International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

September 2022 | Issue 52 | Volume 14 | Number 3 | Pages 207-211

SHARE AND RETRIEVE IMAGES SECURELY USING BLOCKCHAIN TECHNOLOGY

A.A.A. Shareef [1] P.L. Yannawar [1] A.S.H. Abdul-Qawy [2] M.G. Almusharref [3]

1. Vision and Intelligence System Lab, Department of Computer Science and IT, Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India, shareef.kin@gmail.com, pravinyannawar@gmail.com
2. Department of Mathematics and Computer Science, Faculty of Science, Sumait University, Zanzibar, Tanzania antarabdulqawy@sumait.ac.tz
3. Department of Computer Science and IT, Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India, almosharf@gmail.com

Abstract- Image integrity refers to determining whether or not the bits in an image file have been modified at any stage. Platforms may cause a digital file to change. This system would be entirely online. Editing software is becoming more intelligent as the number of individuals using the internet grows. Most files are uneditable in some operating systems or file systems. However, so-called hackers or electronic device masters have file systems that can readily access and change any file data. In this paper, we integrate the benefits of Blockchain and Cryptography to give a fast, decentralized, and safe way to store and distribute files. Cryptography is used to hide our data, whereas Blockchain is used to make it difficult to change the data that has been saved and to allow the user to recover it from several servers. We use the Advanced Encryption Standard (AES) technique to encrypt the data file. The IPFS (InterPlanetary File System) generates a unique hash for the file. Smart contracts store the whole transaction and display the user's files on the Blockchain.

Keywords: Blockchain, Cryptography, IPFS, AES, Ethereum, Smart Contracts.

1. INTRODUCTION

One of the most critical technologies in the world is blockchain technology [1]. A distributed database shared by many nodes in a computer network is known as a blockchain. A blockchain is a database that keeps data digitally. Without the assistance of a reliable third party, the Blockchain's uniqueness ensures the security and validity of a data record while also fostering trust [2]. The Blockchain securely transmits assets such as money, property, contracts, and other data without needing an intermediate third-party like government, company, or a bank. It is tough to modify data after being stored on a blockchain [3]. Blockchain is a distributed database that exists on numerous computers simultaneously and is decentralized. As new sets of recordings, or 'blocks', are uploaded, it continues to grow.

Each block has its own timestamp and connection to the preceding block, forming a complete chain. The entire database is copied to everyone on the network. Old blocks are maintained indefinitely, and new blocks are irreversibly added to the ledger, making it hard to tamper with by fabricating documents, transactions, and other data. The blocks are linked cryptographically. Figure 1 depicts the general structure of Blockchain [4].

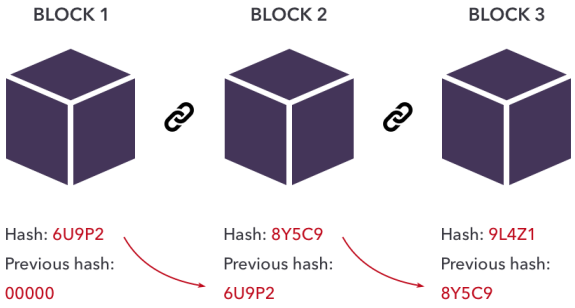

Figure 1. A simple structure of Blockchain [4]

IPFS is a versioned file system that allows you to store files and trace their changes over time. It uses a peer-to-peer network and distributed file system protocol to store and distribute data. It connects all computing devices through a global namespace and employs content-addressing to identify each file within it. Distributed Hash Tables are used (DHT). The data in DHT is distributed across a network of computers and is well-coordinated to allow for quick access and lookup across nodes [5]. Due to the expansion of the computer applications range and its related technology, multimedia-based data has increasingly ginned a significant attention; and thus, digital photographs are regularly transferred via public, unsecured channels in these multimedia data [6]. Based on this, the security of digital image data has poorly been harmed as a result of the advancement of modern computer

technology. Many classical encryption methods have been presented to meet security difficulties thus far. However, many well-developed algorithms were created for text encryption alone and therefore are ineffective for digital image encryption.

