International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

SECURING HOSPITAL DATA WITH BLOCKCHAIN AND AI

I.S HARSHITHA YADAV, KANDALA SREEJA, GOGU NAGARAJU

CSE Department,

Sreenidhi Institute of Science And Technology

Under the guidance of

Dr. CH. NIRANJAN KUMAR

PROFESSOR

CSE Department, Sreenidhi Institute of Science And Technology

---

Abstract - In this project, we aim to develop methods to protect the private data(the details of the patient)with high security by using Blockchain technology and Artificial Intelligence. Blockchain technology is a decentralized, distributed ledger technology that records the transactions in various computers and have the advantage of transparency, immutability and smart contracts. Data is the key resource for the wide emerging information-based technology. Data like customer preference, user's details, location and many more are collected and are used by big businesses and companies. The owner of the data is unaware of who is using their data and there is lack of privacy. The data can also be misused and there is a potential risk for the data owners with the traditional systems. With the powerful combination of Blockchain with AI, we can ensure there is security of the data. In this project, we are focusing on the hospital sector, wherein the data provided by the patients will be stored with high security by recording them as blockchains (with strong hashcodes). The patient can control on to whom they want to share their data. The data is highly secure and the data owners can benefit from also the incentives. We develop a web application using Django through which patients register themselves and create the profile with their data and also select the Hospital to which they want to give access. Hospital logins and they can get the data for which they have the access . MYSQL is used as an python interface to connect the databases.

***Key Words*:** Blockchain, Artificial Intelligence, data security, hash, proof of work

1.INTRODUCTION

In today's data driven technology, data is the key resource for information utilized by big businesses and organizations. This data is collected from its owners and there is a risk of privacy of data. The new algorithms used by the corporates are secretly collecting huge amounts of data like customer preferences, user details, location etc. which leads to threat of the privacy of the owner of the data. On the other hand, the data owners have no idea on how the data is used and is used by who as there is no reliable method of recording the data. As a result, there are a very few ways to locate or punish those who misuse the data. Once the data is obtained by the third parties, the data owners can't manage the risks associated with it. Therefore, the absence of a reliable efficient ways to collect the data poses the potential risks for the privacy of data owners. If there is an efficient way of recording the data, then the performance of AI will be significant be improved and will have huge benefits and exceed the capabilities of the humans. Hence , we propose the use of Blockchain technology to efficiently record the data thereby enhancing the security of the data. Through this the data owners can choose with whom they want to share the data. Through this the data sharing is trusted and secure. Through Blockchain there is a guarantee for tamper-proof methods of data sharing and with the benefit of monetary incentives! Therefore, we aim at providing efficient ways of data sharing by combining Blockchain and artificial intelligence together and significantly enhancing data security.

2. Existing System

In the existing systems, there is no effective way of data security. Data collected from various resources like customer data , preferences, confidential data, location etc. was used by various third party organizations for their businesses without the consent of its owners. This leads to misuse of data. There was no privacy. Though there are AI algorithms which give good performance of data analysis , but the data is insecure. Existing system uses simple data storage and no advanced security feature.

Disadvantages of existing system:

- Less security
- Data tampering
- Less privacy

3.Proposed System

The proposed system uses blockchain combined with AI. Through blockchain there is high security. Data collected is stored as blockchains which have unique hashing techniques. The blockchain technology the chances of data tampering is very low as the each blockchain as a previous hash too which means that the intruder gets a high task of changing all the previous hashes which is very tough and high time consuming denoting the unsuccess of data tamper. Thus, this methodology has a secure networking paradigm. Through this system there is secure data storage,sharing and computing. Data ownership is guaranteed with use of Blockchain. Artificial intelligence based secure computing is a appreciated work and incentives benefits is the other advantage of the blockchain technology.

Advantages:

- High advances Security.
- High accuracy.
- Incentive based.
- Data privacy.
- Data ownership guarantee.

Requirements

Software Requirements:

Programming Language used: Python

Operating System: Windows

IDE: Visual Studio Code

Web framework: Django

Languages used: Python , Javascript, HTML, CSS

Packages required:

Django 2.1.7

Mysqlclient: Version 1.4.3 or greater.

