassan, A.M. and AL-Nwany, M.M., 2013. Blind Fake Image detection. International Journal of Computer Science Issues (IJCSI), 10(4), p.180.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details