IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 2, September 2024

Blockchain Based Secure File Transfer System with Password Protection

Avinash R. Avhad[1], Pushpak S. Gangad[2], Shubham M. Kharote[3],
Shreyas S. Muntode[4] , Prof. M. D. Sanap[5]
Department of AIML (Artificial Intelligence & Machine Learning)[1,2,3,4,5]
Loknete Gopinathji Munde Institute of Engineering Education & Research (LOGMIEER)s, Nashik, India

Abstract: *The need of secure file transfer systems is higher nowadays. In order to enhance the security and privacy of private information transferred over the internet, our paper presents a blockchain-based secure file transfer system (BSFTS) with password protection. This system takes advantage of the decentralized and immutable properties of blockchain technology to ensure that every file transfer is Safe and Secure, offering verifiable audit trails that can minimize the threats associated with data tampering and unauthorized access.*

Through forcing people to use strong, unique passwords for decryption as well as encryption, the combination of password protection further secures files by ensuring that only specified people may access the information. In addition to enhancing data confidentiality, this dual-layer strategy increases defences against possible cyberthreats, including phishing and brute force attacks.

Research shows that the blockchain-based secure file transfer system with password protection far exceeds standard file transfer techniques in terms of security and user experience. The results illustrate that password protection and blockchain technology work together to build a robust framework for secure file sharing. For companies trying to enhance their data protection plans in the face of changing security threats in the world of technology, this study provides helpful data.

Keywords: Blockchain, Cloud Computing, Data Encryption and Decryption, Tokenisation, Data Security, Password Protection

I. INTRODUCTION

Secure transferring of data has become a fundamental need in the current digital World for both individuals and Organisations. It is more important than ever to protect sensitive data integrity and security during transfer, as data breaches and cyberattacks become more common and complex. Traditional file transfer techniques frequently depend on centralized systems that are vulnerable to manipulation, unauthorized access, and attack. A strong answer to these issues is a blockchain-based secure file transfer system with password protection.

The distributed, transparent, and immutable features of the blockchain system make it a great choice for secure file transfers. This solution ensures secure information transfers that are unable to modification or unauthorized access by using blockchain technology. Moreover, the provision of password protection Give the High level of safety by giving users control over who mayview the data that is being sent.

This approach provides a reliable and secure Solution For transfer important information by combining encryption and Decryption methods of blockchain technology. Users may feel secure understanding that only authorized users can access the data due to the extra level of security provided by passwords. This technique provides verifiable and unbreakable traceability by recording each data transfer on the blockchain, which not only enhances security but also increases transparency in file Transferring system in today’s Digital world.

Using It to the increasing need for safe, effective, and user-controlled data transfer techniques, the Blockchain-Based Secure File Transfer System with Password Protection provide a Valuable solution for current cybersecurity threats.

DOI: 10.48175/IJARSCT-19651

II. LITERATURE SURVE

SR. NO.	TITLE	YEAR	AUTHOR	Discussion
1)	"Blockchain Based, Decentralized Access Control for IPFS"	2018	M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State	In this paper Discussion on the modified version of the Inter Planetary File system (IPFS) that leverages Ethereum smart contracts to provide access-controlled file sharing
2)	"Trustworthy Electronic Voting Using Adjusted Blockchain Technology"	2019	B. Shahzad and J. Crowcroft	Discuss About Secure Pooling Process using effective hashing techniques of Blockchain Technology.
3)	"Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS"	2020	J. Sun, X. Yao, S. Wang and Y. Wu	combined blockchain technology with the decentralized Interplanetary File System (IPFS) to secure the Electronic medical records.
4)	"Blockchain-Based Address Alias System"	2021	Bodziony, Norbert, Paweł Jemioło, Krzysztof Kluza, and Marek R. Ogiela	Creating a cryptocurrency wallet with a full on-chain solution for aliasing accounts and tokens to improve user experience and avoid unnecessary errors in the Network.
5)	“Blockchain-Based Decentralized Storage Design for Data Confidence Over Cloud-Native Edge Infrastructure”	2024	HANNIE ZANG AND JONGWONKIM (Graduate Student Member, IEEE), HO KIM (Senior Member, IEEE)	Discuss on decentralized storage system that melds cloud-native concepts with blockchain technology. The proposed design delivers enhanced scalability, data security, and privacy.

