International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0141
e ISSN: 2584-2854
Volume: 03
Issue:03 March 2025
Page No: 870-874

Blockchain Based Secure File Transfer System with Multi Factor Authentication

Avinash R. Avhad [1], Shubham M. Kharote [2], Pushpak S. Gangad [3], Shreyas S. Muntode [4], Prof. M. D. Sanap [5], Prof. P. B. Rajole [6]

[1,2,3,4]UG Scholar, Dept. of AIML, Loknete Gopinathji Munde Institute of Engineering Education & Research., Nashik, Maharashtra, India.

[5,6]Associate professor, Dept. of AIML, Loknete Gopinathji Munde Institute of Engineering Education & Research., Nashik, Maharashtra, India.

Email ID: *avinashavhad491@gmail.com[1], kharoteshubham2003@gmail.com[2], pushpakgangad1916@gmail.com[3], shreyasmuntode@gmail.com[4]*

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 Multi Factor Authentication. 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 multi factor authentication 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 multi factor authentication far exceeds standard file transfer techniques in terms of security and user experience. The results illustrate that multi factor authentication 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, Data Encryption and Decryption, Tokenisation, Data Security,Multi Factor Authentication,Face Recognition.*

1. 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 Multi Factor Authentication. The distributed, transparent, and immutable features of the blockchain system make it a great choice [1-3] 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 multi factor authentication Give the High level of safety by giving users control over who may view 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 multi factor authentication i.e. Two factor authentication,face recognition. This technique provides verifiable and unbreakable traceability by

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0141
e ISSN: 2584-2854
Volume: 03
Issue:03 March 2025
Page No: 870-874

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 Multi Factor Authentication provide a Valuable solution for current cybersecurity threats. [4]

2. Methodology

2.1. 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. [5]

Features of blockchain technology

1. Cryptographic hashes
2. Consensus mechanisms
3. Decentralization
4. Immutability

2.2. 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. [6]

Types of encryptions

- Symmetric encryption: user Uses the same key for encryption and decryption of data.
- 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.

2.3. 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. [7]

2.4. 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.

2.5. Multifactor Authentication

(MFA) is a security mechanism that requires users to verify their identity using multiple authentication factors before gaining access to a system, application, or account. MFA enhances security by ensuring that even if one factor is compromised; unauthorized access remains difficult. (Figure 1)

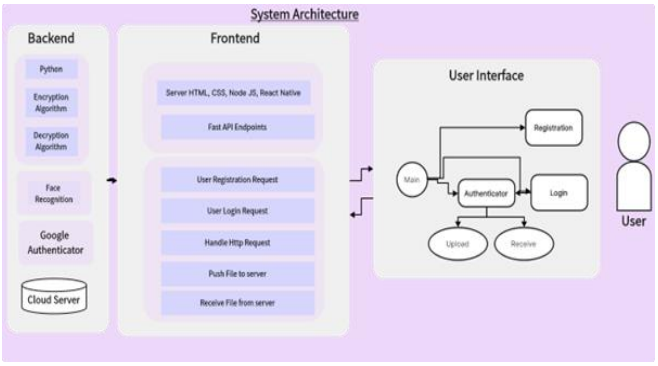

Figure 1 System Architecture

Results and Discussion

The result should include the files send by the user with accurate datatype. The received file should be reassembled from the blockchain without any tampering to the data, because secure and reliable file transfer is the main feature of our application and the multiple authentication algorithms help safeguard the data from unauthorized users and prevent tampering during transaction. There is no limit on the size of the file because of chunking algorithm so there should be no changes in the metadata of received file. (Figure 1)

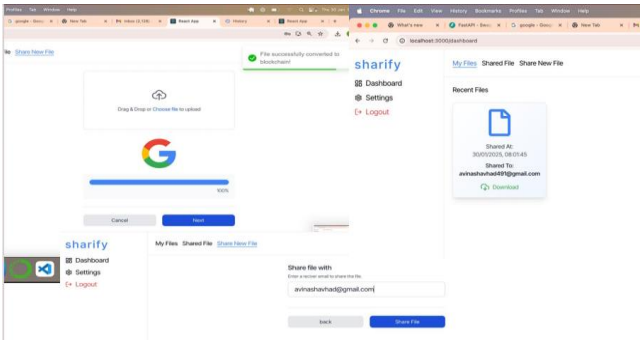

Figure 1 Main UI

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0141
e ISSN: 2584-2854
Volume: 03
Issue:03 March 2025
Page No: 870-874