Text encryption techniques are complex for image data due to several characteristics including large data quantities and higher correlation between pixel values [7]. Due to third-party participation, traditional security solutions for sensitive data are vanishing in IoT contexts. As a modern technology, Blockchain is used to address trusting issues as well as to eliminate or minimize of the impact of third parties. The authors [3] offered a private permission approach based on blockchain technology for secure image encryption when it is used in the IoT-based environments. The values of cryptographic pixels of the encrypted images are saved on the Blockchain in this system, assuring the image data's privacy and security [8]. Generally, images are electronic documents that play a critical function in society by storing and disseminating information about a historical event.

Image frauds involving image-altering tools have emerged due to digitalization in developing countries such as India. Because a server's security can be breached by hackers or other internet experts, as well as by electronic devices with technological flaws, we cannot use a conventional database to maintain track of the image's context [9]. Blockchain, an emerging technology that can be used to store data (here image) in such a way that it is verified before being stored; and thus, no one can change it. This is due to the fact of decentralized peer-to-peer networking model of a group of people where everyone has a copy of the public ledger containing information of a portion with the image in it. Because Blockchain operates collectively, it is challenging to construct a blockchain and nearly impossible to update its data [10].

2. RELATED WORK

There are some research articles and project work on Blockchain-based data and file sharing securely. This section summarizes some of them. A.K. Pathak and S. Shankhari [10] have developed a system that provides users with a social media platform for storing images and verifying them through their system using blockchain technology. Their work details a practical implementation of the Online Biding system, which allows for secure key exchange and agreement. They have put in place a method for capturing and uploading images. Image processing, image signing, making a transaction, creating a block in the server, and adding it to the chain.

B.K. Zheng, et al. [11] introduced a new solution based on blockchain for trusted data exchange and sharing. They have used Blockchain to prohibit tampering with the shared data and a Paillier cryptosystem for ensuring its confidentiality. The suggested approach allows for trading shared data while protecting transaction information with the (p, t) threshold Paillier cryptosystem. They conducted their experimental work in a cloud-based storage environment, and concluded that the proposed technique is efficient and effective.

In April 2019, Y. Ranka, et al. [12] proposed a new solution called DAPP for an efficient data storage. They have integrated Blockchain and Cryptography technologies to create a fast, decentralized, and safe way to store and distribute files. Cryptography is used to hide their data, whereas Blockchain is used to make it difficult to change the data that has been saved and to allow the user to recover it from several servers. They employed a symmetric key to encrypt their data files in the recommended technique. Whisper provides decentralized communication, whereas Swarm provides decentralized storage. Ethereum Whisper is used to communicate between users. It allows users to send encrypted messages to one another. We use Advanced Encryption to encrypt the data file.

R. Kumar, et al. [13] have offered a new solution called InterPlanetary File System (IPFS) for video and image sharing based on blockchain decentralized peer-to-peer model. The perceptual hash (pHash) method is used in their technology in order to find instances of any infringement of multimedia copyright. The pHash of the multimedia file posted to IPFS is calculated and compared to other pHash values in the blockchain network. If the multimedia matches the current pHash values, it will be flagged as altered. Due to the absence of a third party.

B.Q. Liu, et al. [14] have implemented a new infrastructure based on blockchain that aims to achieve security in trading and sharing X-Ray picture data, which might be utilized for more in-depth research. The actions in the precise depiction are as follows: (i) to safeguard patient privacy, (i.e., personal information such as name, ID, etc.) in the encrypted data of the image using a hashing-based technique; (ii) a watermark is placed to the picture data; (iii) Blocks are formed using the blockchain consensus process; and (iv) the plan put out in this article solves the security problems that standard cloud-based picture data management solutions have. This includes disclosure of user privacy, unauthorized manipulation, and the possible data stealing or sale. The massive data of clinical medicine image is instead given more scientific research value by creating secured transaction systems that links different users with various data demands.

