International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Impact of Hybrid LSTM Based Deep Learning Model Over Blockchain Security and Performance Enhancement

Bukka Shobharani[1], Dr. Veera Talukdar[2], Mrs. Reshma Ramakant Kanse[3], Dr. Vaishali V. Sarbhukan[4], Dr. S. Farhad[5], Harshal Patil[6], Ankur Gupta[7, *]

Submitted: 02/10/2023 **Revised**: 19/11/2023 **Accepted**: 30/11/2023

Abstract: There is a need to maintain patient records and identity management in real time system due to the increasing need for record management. The function of blockchain technology in ensuring the safety of data is the focus of the current study. The main goal of this study is to suggest improvements that use hashing and encryption methods. In this approach, a record is seen as a transaction, and each transaction on a blockchain is recorded and kept in a public ledger as a little piece of labor. Encrypting data before storing it on blockchain is an extra security measure that is now the subject of investigation. To further ensure the safety and efficiency of the blockchain, the SHA-256 hashing algorithm has been used. To further ensure the privacy, authenticity, and immutability of data kept in the distributed ledger, hashing and encryption are essential components of blockchain technology. To prevent unauthorized parties from reading sensitive data, encryption transforms it into ciphertext, which can only be decrypted with the correct cryptographic key. Blockchain security is built upon hashing and encryption, which together provide a strong barrier against data modification, unauthorized access, and guarantee the distributed ledger's reliability. Improvements in security and performance are shown by evaluation of mistake rate, performance, accuracy, and security. We have measured performance in terms of time, security in terms of displaying blocks that have been attacked from the outside, and accuracy in terms of recall, precision, and f1-score.

Keywords: *Deep Learning, Block chain, Security, Privacy*

1. Introduction

Blockchain technology has gained significant attention and is being increasingly adopted across various real-life applications due to its unique characteristics. Here are some key areas where blockchain plays a crucial role, along with the need for security and performance:

1. Cryptocurrencies and Finance:

- Role: Blockchain is the underlying technology for cryptocurrencies like Bitcoin and Ethereum, enabling secure and transparent peer-to-peer transactions without the need for intermediaries.

- Security Need: Cryptocurrencies require strong security measures to protect users' funds and prevent fraudulent activities, such as double-spending and hacking attacks on exchanges.

- Performance Need: Scalability is a significant concern to handle a large number of transactions efficiently.

2. Supply Chain Management:

- Role: Blockchain can be used to create transparent and traceable supply chains by recording every transaction and movement of goods on the blockchain. This helps in reducing fraud, ensuring authenticity, and improving overall efficiency.

- Security Need: Ensuring the integrity of the supply chain data is crucial to prevent tampering or counterfeiting, which makes security a top priority.

- Performance Need: Supply chains involve a large

1 Research Scholar, Department of English, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh-522502, India Email: 193240007@kluniversity.in

2 Professor, Department of Computer Science, D Y Patil International University, Akurdi Pune, Maharashtra, India Email: bhaskarveera95@gmail.com

3 Assistant Professor of AI and ML, Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, Navi Mumbai, India Email: rrkanse@bvucoep.edu.in

4 Associate Professor, Department of Information Technology, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, Maharashtra, India Email: vaishali5780@gmail.com

5 Associate Professor, Department of English, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh-522502, India Email: farhad.anu21@gmail.com

6 Associate Professor, Department of Computer Science and Engineering, Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, India Email: harshal.patil@sitpune.edu.in

7, Assistant Professor, Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: ankurdujana@gmail.com*

** Corresponding Author Email: ankurdujana@gmail.com*

volume of transactions and data, necessitating a scalable and efficient blockchain system.

3. Smart Contracts in Legal Agreements:

- Role: Blockchain enables the execution of self-executing smart contracts, which are programmable contracts with the terms directly written into code. This automates and enforces the execution of agreements.

- Security Need: Security is critical to prevent vulnerabilities in smart contracts that could be exploited, leading to financial losses or legal disputes.