PyMySql: Version 0.9.3

Database: MySql

Hardware Requirements

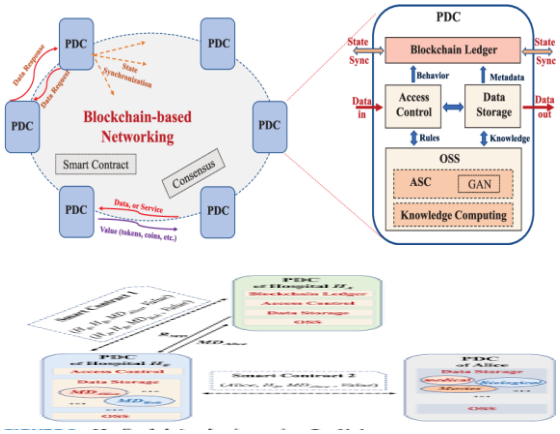
Hard disk

RAM: 2GB

Good processor: Intel

Speed: 2.53GHZ

4. System Architecture



Securing hospital data using a combination of blockchain and AI involves leveraging the strengths of both technologies to create a robust and secure system architecture. Here's a high-level overview of how such a system could be designed:

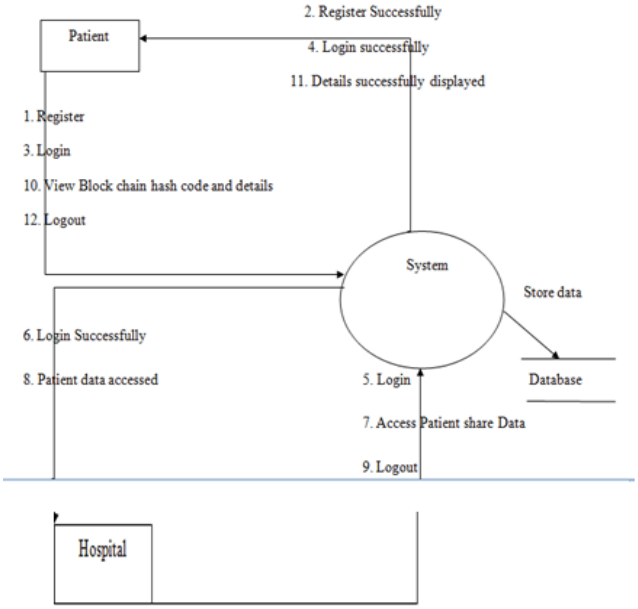
1.Data Encryption and Access Control:

- Patient data is encrypted to ensure confidentiality. Encryption keys are securely stored.
- Access control mechanisms are implemented to restrict data access based on user roles and permissions.
- AI algorithms can be employed for advanced authentication methods such as biometrics or facial recognition.

2.Blockchain for Data Integrity and Auditability:

- Utilize a private or permissioned blockchain network for storing and managing hospital data.
- Each transaction or update to the data is recorded as a transaction on the blockchain, ensuring immutability and tamper resistance.
- Blockchain-based smart contracts can enforce data access rules and automate consent management.

5.Data flow diagram



Data flow diagram represents the flow of the process.

1. The first step is to register by the patient.
2. Next the system ensures that the account created successfully.
3. The third step is the patient logins from its system.
4. Login is successful
5. The hospital logins.
6. Login is successful ensured by system.
7. The hospital access the patient data by searching.
8. Patient data displayed.
9. Hospital log outs.
10. The patient can check for its hash code and incentives.
11. Details are successfully shown by system.
12. The patient logs out.

METHODS AND IMPLEMENATION

A django web framework is used to develop the website to collect the data. With this application the registered patients can share he data. Blockchain technology is used for data storage. Every blockchain has the data , a unique string hash, a previous hash and proof of work. With the previous hashes all the blocks are connected together and hence data cant be breached. Using artificial intelligence the computing is done. In this way, data is stored. The hospital also registers and uses the application. So data is requested and responded. The patients can decide who can access the data so there is also access control in the system.

