IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907009 |

Blockchain Based Secure Data Storage and Access Control System Using IPFS

Shete Kajal Bharat[1], Prof. Monika Rokade[2]

[1]PG Student, Sharadchandra Pawar College of Engineering, Junnar, Pune, India

[2]Assistant Professor, Sharadchandra Pawar College of Engineering, Junnar, Pune, India

ABSTRACT: Today's cloud storage is entirely reliant on major storage providers. These storage providers function as untrustworthy third parties, transacting data for the purposes of storing, delivering, and receiving data from a company. This paradigm has a variety of drawbacks, including high operational costs, data availability, and data security. In this paper, we provide a prototype of a multi-user system for dataset access management that employs blockchain technology to enable secure distributed data storage. The data owner can upload the data to the system via a Web Portal. So, only the user who possesses the secret key to a specific file that was uploaded to the Cloud in encrypted form can access it. Finally, the solution protects data privacy by maintaining the blockchain's mutability by keeping it in the cloud. To harden the security of cloud storage, we presented a blockchain-based secure data storage and access management system.

KEYWORDS: Blockchain**,** IPFS Distributed Cloud, SmartContract, Encryption, Decryption.

I.INTRODUCTION

Enormous companies have had a hurdle in keeping large amounts of data in the modern era. As a result, several businesses have resorted to cloud storage, which offers great data storage, sharing, and transfer capabilities. The key issues that cloud computing has to deal with are data confidentiality and integrity, as well as data security. The majority of consumers choose to save their personal data in the cloud. However, there are potential security issues as well as a copyright issue with the material. The main issue with transmitting data to the external environment is that it can be accessed by anybody other than the owner. Cloud providers do not provide the level of security and privacy that is essential for proper data security and privacy. There are few tools and strategies available to protect data stored on cloud servers at the moment.

To address this issue, this paper describes a system that uses a block chain-based Secure Data Storage and Access System to store and access data. In this work, we propose that Block chain be used as a trusted environment to improve cloud storage security and guard against exploitation attempts.

A blockchain is a tamper-resistant and decentralised distributed database that tracks transactions over a peer-to-peer public or private network. The ledger, which is distributed to all network members, permanently stores transactional data between nodes in an ordered chain of cryptographic hash-linked blocks. The block chain term comes from the fact that all authenticated and approved transaction blocks are associated and linked to the key current block from the beginning of the chain. As a result, the block chain serves as a single source of truth, and all members of a block chain network can only see transactions that they are allowed to see. [1] A blockchain is a technology that enables all participants to maintain a ledger including all transaction data and to upgrade their ledgers to ensure integrity when a new transaction occurs. The single point of failure resulting from overdependence on an approved third party has been resolved as the growth of the Internet and encryption technology has allowed all participants to validate a transaction's validity. A blockchain is a distributed ledger that is used to keep a permanent, tamper-proof record of transactional data.

The blockchain is a structured list that holds data in a distributed database-like format and is designed to be impossible to change arbitrarily because the blockchain is saved and validated by network participants. A header and a body are included in each block. The previous and existing blocks' hash values, as well as the nonce keys, are stored in the header. The index method is used to check the block data in the database. It is extremely difficult to fake and manipulate the registered data since the hash values recorded in each peer in the block are influenced by the parameters of the preceding blocks. [2].

II. LITERATURE SURVEY

The Blockchain's transparency is achieved through the transaction copying mechanism. Each transaction is duplicated to either computer in the Blockchain network, as stated above. Every member has access to all transactions, which means that any activity is visible to all Blockchain participants. [3]

Smart Contracts are executable code that runs on the blockchain to enable, execute, and enforce the terms of a contract between untrustworthy parties. A smart contract's principal goal is to automatically carry out the terms of an agreement once

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907009 |

certain criteria are met. As a result, smart contracts offer lower transaction fees than traditional systems that rely on a trusted third party to enforce and execute an agreement's provisions. There are several blockchain platforms on which smart contracts can be built, but Ethereum is the most popular. This is due to Ethereum's language's Turing-completeness characteristic, which allows for more complicated and customised contracts to be created. [4]

Mr. Anup R. Nimje, Prof. V. T. Gaikwad, and Prof. H. N. Datir [5] compared seven different attribute-based encryption techniques, namely ABE, KP-ABE, EKP-ABE, CP-ABE, CP-ASBE, HIBE, HABE, and HASBE, and came to the conclusion that Hierarchical attribute-based encryption (HASBE) provides the best access control It is more flexible and efficient than previous approaches, with less calculation overhead. The HASBE method employs a delegation algorithm to create a hierarchical structure of system users. Due to flexible and resilient attribute set combinations, the HASBE system supports compound attributes and achieves quick user revocation due to attributes assigned multiple values.