- Performance Need: Efficient execution of smart contracts requires a blockchain with high throughput and low latency.

4. Identity Management:

- Role: Blockchain can provide a secure and decentralized way of managing digital identities, reducing the risk of identity theft and providing individuals with better control over their personal information.

- Security Need: Protecting personal data and ensuring the security of identity information is paramount.

- Performance Need: Efficient identity verification processes require a blockchain with fast transaction processing capabilities.

5. Healthcare Data Management:

- Role: Blockchain can improve the security and interoperability of healthcare data by providing a decentralized and tamper-resistant ledger for medical records.

- Security Need: Protecting sensitive patient information and ensuring data integrity are critical in healthcare applications.

- Performance Need: Efficient management of healthcare data, especially in emergency situations, requires a blockchain with high performance.

Role of blockchain in real-life applications is diverse and impactful. The need for security arises from the decentralized and transparent nature of blockchain, while performance considerations are essential to ensure scalability and efficiency in handling a large number of transactions and data. As blockchain technology continues to evolve, addressing these security and performance challenges will be crucial for its widespread adoption.

1.1. Role of Data compression in size reduction in block chain

Data compression plays a crucial role in size reduction within blockchain technology. In the context of blockchain, where every node in the network maintains a copy of the entire distributed ledger, minimizing the size of data is essential for improving efficiency and scalability. By employing data compression techniques, the amount of storage space required for storing transactions, smart contracts, and other information on the blockchain can be significantly reduced. This reduction in size has several benefits, including faster data transmission across the network, lower storage requirements for each node, and improved overall performance. As the blockchain grows over time, efficient data compression becomes increasingly vital in mitigating the challenges associated with bandwidth limitations and storage capacity. Ultimately, data compression contributes to optimizing the blockchain's resource utilization and enhancing its ability to scale effectively in various real-world applications.

1.2. Working of SHA 256 based Hashing in security of block chain data

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that plays a crucial role in ensuring the security and integrity of data within blockchain technology. Here's how SHA-256 based hashing works in the context of securing blockchain data:

1. Hashing Process:

- When data is entered into a blockchain system, whether it's a transaction, a block of transactions, or other information, SHA-256 is applied to create a fixed-size hash value (256 bits or 64 hexadecimal characters).

2. Deterministic Output:

- SHA-256 is a deterministic algorithm, meaning that the same input will always produce the same hash output. This property is essential for data consistency and verification within the blockchain.

3. Irreversibility:

- SHA-256 is a one-way function, which means it is computationally infeasible to reverse the process and obtain the original input data from the hash value. This property enhances the security of blockchain data, as even small changes in the input will result in a substantially different hash.

4. Collision Resistance:

- SHA-256 is designed to be collision-resistant, meaning that it is highly unlikely for two different inputs to produce the same hash output. This property ensures that each unique piece of data has a unique hash value, reducing the risk of data tampering or fraud.

5. Block Linking and Immutability:

- In blockchain, each block typically contains a reference to the hash of the previous block. This creates a chain of

blocks, and any alteration to the data in a specific block would change its hash, thus affecting the subsequent blocks. This interlinking of blocks through hashed references enhances the immutability of the blockchain.

6. Consensus Mechanism:

- In a blockchain network, nodes validate transactions and agree on the state of the blockchain through a consensus mechanism (e.g., Proof of Work or Proof of Stake). The hash values play a role in reaching consensus, ensuring that all nodes agree on the validity of transactions and the order in which they are added to the blockchain.

7. Mining and Proof of Work:

- In Proof of Work-based blockchains, miners compete to solve a computationally intensive mathematical problem. The solution, along with other data, is hashed using SHA-256. The resulting hash must meet certain criteria to be considered valid, and this process helps secure the network by making it computationally expensive to tamper with the blockchain.

8. Digital Signatures:

- Hash values are often used in conjunction with digital signatures to verify the authenticity of transactions. The hash of a transaction is signed by the sender, and the signature is verified by others using the sender's public key.