K. Koptyra and M.R. Ogiela [15] have proposed a new technique to secure images using Blockchain. This technique is called imagechain, a cryptographic framework that uses hash links to link digital images together. The most notable aspect that sets it apart from Blockchain is that the images are not stored within the blocks. Instead, the block and the picture are mixed during the embedding phase. As a result, the imagechain is made up of regular graphic files that may be used in the same way as any other image, but each one also includes a data block that connects it to a previous part in the chain. Except for the photos, the offered approach does not require any other files. It is portable and user-friendly because it supports many file formats and embedding methods. Simultaneously, the method delivers a high level of security and forgery resistance.

X. Dong [16] has developed a blockchain-based technique for protecting image privacy that deals with

image privacy content while preserving the copyright of pictures on the network to preserve the rights and privacy of image owners. The user uploads pictures after editing the section's settings. The server creates an intelligent picture trading contract after pre-processing the user-provided photos. The server then switches to the number depending on the blockchain. The image thumbnail can be viewed by other users via personal space of authors so the transaction can be completed through paying the given amount of the smart contract. A transaction, then, is initiated by The Word Money Network for recording author's copyrights to the pictures and save the transaction information to the database. The creation processes the image's private data and employs the blockchain technology for safeguarding the rights and privacy of the image owner.

F. Gao, et al. [17] have proposed a data encryption algorithm based on blockchain technology. In their wok The DES encryption algorithm is presented in detail by examining the symmetric key algorithm and the public key algorithm. To guarantee the accuracy of the data and the one-time encryption of the data, the two related technologies of digital envelopes and message authentication are examined. Based on this, the asymmetric encryption algorithm based on chaotic sequence of neural networks and the asymmetric encryption algorithm based on chaotic attractor of neural networks are examined, and the security is tested.

3. PROPOSED WORK

We propose a decentralized system to share images securely using Blockchain, IPFS, and AES encryption technologies. We ensure that data transmitted on the network cannot be tampered with or corrupted by incorporating blockchain technology. We maintain the whole history of all files transferred, providing users with a sense of security.

The software used to implement the system is a visual studio, HTML, and python3. The system is implemented on localhost using two ends, client and server, the user on the client uploads an image to the system using three parameters sender name, receiver name and file's key. The uploaded image will encrypt using the AES algorithm, and a blockchain hash will generate for an image using the IPFS system. The copy on encrypted image with the AES extension is stored on the sender computer. The receiver needs two parameters to download the picture, and these parameters are the file's key shared by the sender and the file hash generated by the IPFS system. The receiver can download an image by using these two parameters. Only the person who has these parameters can download the image. In same way the user on server can share photo to client. The proposed model by the authors is in Figure 2.

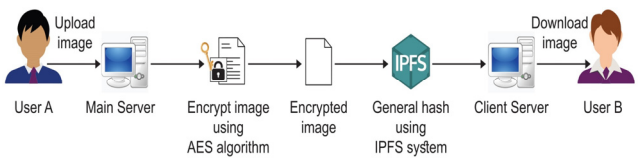

Figure 2. Blockchain-based image encryption model

4. IMPLEMENTATION

The first stage of the system starts by uploading the image. The proposed model examines the image's contents, encrypts it, and then uploads it to the Blockchain. As shown in Figure 3, this stage steps can be stated as follows: (i) read the original data from the image that the user wishes to upload; (ii) encrypt the image's contents using the AES algorithm; (iii) create an image file containing the encrypted data and the file name by aes extension; (iv) generate the image's hash using the IPFS system, and the hash will store in the Blockchain; (v) the image's hash is subsequently uploaded to the Blockchain, which may be used to get the image from the network. The system interface is shown in Figure 4.