Table 1 Author & Title

S. No.	Title	Year	Author
1)	"Blockchain Based, Decentralized Access Control for IPFS"	2018	M. Steichen, B. Fiz, R. Norvill, W. Shbair and R. State
2)	"Trustworthy Electronic Voting Using Adjusted Blockchain Technology"	2019	B. Shahzad and J. Crowcroft
3)	"Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS"	2020	J. Sun, X. Yao, S. Wang and Y. Wu
4)	"Blockchain-Based Address Alias System"	2021	Bodziony, Norbert, Paweł Jemioło, Krzysztof Kluza, and Marek R. Ogiela
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)
6)	Blockchain Based Secure File Transfer System with Password Protection,	2024	Avinash Shubham Shreyas Pushpak

Discussion

The proposed blockchain-based secure file transfer system ensures data integrity, reliability, and authentication through a multi-factor authentication (MFA) mechanism. The system employs a chunking algorithm to divide large files into fixed-size segments, each securely hashed and stored in a decentralized network such as IPFS. By leveraging cryptographic hash functions and the system guarantees tamper-proof data reassembly while preserving the original metadata. The blockchain records immutable transaction logs, ensuring transparency and security. The integration of MFA prevents unauthorized access, mitigating security risks. This approach aligns with IEEE security standards, offering a scalable and robust file transfer solution. (Figure 2)

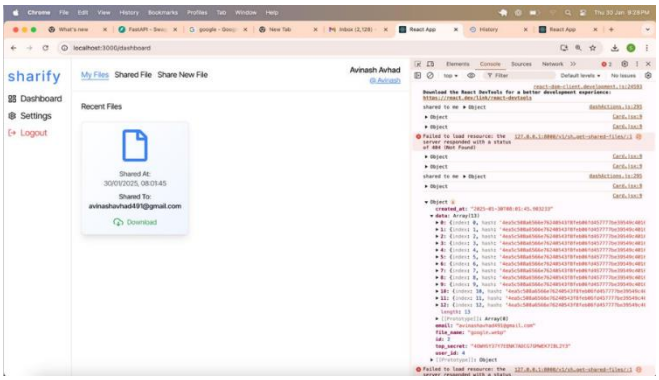

Figure 2 File Received with Blockchain Data

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0141
e ISSN: 2584-2854
Volume: 03
Issue:03 March 2025
Page No: 870-874

Conclusion

The Blockchain-Based Secure File Transfer System with Multi-Factor Authentication provides an innovative solution to modern cybersecurity challenges. By leveraging blockchain's decentralized and immutable nature, the system ensures data security, transparency, and integrity during file transfers. Cryptographic encryption and decryption techniques protect sensitive data, preventing unauthorized access and ensuring only verified users can retrieve files. Smart contracts further enhance security by automating secure transactions and preventing data tampering. Multi-factor authentication plays a crucial role in strengthening access control by requiring multiple verification methods, such as passwords, biometrics, or security tokens. This significantly reduces risks associated with credential theft and unauthorized access. Additionally, blockchain's permanent ledger maintains an auditable transaction record, ensuring compliance with cybersecurity standards while providing a transparent file access history.

The system's scalability and modularity make it suitable for various industries, overcoming the limitations of centralized file transfer methods. Unlike traditional systems prone to security vulnerabilities, this decentralized approach provides a resilient infrastructure for secure file exchange. Future enhancements could include advanced encryption techniques, AI-driven threat detection, and quantum-resistant cryptography to further improve security. In summary, this blockchain-based system with multi-factor authentication offers a highly secure, reliable, and scalable method for digital file transfers. By addressing conventional file transfer weaknesses, it sets a new standard for data security, ensuring privacy, integrity, and control over digital assets in an evolving cybersecurity landscape.

Acknowledgements

We express our heartfelt gratitude to our esteemed mentors and professors, especially Prof. M. D. Sanap and Prof. P. B. Rajole 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 and Prof. P. B. Rajole 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]. Blockchain Based Secure File Transfer System with Password Protection, https://www.ijarsct.co.in/Sep4i2.html DOI: 10.48175/IJARSCT-19651

[2]. Hannie Zang And Jongwonkim,(Graduate Student Member, Ieee), Ho Kim,(Senior Member, Ieee) "Blockchain-Based Decentralized Storage Design for Data

[3]. 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

[4]. 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

[5]. 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

[6]. 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,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0141
e ISSN: 2584-2854
Volume: 03
Issue:03 March 2025
Page No: 870-874

Xi an 710054, China.

[7]. 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.