SHA-256 based hashing is fundamental to the security architecture of blockchain. It provides data integrity, irreversibility, and collision resistance, ensuring that once data is added to the blockchain, it becomes highly resistant to tampering. The properties of SHA-256 contribute to the trustworthiness and immutability of the blockchain, making it a foundational element in various blockchain implementations.

1.3. Factors influencing Performance of transaction on blockchain

The performance of transactions on a blockchain is influenced by various factors, and optimizing these elements is crucial to ensuring the efficiency and scalability of the blockchain network. Here are key factors that impact the performance of transactions on a blockchain:

1. Blockchain Consensus Mechanism:

- The consensus mechanism used by the blockchain significantly influences transaction performance. For example, Proof of Work (PoW) involves complex computations, potentially causing longer transaction confirmation times, while Proof of Stake (PoS) and other consensus algorithms may offer faster confirmation times.

2. Block Size and Block Time:

- The size of blocks in the blockchain and the time it takes to generate a new block are critical factors. Larger block sizes can accommodate more transactions, but they also require more resources for validation and propagation. Shorter block times can lead to quicker confirmation, but it may increase the chances of forks.

3. Transaction Throughput:

- The maximum number of transactions a blockchain can handle per unit of time is known as transaction throughput. Higher throughput is desirable for scalability. Blockchain networks need to scale their throughput to accommodate growing user bases and increasing transaction volumes.

4. Network Latency:

- The time it takes for data to travel across the network can impact transaction speed. Network latency can be influenced by factors such as geographical distance between nodes, network congestion, and the efficiency of the underlying network infrastructure.

5. Blockchain Interoperability:

- Interoperability with other blockchains and external systems can affect transaction performance. Seamless communication between different blockchains or with external databases requires efficient protocols and standards.

6. Smart Contract Complexity:

- Smart contracts are self-executing contracts with the terms directly written into code. Complex smart contracts can increase the computational load on the network, leading to longer transaction confirmation times. Optimizing smart contract code is essential for better performance.

7. Node Scalability:

- The number of nodes in the blockchain network influences its scalability. Increasing the number of nodes may improve decentralization but can also impact performance. Scalability solutions, such as sharding or layer 2 solutions, aim to address this challenge.

8. Blockchain Governance:

- Governance structures and decision-making processes within a blockchain network can impact its ability to adapt and implement performance-enhancing upgrades. Efficient governance can lead to timely updates and improvements.

9. Transaction Fees:

- Transaction fees can affect the priority and speed of transaction processing. Higher fees may incentivize miners to include transactions in blocks more quickly, but

excessive fees could discourage usage.

10. Security Measures:

- The level of security implemented in the blockchain network, such as the strength of cryptographic algorithms, impacts the time required for transaction validation and confirmation. Striking a balance between security and performance is essential.

11. Storage and Computational Resources:

- The availability and capacity of storage and computational resources on nodes in the network influence transaction processing. Inadequate resources can lead to delays and increased transaction costs.

12. Blockchain Forks:

- Forks in the blockchain, whether intentional (hard forks) or unintentional (soft forks), can impact transaction processing and cause temporary disruptions. Governance mechanisms and coordination are critical to managing forks effectively.

Optimizing these factors and finding a balance between security, decentralization, and scalability is an ongoing challenge for blockchain developers and architects. The selection of specific blockchain technologies, consensus mechanisms, and design choices can significantly impact the overall performance of transactions on a blockchain.

1.4. Factors influencing Accuracy parameter during data classification in block chain.

In the context of data classification within a blockchain, the accuracy parameter is crucial for ensuring the reliability of the classification process. Several factors can influence the accuracy of data classification in a blockchain environment. Here are key considerations:

1. Quality of Training Data:

- The accuracy of a data classification model in blockchain depends heavily on the quality of the training data used to train the model. If the training data is biased, incomplete, or not representative of the real-world scenarios, the model may exhibit poor accuracy.