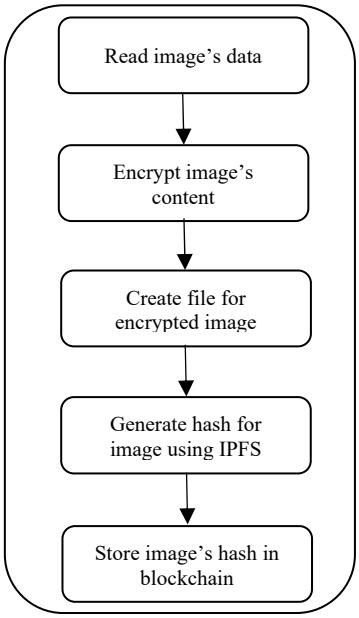

Figure 3. Steps to upload the image to the system

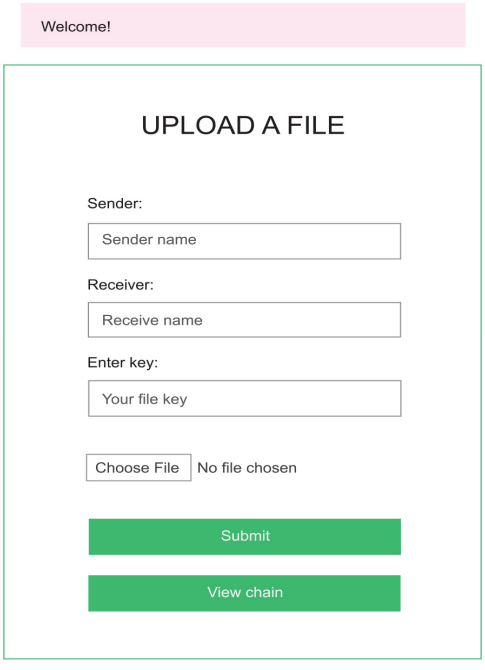

Figure 4. Upload the image to the system

After uploading the image and encrypting it, the user on the other end can now download the encrypted image. The proposed method obtains the image content from the Blockchain, decrypts it, and saves it on local system. The procedure of download an image is as follows :(i) get the image hash and the image key added by user A; (ii) get the image content from the IPFS system by using the hash; (iii) using the image's key and hash, decrypt the data obtained in the previous step (the Image's key used for uploading and downloading the image should be the same); (iv) Download the image to the local system. These steps are shown in Figure 5, while the system interface is shown in Figure 6.

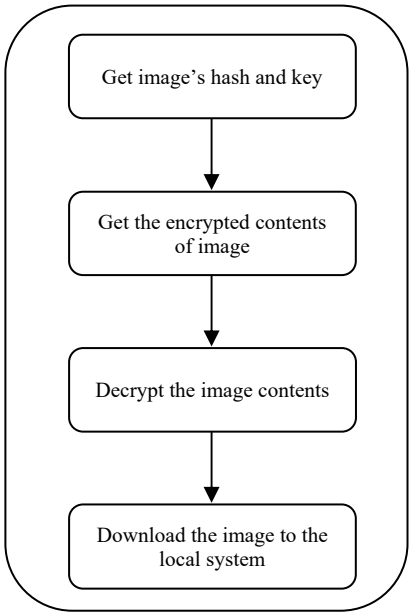

Figure 5. Steps to download the image from the system

There are many benefits of our system by using Blockchain to secure images and share it: (i) the original image is encrypted using AES (Advanced Encryption Standard), and only authorized users with the key can see, edit and download it; (ii) The image is shared, distributed, and replicated across numerous nodes, making access to the entire image impossible for a hacker; (iii) Secure communication between users is formed utilizing a decentralized network to transfer credentials, avoiding the need to store communications on a central server; (iv) true ownership of an image is ensured since Blockchain transactions are immutable; (v) There is unlimited image storage available. Comparing to the previous related studies, our work is become more accurate and more secure because we used AES algorithm which is used for advanced encryption, from its name which stands for Advanced Encryption Standard. Some previous works used DES to encrypt their data and their data was text whereas we proposed system to secure an image, prevent the access to its details without permission and transmit it in secure environment. Moreover, we used two keys to send and receive files between tow end users, the first key entered by sender and the second key generated automatically by IPFS which is very difficult to break it by hacker or unauthorized user.