In this project, we develop a website using Django framework, javascript, HTML, CSS. The various web pages that are created are Home Page, Hospital login page,patient login page, patient share data access screen, patient create profile page, view data page.

Home page/ index page : It is the landing page and has modules like patient login, hospital login, Create profile, patient share data access page

Create Profile page: This page is used for registeration. It takes the input of various details and the data is stored as tables in MySQL.

Hospital page: The page is used for hospital login with username and password.

Hospital Login page: If the hospital has successfully login ,then the welcome page is displayed.

Access data page: Through this page, hospital can access the data which is given access to them. The search string is to be given and the patient details and the problem details will be displayed.

Patient page: Patient can login through this page by patient ID.

Patient Login : The patient can view their data and check their hash code and incentives.

Patient data access page: Dispalys the patient details if it is accessible or else empty table.

Create profile data page: When the profile is created , we get a completed message in this page.

BLOCKCHAIN

Blockchain technology is a decentralized and distributed ledger system that enables the secure recording, verification, and storage of data across a network of computers. It was originally introduced as the underlying technology behind Bitcoin, a digital cryptocurrency, but has since expanded its applications to various industries beyond finance. Here are some key aspects and characteristics of blockchain technology:

1.Decentralization: Blockchain operates as a decentralized network, meaning it doesn't rely on a central authority or intermediary for data storage and verification. Instead, multiple participants (nodes) in the network maintain and validate the blockchain collectively.

2.Distributed Ledger: The blockchain ledger consists of a chain of blocks, where each block contains a list of

transactions or data. The ledger is replicated and distributed across all participating nodes, ensuring transparency and redundancy.

3.Security and Immutability: Transactions or data recorded on the blockchain are secured using advanced cryptographic techniques. Each block contains a hash value that links it to the previous block, forming an immutable chain. Once data is added to the blockchain, it becomes extremely difficult to alter or tamper with.

4.Consensus Mechanisms: Blockchain networks use consensus algorithms to achieve agreement on the state of the blockchain across multiple nodes. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). These mechanisms ensure that all participants in the network agree on the validity of transactions and the order in which they are added to the blockchain.

5.Transparency and Auditability: Blockchain provides transparency by allowing all participants to view and verify the transactions and data stored on the blockchain. The distributed nature of the ledger ensures that records are difficult to manipulate, providing an auditable and trustworthy system.

6.Smart Contracts: Smart contracts are self-executing contracts with the terms and conditions directly written into code on the blockchain. They automatically execute actions when predefined conditions are met, eliminating the need for intermediaries and enabling trustless and automated transactions.

7.Use Cases: Blockchain technology has found applications in various industries, including finance, supply chain management, healthcare, voting systems, real estate, and more. It enables secure and efficient data management, improved transparency, reduced fraud, and streamlined processes across different sectors.

8.Challenges: While blockchain offers numerous advantages, there are challenges to consider, including scalability, energy consumption (in the case of PoW consensus), regulatory and legal considerations, interoperability between different blockchain networks, and privacy concerns.

Overall, blockchain technology provides a decentralized, secure, and transparent way of recording and managing data. Its potential to transform industries and establish new trust and efficiency models has led to widespread interest and exploration of its applications.

SHA-256 Algorithm in blockchain

The SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function widely used in blockchain technology, including popular blockchain networks like Bitcoin and Ethereum. It is an integral part of the consensus mechanism and ensures the integrity and security of the data stored on the blockchain. Here's an overview of the SHA-256 algorithm and its role in blockchain:

Hash Function:SHA-256 is a one-way hash function that takes an input (data) of any size and produces a fixed-size output (hash value) of 256 bits.

- It is deterministic, meaning that the same input will always produce the same output.
- The hash function is designed to be computationally expensive and computationally infeasible to reverse-engineer or find collisions (different inputs producing the same hash).

Data Integrity:

- In blockchain, each block contains a reference (hash) to the previous block's hash, forming a chain of blocks.
- SHA-256 is used to calculate the hash of each block, including the data within the block and the hash of the previous block.
- This chaining mechanism ensures the integrity of the blockchain since altering the data in a block or any previous block will change the hash value, and subsequent blocks will no longer reference it correctly.