2. Feature Selection:

- The features or attributes chosen for classification play a significant role. Relevant features that capture essential characteristics of the data contribute to accurate classification, while irrelevant or redundant features may introduce noise and decrease accuracy.

3. Model Complexity:

- The complexity of the classification model can impact accuracy. Overly complex models may perform well on the training data but could struggle to generalize to new, unseen data, leading to overfitting. On the other hand, overly simplistic models may not capture the complexity of the underlying patterns.

4. Hyperparameter Tuning:

- Fine-tuning the hyperparameters of the classification algorithm is crucial for optimizing model performance. Adjusting parameters such as learning rate, regularization, and tree depth can significantly impact accuracy.

5. Data Preprocessing:

- The preprocessing steps applied to the data, such as normalization, scaling, and handling missing values, can influence the accuracy of the classification model. Proper data preprocessing ensures that the model is more robust and performs well on diverse datasets.

6. Class Imbalance:

- In blockchain applications, the distribution of different classes of data may not be uniform. Class imbalances can lead to biased models, where the classifier may be more accurate for the majority class but less accurate for minority classes. Techniques like oversampling or undersampling may be employed to address this issue.

7. Blockchain Data Characteristics:

- The unique characteristics of blockchain data, such as its structure, volume, and format, can impact classification accuracy. Understanding how blockchain-specific features influence the data and adapting classification models accordingly is essential.

8. Security Measures:

- Security features implemented in the blockchain, such as encryption and privacy-preserving techniques, may impact the accuracy of data classification. Balancing security requirements with the need for accurate classification is a key consideration.

9. Decentralization and Consensus:

- In a decentralized blockchain network, achieving consensus on the classification of data may introduce challenges. Ensuring that all nodes agree on the classification results is essential for maintaining the accuracy of the classification across the network.

10. Adversarial Attacks:

- The security of the blockchain may also be influenced by adversarial attacks, where malicious actors attempt to manipulate the data to deceive the classification model. Robustness against adversarial attacks is crucial for maintaining accuracy.

11. Dynamic Nature of Data:

- Blockchain data may be dynamic, with changes occurring over time. The accuracy of a classification model needs to account for the evolving nature of the data, and the model should be capable of adapting to changes.

12. Cross-Validation:

- The use of proper cross-validation techniques is important for obtaining a realistic estimate of the model's accuracy. Cross-validation helps assess how well the model will perform on unseen data.

Optimizing these factors and addressing the unique challenges posed by blockchain data contribute to achieving high accuracy in data classification within a blockchain environment. It's important to continually monitor and update the classification model to adapt to changes in the data and maintain accurate results over time.

2. Literature Review

Over the course of the last ten years, "block chain" has been the subject of research at a wide range of educational institutions and businesses. It is widely regarded as one of the most fascinating newly discovered technologies. Blockchain is a distributed and immutable ledger that eliminates the need for a trusted third party to verify and record financial transactions. Blockchain is a distributed ledger. These pioneers include the government, the energy industry, and the healthcare sector. Blockchain 3.0 is the next version of blockchain technology, and it is currently being developed by a number of different organizations. Because of the many ways in which these technologies have the potential to enhance patient care, health care practitioners have enthusiastically welcomed them. The decentralized nature of blockchain, in addition to the privacy safeguards and security measures that are incorporated into the system, makes it an appealing technology for use in the healthcare industry. It is possible to make use of these choices in order to guarantee that only authorized personnel have access to personally identifiable medical information.

The Bitcoin protocol was the first to include the idea of a blockchain, which was first presented in the year 2008. One way to think of it is as a distributed bookkeeping system. Through the use of a distributed public ledger that is referred to as a chain of blocks in blockchain, each and every network transaction is recorded and validated. In each block, there is a header and a body part. The hash of the block that came before it is shown in the header of each new block that is loaded. The blocks that come after one another in a chain or linked list are related to the blocks that came before them. In the process of evaluating the transactions included inside a block, the use of tools like as Merkle trees, timestamps, and nonces in block headers has the potential to expedite the process and reduce the amount of labor that is required. In the event that miners are attempting to solve a mathematical issue, they may sometimes change the nonce number.