More from Pooja [6] presented an Attribute-based Key Aggregate Cryptosystem for cloud data security. To search the document stored on the cloud, the system employs a trapdoor key and searchable keywords. Once the document has been fetched, the aggregate key is used to decrypt and download a specific document from the pool of documents. The trapdoor key is open to the public for a specific group, but aggregate key access is determined by the data owner's attributes. The system employs the CP-ABE method with a fixed size of ciphertext and key, which improves performance by forming two independent files, one for the key and the other for the set of characteristics, rather than tying user attributes to akey.

Ilya Sukhodolskiy and Sergey Zapechnikov [7] presented a blockchain-based cloud storage access control system. It offers a method for accessing data kept in untrustworthy environments, such as cloud storage. Data such as multimedia content, documents, and other types of data will be saved in cloud storage, with metadata identifying the file available only on the blockchain. Because the data kept in blockchain is public, it is encrypted before being sent to storage and access is controlled. To read a file, the user must fit the access policy and have the requisite keys to decrypt and download it. The owner of the data provides the decryption keys. The following are some of the key advantages of an access control system: the ability to create dynamic access policies, the ability to customise the access policy for encrypted data without duplication, the fact that changing the access policy does not necessitate additional actions from other members, and the fact that the user keys remain unchanged. The use of blockchain and smartcontracts ensures the integrity and secrecy of information about all transactions, including granting and altering access, facts obtain access to file, fact rejection, and the inability to edit and amend these data.

When writing smart contracts in Solidity, Maximilian Wöhrer and Uwe Zdun [8] identified six design patterns to handle security issues: rate limit pattern, speed bump pattern, mutex pattern, balancing pattern, check-effects-interaction pattern, and emergency stop pattern. These patterns address the absence of execution control that occurs once a contract is launched as a result of Ethereum's distributed execution environment. This unique feature of Ethereum allows programmes on the blockchain to run independently, but it also has consequences. These flaws manifest themselves in a variety of ways, including as harmful callbacks, ineffective callbacks, and ineffective callbacks, adverse circumstances on how and when functions are executed, or uncontrollably high financial risks at stake. By applying the presented patterns, we can address the sesecurity problems and mitigate typical attacks cenarios.

Monika Rokade and Yogesh Patil [11] proposed a system deep learning classification using nomaly detection from network dataset. The Recurrent Neural Network (RNN) has classification algorithm has used for detection and classifying the abnormal activities. The major benefit of system it can works on structured as well as unstructured imbalance dataset.

The MLIDS A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset has proposed by Monika Rokade and Dr. Yogesh Patil in [12]. The numerous soft computing and machine learning classification algorithms have been used for detection the malicious activity from network dataset. The system depicts around 95% accuracy ok KDDCUP and NSLKDD dataset.

Monika D. Rokade and Yogesh Kumar Sharma [13] proposed a system to identification of Malicious Activity for Network Packet using Deep Learning. 6 standard dataset has sued for detection of malicious attacks with minimum three machine learning algorithms.

Sunil S. Khatal and Yogesh kumar Sharma [14] proposed a system Health Care Patient Monitoring using IoT and Machine Learning for detection of heart and chronic diseases of human body. The IoT environment has used for collection of real data while machine learning technique has used for classification those data, as it normal or abnormal.

Data Hiding In Audio-Video Using Anti Forensics Technique For Authentication has proposed by Sunil S.Khatal and Yogesh kumar Sharma [15]. This is a secure data hiding approach for hide the text data into video as well as image. Once sender hide data into specific objects while receivers does same operation for authentication. The major benefit of this system can eliminate zero day attacks in untrusted environments.

Sunil S.Khatal and Yogesh Kumar Sharma [16] proposed a system to analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. This is the analytical based system to detection and prediction of heart disease from IoT dataset. This system can able to detect the disease and predict accordingly.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907009 |

III.PROPOSED SYSTEM

Cloud computing is one of the most important and beneficial technologies in today's world. Cloud storage is a digital storage solution that stores data safely across several servers in different locations. Cloud storage has expanded in popularity in recent years, and it has become a direct competitor to local storage. Cloud computing has evolved into a promising computing paradigm that is hosted by a variety of third-party service providers. The cloud provides a data storage solution that allows data owners to store their data in the cloud and grant access to businesses that require it.

1. Data privacy
You don't want anyone to have access to your data unless you give them permission. The ability of an individual or a group to separate them or selectively share information about themselves is known as privacy. It also allows consumers to control their data when it is stored and managed in the cloud, preventing theft, unlawful use, and selling. When you save data locally, this is simple to maintain, but what about in the cloud? Because your data is stored in multiple locations, it may be difficult to determine how secure it is. When you don't manage the servers where it's stored, how can you be sure no one can access it? Be careful that migrating sensitive data to the cloud may result in the loss of important privacy measures.