III. METHODOLOGY

A. Blockchain Technology

The blockchain is a decentralized, distributed ledger that Store the data in blocks that are linked together in a chain. Blockchain technology are Popular for their use in cryptocurrency, but they can be used in many other industries or Sectors Now a day.

Features of blockchain technology

- Cryptographic hashes
- Consensus mechanisms
- Decentralization
- Immutability

B. Data Encryption And Decryption

The Encryption and decryption of data are based on cryptography, it is the science of encoding and decoding the information. It is done by using different types of mathematical models called algorithms, which transfer the data's digital content. The sender and recipient use a secret key to encrypt and decrypt that data.

Encryption of data protects data from being stolen, changed, or compromised. It's important to keep the decryption key secret and protected from unauthorized access or user.

Types of Encryptions

1. Symmetric encryption: user Uses the same key for encryption and decryption of data.
2. Asymmetric encryption: sender user Uses a private key for the owner of the data and a public key for the recipient i.e. Receiver User.

C. Password Protection

Password protection is an access control technique that helps keep important information safe from hackers and it can only be accessed by using the right credentials.

D. Tokenisation

It is the process of creating a digital format of a real thing. Tokenization is used to protect sensitive data or information From Generating the Specific token for it.

E. Cloud Computing

Cloud computing is the on-demand availability of computer system and its resources, especially for data storage (cloud storage) and computing power such As data Processing, without direct active management by the user. Large clouds have functionalities to distributed over multiple locations, each of which is a data centre for store the information. Cloud computing relies on sharing of resources to achieve coherence and typically uses a pay-as-you-go model, which can help in reducing cost of time and money but may also lead to unexpected operating expenses for users.