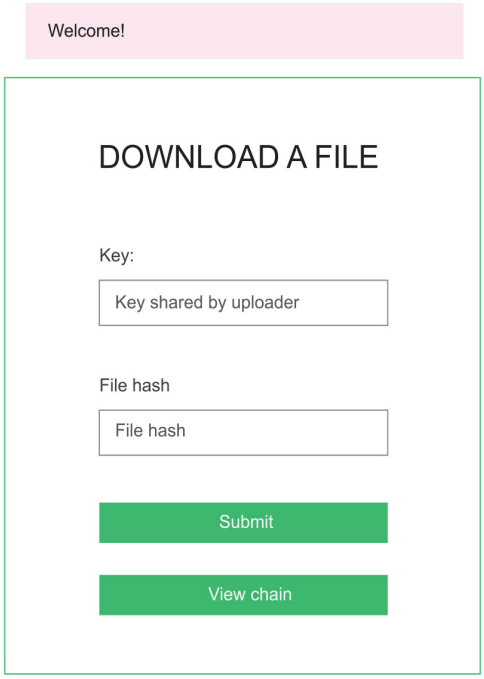

Figure 6. Download the image from the system

5. CONCLUSIONS

In this paper, we have proposed a new method to share images securely using Blockchain. We create two servers, the central server and the client-server. The user uploads the image to one of these two servers. The user should add a key for the image uploaded. We first encrypt the image with an AES algorithm using the unique key provided by the user and upload it to the IPFS system. The IPFS system generates a specific hash for the image, and this hash will store in the Blockchain. The receiver should know the unique key provided by the sender and hash file to be able to download and see the encrypted image. Thus, we offer a secure way to store and share images using blockchain technology. The benefits of this technique are that the authorized user can see and download the image, and the transferred image is stored on multiple nodes, making it difficult for the hacker to access it.

REFERENCES

[1] L. Brunese, F. Mercaldo, A. Reginelli, A. Santone, "A Blockchain Based Proposal for Protecting Healthcare Systems Through Formal Methods", Procedia Comput. Sci., Vol. 159, pp. 1787-1794, 2019.

[2] "Blockchain Definition: What You Need to Know", https://www.investopedia.com/terms/b/blockchain.asp (accessed May 04, 2022).

[3] P.W. Khan, Y. Byun, "A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things", Entropy, Vol. 22, No. 2, 2020.

[4] "Blockchain 101: The Simplest Guide You Will Ever Read", https://www.velotio.com/engineering-blog/introduction-to-blockchain-and-how-bitcoin-works (accessed Aug. 27, 2022).

[5] "Learn to Securely Share Files on the Blockchain with IPFS! | by Coral Health | Medium", https://mycoralhealth.medium.com/learn-to-securely-share-files-on-the-block