Proof of Work (PoW) Consensus:

- In many blockchain networks like Bitcoin, SHA-256 is used in the Proof of Work (PoW) consensus algorithm.
- Miners compete to solve a computationally intensive mathematical puzzle (mining) by finding a nonce (a random number) that, when combined with the block data, produces a hash value below a certain target threshold.
- Miners repeatedly perform SHA-256 computations by modifying the nonce until a valid solution (hash value below the target) is found.
- The successful miner's block, along with the correct nonce, is added to the blockchain, and other nodes can easily verify the solution by performing the same SHA-256 calculation.

Data Integrity Verification:

- Any participant in the blockchain network can independently calculate the SHA-256 hash of a block and compare it with the stored hash value to verify the integrity of the block.

- This ensures that the stored data has not been tampered with since any modification would result in a different hash value.

The SHA-256 algorithm is critical for maintaining the immutability, integrity, and security of data stored in a blockchain. Its cryptographic properties make it a suitable choice for generating secure and unique hash values, enabling consensus, and providing data integrity verification mechanisms within a blockchain network.

CONSENSUS MECHANISM:

A consensus mechanism is a set of rules and protocols employed by blockchain networks to achieve agreement among participants on the state of the blockchain. It ensures that all nodes in the network reach a consensus on the validity and order of transactions, the addition of new blocks, and the overall network rules. Consensus mechanisms are crucial for maintaining the integrity, security, and decentralized nature of blockchain networks. Here are some commonly used consensus mechanisms:

Proof of Work (PoW):In PoW, miners compete to solve complex mathematical puzzles by performing computationally intensive calculations.The miner who successfully solves the puzzle first adds the next block to the blockchain.PoW requires a significant amount of computational power and energy consumption, as miners need to find a nonce that results in a hash value with specific properties.

Proof of work:

Proof of Work (PoW) is a consensus mechanism used in blockchain networks to achieve agreement and validate transactions. It is a computationally intensive process that requires participants, known as miners, to solve complex mathematical puzzles to add new blocks to the blockchain. Here's how Proof of Work works:

1.Mining Process:

- Miners collect pending transactions and package them into a block.
- To add the block to the blockchain, miners must find a nonce (a random number) that, when combined with the block data, produces a hash value that meets specific criteria.
- The criteria typically involve finding a hash value that has a certain number of leading zeros or is below a specific target value.

2.Hash Function:

- Miners use a cryptographic hash function, such as SHA-256 (Secure Hash Algorithm 256-bit), to calculate the hash value of the block.
- The hash function takes the block header (which includes the nonce and other metadata) and returns a fixed-length output, which is the hash value.

3. Difficulty Adjustment:

- The difficulty of finding a valid nonce is adjusted periodically to maintain a consistent block creation rate. This adjustment ensures that the average time to mine a block remains relatively constant.
- The difficulty is usually based on the total computational power of the network, making it more challenging to find a valid nonce as more miners join the network.

4. Validating the Proof:

- Once a miner finds a nonce that produces a valid hash value, they broadcast the new block to the network.
- Other nodes in the network can easily verify the validity of the proof of work by independently calculating the hash value using the same block data and confirming that it meets the required criteria.

5.Consensus and Longest Chain Rule:

- In PoW-based blockchains, the longest valid chain is considered the "true" or "valid" chain.
- When multiple miners find valid proofs at approximately the same time, temporary forks may occur. However, miners will continue building on the longest chain, adding blocks to it, and eventually, the longest chain will become dominant as it grows faster.

6.Security and Attack Resistance:

- The PoW consensus mechanism provides security against malicious activities such as double-spending or tampering with past blocks. To modify a block, an attacker would need to recalculate the proof of work for that block and all subsequent blocks, which becomes increasingly computationally expensive as the blockchain grows.

While PoW has been widely used in blockchain networks like Bitcoin, it is associated with high energy consumption due to the computational resources required for mining. To address this concern, alternative consensus mechanisms such as Proof of Stake (PoS) have been developed, which use different criteria for block validation and participation in the consensus process.