2. Lack of control
When you entrust data storage to a third party, you relieve yourself of a significant amount of responsibility. However, this is a two-edged sword. On the one hand, you will not be responsible for data management; on the other hand, someone else will. If your storage provider experiences problems, such as outages or virus infections, it will have a direct impact on your data access. You'll have to rely on the service provider to resolve the problems. The longer your data is exposed to the elements, the more dangerous it becomes.

3. Dataleakage
Making ensuring no one outside your organisation tries to access your data is a big aspect of safe data storage. Another aspect is ensuring that your data is not sent to anyone outside your company. Data leaking can be problematic since it exposes business-critical or confidential data to outside parties.

4. Data Breaches
These are the results of an assault or a worker's negligence and error. On cloud systems, this is the most common source of concern. Information breaches can also be caused by flaws in the implementation or insufficient safety practises. Employees may use their personal devices or laptops to log into cloud services, exposing the scheme to targeted attacks. The information includes personal health information, financial information, personally identifying information, trade secrets, and intellectual property that is not meant for public publication.

5. System Vulnerabilities
System vulnerabilities may exist in cloud computing devices, particularly in networks with complex infrastructures and a variety of third-party apps. Once a vulnerability has been discovered using a common third-party system, it can be easily exploited by hackers.

IV. ANALYSIS OFALGORITHM

AES
The AES algorithm is a block cipher that operates on an input block of data of a concise and outputs a block of data of the same size. The AES algorithm also requires an input key as a parameter. It supports three distinct key lengths of 128,192, and 256 bits, as well as data lengths of 128,192, and 256 bits. The AES algorithm is a symmetric key algorithm, which means it encrypts and decrypts data with the same key. Furthermore, the AES algorithm generates cipher text that is the same size as plain text data. We use the AES256 encryption technique in our system. We developed a collection of text files that were less than or equal to 6MB in size to examine the data saved in the cloud.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907009 |