IV. WORKFLOW OF SYSTEM

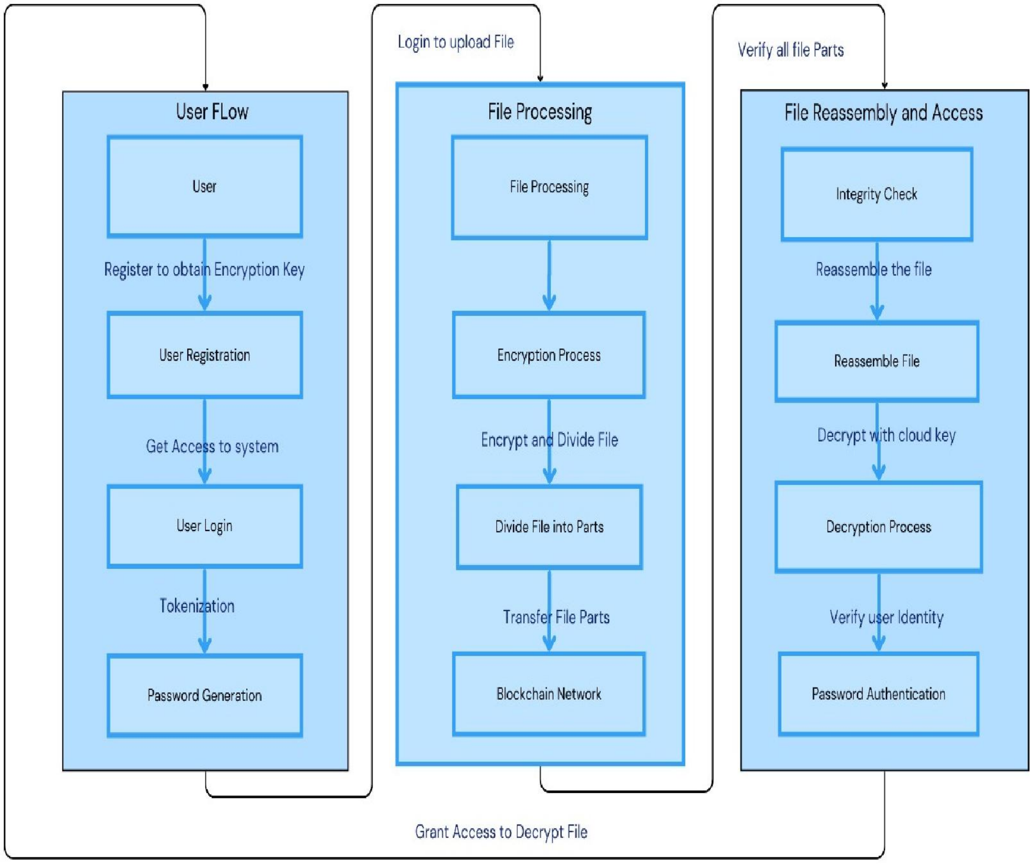

Fig. 1Workflow Of Blockchain Based Secure File Transfer System With Password Protection System

V. PROPOSED SYSTEM

The Blockchain Based Secure File Transfer System with Password Protection isuse For the Transfer the File From one User to Other Without Knowing to Anyone. For Creating This System, The System Architecture Are Describe Below in Fig. 2

The Working of The Blockchain Based Secure File Transfer System with Password Protection Are

- User: first User Resister to the Platform and User Get a Permission to Login After login user The System generate the unique ID for Each User i.e. Token number
- File: After That User select the File from Local System That User Want to Send to Another User
- Encryption: After Selecting the File, The System Start to Encrypt the Given File with The Help of The SHA256 Blockchain Algorithm and At the Last It Convert in To the Small Block of The Blockchain
- Password Protection: After Encryptthe Data And Convert It into The Small Number of Blocks We Needs to Protect or Secure It Using the Password. The System Generate the Half Password from The Token No (i.e. Unique Id) and Pass it To the Cloud

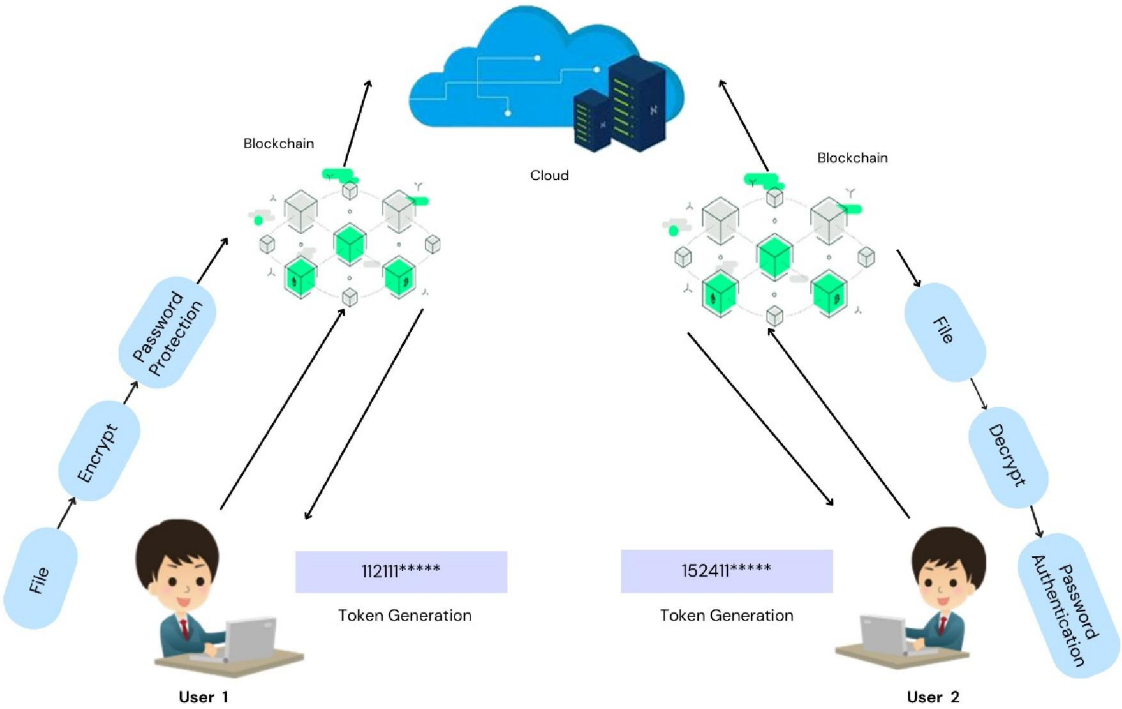

Fig. 2 System Architecture Of Blockchain Based Secure File Transfer System With Password Protection System