NONCE: In the context of blockchain and cryptography, a nonce is a number used only once in a cryptographic algorithm. The term "nonce" stands for "number used

once." A nonce is typically a random or arbitrary value that is added to other data during a cryptographic operation, such as hashing, to ensure uniqueness and increase security.

DIFFICULTY CRITERIA: In blockchain networks that use Proof of Work (PoW) as a consensus mechanism, the difficulty criteria refer to the specific conditions that a miner's solution must meet in order to successfully mine a new block. These criteria are set to control the rate at which new blocks are added to the blockchain.

Validating the proof:

To determine if a proof is valid in the context of a Proof of Work (PoW) consensus mechanism used in blockchain networks, you typically follow these steps:

1.Retrieve the Block: Obtain the block for which the proof needs to be validated. This includes the block header and the associated nonce.

2.Calculate the Hash: Use the same hash function employed in the PoW algorithm (e.g., SHA-256) to calculate the hash of the block header. The block header includes all the necessary data, such as the previous block hash, timestamp, Merkle root of the transactions, and other metadata.

3.Combine with Nonce: Append the nonce to the block header data and recalculate the hash using the hash function.

4.Compare with Target: Compare the resulting hash value with the target value or difficulty target. The target value is derived from the current difficulty level, which is adjusted periodically in PoW-based networks.

5.Validate the Proof: If the calculated hash value is below the target or meets the difficulty criteria specified by the consensus mechanism, the proof is considered valid. This indicates that the miner has successfully found a nonce that, when combined with the block data, produces a hash value that fulfills the requirements.

Validating a proof involves confirming that the calculated hash value falls within the specified range or satisfies the difficulty criteria set by the blockchain network. If the proof meets these criteria, it is considered a valid proof of work.

MINE:

In the context of blockchain, the term "mine" refers to the process of validating and adding new blocks to the blockchain through the Proof of Work (PoW) consensus mechanism. Miners, who are participants in the network, compete to solve complex mathematical puzzles in order to find a valid nonce and create a new block. Here's an overview of the mining process:

1.Collect Pending Transactions: Miners gather a set of pending transactions from the network's mempool. These transactions are typically waiting to be included in the next block.

2.Create the Block Template: Miners create a new block template, which includes the previous block's hash, a timestamp, a list of transactions, and other relevant metadata. The block template acts as a foundation for the block they are trying to mine.

3.Find a Valid Nonce: Miners repeatedly modify the nonce value in the block template and calculate the resulting hash using a cryptographic hash function (e.g., SHA-256). The goal is to find a nonce that, when combined with the block data, produces a hash value that meets the required difficulty criteria set by the network.

4.Check Validity: After finding a nonce, miners calculate the hash value of the block using the updated block data, including the new nonce. They then compare this hash value against the target value or difficulty target specified by the network's consensus rules.

5.Broadcast the New Block: If the calculated hash value is below the target or meets the difficulty criteria, the miner has found a valid block. They broadcast this new block to the network, allowing other participants to verify the proof of work and add the block to their local copies of the blockchain.

6.Reward and Incentives: Miners are incentivized to mine blocks through rewards, such as cryptocurrency tokens. In some blockchain networks, like Bitcoin, miners who successfully mine a block are rewarded with newly minted tokens (block reward) and transaction fees associated with the included transactions.

The mining process requires significant computational power and energy consumption. Miners compete against each other to find a valid nonce, and the first miner to find a valid solution gets to add the new block to the blockchain. This process ensures the security and integrity of the blockchain by making it computationally expensive for malicious actors to manipulate the transaction history.