chain-with-ipfs-219ee47df54c (accessed May 04, 2022).
[6] M. Sayrac, M. Ari, M.C. Taplamacioglu, "General Overview of Wireless Communication Technology", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 38, Vol. 11, No. 1, pp. 25-30, March 2019.
[7] J. Ahmad, S.O. Hwang, "A Secure Image Encryption Scheme Based on Chaotic Maps and Affine Transformation", Multimed. Tools Appl., Vol. 75, No. 21, pp. 13951-13976, 2016.
[8] M. Bilgili, F. Ekinci, A. Ozbek, T. Demirdelen, "Short Term Renewable Energy Strategic Vision in the World", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 51, Vol. 14, No. 2, pp. 111-123, 2022.
[9] N. Tohidi, R.B. Rustamov, "Short Overview of Advanced Metaheuristic Methods", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 51, Vol. 14, No. 2, pp. 84-97, June 2022.
[10] S. Shankhari, "Image Integrity Analysis with BlockChain Technology Bachelor Thesis Indian Institute of Information Technology Kalyani Department of Computer Science and Information", Social Media Platform, May 2019.
[11] B.K. Zheng, et al., "Scalable and Privacy-Preserving Data Sharing Based on Blockchain", J. Comput. Sci. Technol., Vol. 33, No. 3, pp. 557-567, 2018.
[12] Y. Ranka, J. Bagrecha, K. Gandhi, B. Sarvaria, P.M. Chawan, "A Survey on File Storage and Retrieval using Blockchain Technology", Int. Res. J. Eng. Technol., Vol. 05, No. 10, p. 4, 2018.
[13] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T.R. Gadekallu, N.N. Xiong, "A Secured Distributed Detection System Based on IPFS and Blockchain for Industrial Image and Video Data Security", J. Parallel Distrib. Comput., Vol. 152, pp. 128-143, 2021.
[14] B. Liu, M. Liu, X. Jiang, F. Zhao, R. Wang, "A Blockchain-Based Scheme for Secure Sharing of X-Ray Medical Images", Adv. Intell. Syst. Comput., Vol. 895, No. 6, pp. 29-42, 2020.
[15] K. Koptyra, M.R. Ogiela, "Imagechain Application of Blockchain Technology for Images", Sensors, Vol. 21, No. 1, pp. 1-12, Switzerland, 2021.
[16] X. Dong, "A Method of Image Privacy Protection Based on Blockchain Technology", Int. Conf. Cloud Comput. Big Data Blockchain, ICCBB 2018, pp. 1-4, 2018.
[17] F. Gao, "Data Encryption Algorithm for E-Commerce Platform Based on Blockchain Technology", Discret. Contin. Dyn. Syst, Ser. S, Vol. 12, No. 4-5, pp. 1457-1470, 2019.

BIOGRAPHIES

Ahmed Abdullah Ali Shareef was born in Hajjah, Yemen on 11 August 1986. He received the B.Sc. in Computer Science from Sana'a University, Yemen in 2009, and Master of Technology in Embedded Systems from JNTU, Anantapur, India in 2016. He is currently a Ph.D. candidate at Department of Computer Science and IT, Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India. His research interests in artificial intelligence, computer vision, and Blockchain.

Pravin L. Yannawar was born in Maharashtra on 15 May 1979. He received his B.Sc. in Computer Science from Babasaheb Ambedkar Marathwada University, Aurangabad, India in June 1999. He has completed M.Sc., SET (Computer Science and Application) and Ph.D. in 2001, 2006 and 2011, respectively. He is Member of IETE & life member of IAEng, CSTA, IUPRAI and IACSIT. He receives the DST Fast Track Young Scientist research award and successfully completed a major project sanctioned by DST. He is an Associate Professor in Department of Computer Science and Information Technology, Babasaheb Ambedkar Marathwada University, Aurangabad, India. His area of research includes computer vision, intelligent interactive systems, AVSR, OCR, image processing, pattern recognition and AI.

Antar Shaddad H. Abdul-Qawy was born in Taiz, Yemen on 28 December 1980. He received the B.Sc. degree in computer engineering from Hodeidah University, Yemen, in 2005, the Master of Technology degree in computer science from University of Hyderabad, India, in 2014, and the Ph.D. degree in electronics and communication engineering (Internet of Things) from Kakatiya University, India, in 2019. He is currently an Assistant Professor of information technology with Department of Mathematics and Computer Science, and Dean, Faculty of Science, Sumait University, Zanzibar, Tanzania. He has previously worked as an Assistant Lecturer at Department of Computer Engineering, Faculty of Computer Science and Engineering, Hodeidah University, Yemen from 2005 to 2012. His research interests include the internet of things, wireless sensor networks, sensor cloud, the green IoT, and energy-efficient networks. He is a member of ACM.

Mohammed Ghaleb Almusharref was born in Sana'a, Yemen on 01 January 1980. He received the B.Sc. in Computer Science from Yemen University, Yemen in 2015, and Master of Computer Science from B.A.M University, Anantapur, India in 2020. He is currently a Ph.D. candidate at Department of Computer Science and IT, Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India. His research interests in artificial intelligence, computer vision.