- Cloud: In This System the cloud Responsible to Reassemble the password or complete the Half Password and Again Break the Password in To the Two Parts First Part of Password Attachin The Bock of Blockchain And Another half Part of The Password Transfer to Target User in The Form of The Text Attachment and It Transfer It to The Target User
- Decryption: When file reach to the end of the other user Using SHA256 Blockchain Algorithm the Start to Decrypt the Given Data in within the Blockchain Network
- Password Authentication: At The Last When File Reach to Other User End for Access this File the User Needs to Authenticate It Using Require Password Credentials.

VI. CONCLUSION

The Blockchain-Based secure File Transfer System with Password Protection offers a Helpful and cutting-edge solution to the growing challenges related to safe file transfers in the 21st - century. This solution ensures the confidentiality, accessibility, and integrity of important files during transmission by using strong encryption, decryption and password protection, with the decentralized, immutable nature of blockchain technology.

Blockchain technology provides a complete record of all files, ensuring transparency and traceability of file, which decries the chance of unauthorized access of file. Passwords offer an important role of user-controlled authorized users to access data by ensuring that may be sure that only their files.

By providing a highly secure, decentralized solution, this technology effectively overcomes the weaknesses of standard, centralized file transfer techniques. It provides the scalable and modular architecture t.e. Ensures that it is easily expanded to meet changing cybersecurity requirements in the future. Some possible improvements include multi-factor authentication, smart contracts, OTP Authentication, Face recognition System and more advanced data Security techniques.

Finally, it should be noted that the Blockchain-Based secure File Transfer System with Password Protection is a Useful and modern method for safe file transferring that is perfect for businesses and all other Sectors That improve security, privacy, and authority over their digital data.

VII. ACKNOWLEDGMENT

We express our heartfelt gratitude to our esteemed mentors and professors, especially Prof. M. D. Sanap, for their invaluable guidance in our academic and project endeavours. We also extend our thanks to the AIML Engineering Department and its staff for their continuous support. We're indebted to Prof. M. D. Sanap for his encouragement and insights. Our sincere thanks go to Dr. K.V. Chandratre, Principal of Loknete Gopinathji Munde Institute of Engineering Education & Research, Nashik, for his support and permission to complete this project. We appreciate the assistance of our department's support staff, and we're grateful to our parents, friends, and all those who supported us throughout this project.

REFERENCES

[1]. Hannie Zang And Jongwonkim,(Graduate Student Member, Ieee), Ho Kim,(Senior Member, Ieee) "Blockchain-Based Decentralized Storage Design for Data Confidence Over Cloud-Native Edge Infrastructure", School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, Republic of Korea ,Artificial Intelligence Graduate School, Gwangju Institute of Science and Technology, Gwangju 61005, Republic of Korea

[2]. Anusree K, Jagan Sathiaseelan Vadekkat, Abhinu R Dev, Abhinav, "Decentralized File Transfer System Blockchain-based File Transfer", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 11 Issue 05, May-202,2

[3]. Bodziony, Paweł Jemioło, Krzysztof Kluza Marek R. Ogiela, "Blockchain-Based Address Alias System", Journal of Theoretical and Applied Electronic Commerce Research - Norbert Bodziony, N.; Jemioło, P.; Kluza, K.; Ogiela, "Blockchain Based Address Alias System" J. Theor. Appl. Electron. Commer. Res. 2021

[4]. JIN SUN, XIAOMIN YAO , SHANGPING WANG, YING WU, "Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS" School of Science, Xian University of Technology, Xi an 710054, China.

[5]. BASIT SHAHZAD, JON CROWCROFT, "Trustworthy Electronic Voting Using Adjusted Blockchain Technology", Department of Engineering, National University of Modern Languages, Islamabad 44000, Pakistan and Computer Laboratory, University of Cambridge, Cambridge CB3 0FD, U.K.

DOI: 10.48175/IJARSCT-19651