6. CONCLUSION

Securing data with the combined use of blockchain and AI offers several advantages and can significantly enhance data security and privacy. Here is a summary of the key benefits and considerations:

1.Immutable Data: Blockchain's inherent nature of immutability ensures that once data is recorded on the blockchain, it becomes tamper-proof. This feature can protect sensitive information from unauthorized modifications or tampering, providing data integrity and auditability.2.Decentralized Storage: Blockchain operates in a decentralized manner, distributing data across multiple nodes in the network. This decentralized storage approach reduces the risk of a single point of failure and makes it more challenging for hackers to compromise or manipulate data.3.Encryption and Cryptography: Blockchain utilizes cryptographic techniques to secure data. AI can complement this by providing advanced encryption algorithms and cryptographic mechanisms, further strengthening the security of data stored and transmitted within the blockchain network.4.Access Control and Privacy: Blockchain can facilitate granular access control mechanisms, enabling users to control who can access their data. AI can assist in implementing intelligent access control policies based on user behavior, data sensitivity, and context, enhancing data privacy and protection.5.).Smart Contracts for Security Automation: Smart contracts, a feature of blockchain technology, allow the execution of predefined actions based on specified conditions. AI algorithms can be integrated with smart contracts to automatically detect and respond to security incidents, such as detecting anomalies, triggering alerts, or initiating security protocols.

In conclusion, the combination of blockchain and AI technologies offers promising possibilities for securing data. The decentralized and immutable nature of blockchain, combined with the advanced capabilities of AI, can provide enhanced data security, privacy, fraud detection, and automation of security processes.

7.FUTUTE SCOPE

The future scope of securing data with the combination of blockchain and AI is vast and holds significant potential for various industries. Here are some potential areas where this integration can have a significant impact:1.Cybersecurity: Blockchain and AI can revolutionize the field of cybersecurity. The use of blockchain's decentralized and immutable ledger can enhance data integrity, prevent unauthorized access, and mitigate the risk of data breaches. AI algorithms can analyze network traffic, detect anomalies, and identify potential security threats in real-time, enabling proactive security measures.2.Identity Management: Blockchain and AI can be utilized to create decentralized and self-sovereign identity management systems. This would allow individuals to have control over their personal data and share it securely with trusted parties. AI can assist in verifying and authenticating identity information, reducing the risk of identity theft and fraud.

We can also use biometric while creating the profile.

It's important to note that while the potential of securing data with blockchain and AI is significant, there are challenges to overcome, such as scalability, interoperability, legal and regulatory frameworks, and ethical considerations. Continued research, development, and collaboration across industries will be crucial in realizing the full potential of this integration and addressing these challenges.

Acknowledgements

We would like to express our special gratitude to our Guide Dr. CH. Niranjan Kumar and Mentor Mrs. Neja Jhunjhunwala who gave us a golden opportunity to do a wonderful project on this topic. It makes us to do a lot of research and learnt new things. We are really thankful to that.

In addition to that, we would also thank my friends who helped us a lot in finalizing this project within the limited time frame.

8. REFERENCES

[1] H. Yin, D. Guo, K.Wang, Z. Jiang, Y. Lyu, and J. Xing, ``Hyper connected network: A decentralized trusted computing and networking paradigm," IEEE Netw., vol. 32, no. 1, pp. 112117, Jan./Feb. 2018.

[2] K. Fan, W. Jiang, H. Li, and Y. Yang, ``Lightweight RFID protocol for medical privacy protection in IoT," IEEE Trans Ind. Informat., vol. 14, no. 4, pp. 16561665, Apr. 2018.

[3] T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, and N. Zeldovich, ``Amber: Decoupling user data from Web applications," in Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV), Warth-Weiningen, Switzerland, 2015, pp. 16.

[4] M. Lecuyer, R. Spahn, R. Geambasu, T.-K. Huang, and S. Sen, ``Enhancing selectivity in big data," IEEE Security Privacy, vol. 16, no. 1, pp. 3442, Jan./Feb. 2018.

[5] Y.-A. de Montjoye, E. Shmueli, S. S.Wang, and A. S. Pentland, ``openPDS: Protecting the privacy of metadata through SafeAnswers," PLoS ONE, vol. 9, no. 7, 2014, Art. no. e98790.

[6] C. Perera, R. Ranjan, and L.Wang, ``End-to-end privacy for open big data markets," IEEE Cloud Comput., vol. 2, no. 4, pp. 4453, Apr. 2015.