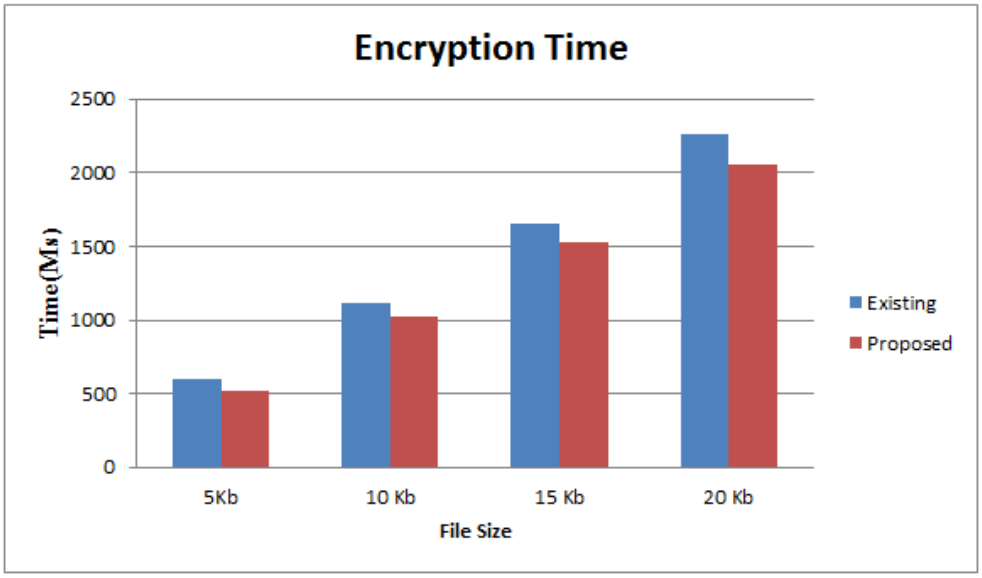

Figure 1: Data encryption performance base on file data size

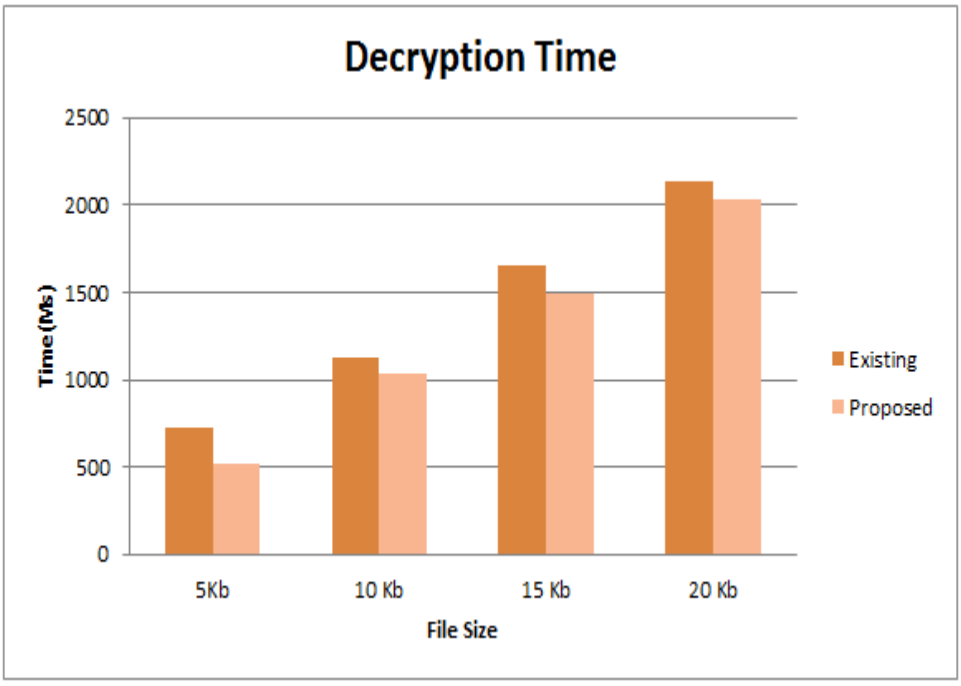

Figure 2: Data decryption performance base on file data size

V. CONCLUSIONS

The proposed method proposes a prototype of a secure IPFS cloud storage system based on block chain technology. The proposed approach protects data kept in untrustworthy contexts. Some security algorithms with suitable time complexity, functionality, and efficiency have been chosen to create the system. The information identifying the file will only be available on the block chain, and the data will be stored in the cloud. AES256 encryption is used in the suggested model. To protect the document by encrypting it. Because the data kept in a block chain is public, it is encrypted before being sent to storage, and access to it is controlled. To decrypt and download a document, the data owner's encryption key is used.
The findings of the study and evaluation show that the suggested model can be used to construct a realistic data sharing platform based on public cloud storage.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907009 |

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE International Conference on Big Data (Bigdata congress), 2017.
[2] Jin Ho Park and Jong Hyuk Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions", Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech) 01811, Korea, 18 August2017. [3] Julija Golosova, Andrejs Romanovs**, "**The Advantages and Disadvantages of the Blockchain Technology", IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)**,**2018**.**
[4] Maher Alharby and Aad van Moorsel, "Blockchain-Based Smart Contracts: A Systematic Mapping Study", Fourth International Conference on Computer Science and Information Technology(CSIT), 2017.
[5] Mr. Anup R. Nimje, Prof. V. T. Gaikwad, Prof. H. N. Datir, "Blockchain Attribute-Based Encryption Techniques in Cloud ComputingSecurity:AnOverview",InternationalJournalof Computer Trends and Technology, Volume 4, Issue 3-2013.
[6] Pooja More, **"**Cloud data security using attribute-based key-aggregate cryptosystem**",**International Conference on Wireless Communications, Signal Processing andNetworking (WiSPNET), 2016.
[7] Ilya Sukhodolskiy, Sergey Zapechnikov, "A Blockchain-Based Access Control System for Cloud Storage," IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2018.
[8] Maximilian Wöhrer, Uwe Zdun, " Smart contracts: Security patterns in the ethereum ecosystem and solidity", International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018.
[9] Naresh vurukonda, B.Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing", 2nd International Conference on Intelligent Computing, Communication & Convergence,2016.
[10] H. Khali, MIEEE, R. Mehdi, A. Araar, "A System-Level architecture For Hash Message Authentication Code", 12th IEEE International Conference on Electronics, Circuits and Systems,2005.
[11] Monika D.Rokade ,Dr.Yogesh kumar Sharma,"Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic." IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719
[12] Monika D.Rokade ,Dr.Yogesh kumar Sharma"MLIDS: A Machine Learning Approach for Intrusion Detection for Real Time Network Dataset", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE
[13] Monika D.Rokade, Dr. Yogesh Kumar Sharma. (2020). Identification of Malicious Activity for Network Packet using Deep Learning. International Journal of Advanced Science and Technology, 29(9s), 2324 - 2331.
[14] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Health Care Patient Monitoring using IoT and Machine Learning.", IOSR Journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN (p): 2278-8719
[15] Sunil S.Khatal ,Dr.Yogesh kumar Sharma, "Data Hiding In Audio-Video Using Anti Forensics Technique ForAuthentication ", IJSRDV4I50349, Volume : 4, Issue : 5
[16] Sunil S.Khatal Dr. Yogesh Kumar Sharma. (2020). Analyzing the role of Heart Disease Prediction System using IoT and Machine Learning. International Journal of Advanced Science and Technology, 29(9s), 2340 - 2346.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details