A blockchain transaction is a little amount of work that is recorded and stored in a unit of data storage known as a block. This block is how the blockchain is organized. In any given transaction, there can be no more than two parties participating at any one time. It is necessary for the overwhelming majority of users associated with the system to reach a consensus in order for a transaction to be successful. After a transaction has been recorded on a blockchain, it is impossible for anybody to change it, which is why blockchains are fully trustworthy. In light of the immutability of blockchain technology, it is sufficient for each participant to maintain just a single copy of the ledger at all times. In order to ensure that transactions can be carried out without any disruptions, the business logic of a blockchain is encoded into computer code that is referred to as smart contracts. This code is then performed automatically on the blockchain's underlying architecture.

The incorporation of a smart contract into a blockchain makes it capable of self-verification, which is made possible by the automated capabilities of the blockchain, and it also becomes self-enforcing when all of the rules are satisfied. Blockchain technology is decentralized, permanent, accessible, and anonymous, which means that it cannot be manipulated or tampered with in any way. There is a great deal of difficulty involved in manipulating people.

Several of the numerous researches that are relevant to blockchain technology and healthcare are covered in the following paragraphs.

According to Kristen N. Griggs et al. (2018), more weaknesses in data transmission and recording become evident as the number of people who utilize the Internet of Things (IoT) and other kinds of remote monitoring increases. They suggest employing smart contracts that are based on blockchain technology in order to analyze and handle protected health information (PHI) from medical sensors in a safe manner. [1] Igor Radanovi and colleagues (2018) introduced blockchain, which is a distributed database that is made up of blocks of data that are linked cryptographically. Blockchain is used to record the past deals of a decentralized network's assets and transactions [2]. MAS-based distributed systems that deal with sensitive data were the subject of an investigation by Davide Calvaresi and colleagues (2018) [3]. Researchers Aiqing Zhang et al. (2018) found that working together on medical data online might potentially lead to more accurate

diagnoses; however, they also stressed that patients' privacy must be respected [4]. For example, according to Xueping Liang et al. (2018), the public's interest in monitoring their own health has been spurred by wearable technology, which has caused people to be more concerned than they have ever been before. By using the blockchain and the Intel SGX trusted execution platform, this research study provides a decentralized approach to the preservation of individuals' privacy [5]. Mahdi H. Miraz et al. (2018) were the first to discuss how the blockchain technology that underpins Bitcoin is now being deployed in the current Internet of Things context. Over the last several years, researchers and practitioners working in the private sector have been putting more of their attention on this particular field of investigation. POW is a cryptographic problem that is used to increase the safety of Bitcoin Cash by guaranteeing that the digital ledger that keeps track of all Bitcoin Cash transactions is unalterable [6]. This is accomplished by ensuring that the ledger cannot be altered. As a result of the broad prevalence with which blockchain-based technology is being used in connection with Android mobile devices, criminals are developing mobile malware that is capable of breaching blockchains, as stated by Ahmad Firdaus et al. (2018). As proven by Hongyu Li et al. (2018), the vast changes that have taken place in the quantity and quality of medical records have made it possible for no one to ever again be in a position where they are unable to get care. A blockchain-based healthcare distributed ledger system (DPS) is the topic of discussion in this article.

The utility and efficiency of the system are shown by performance analysis [8]. A number of businesses, such as the food and pharmaceutical industries, the real estate market, and the financial sector, are expected to benefit from the implementation of distributed ledger technology, according to the predictions made by Gregory Epiphaniou and colleagues. There are now a number of Blockchain healthcare pilot projects that are being carried out, and this article will address both the advantages and disadvantages about these programs [9]. According to the findings of Tong Zhou et al. (2019), a great number of individuals, including academics and medical professionals, are looking forward to the introduction of electronic health records. With the use of the Med-PPPHIS prototype, they propose a closed-loop approach to the problem of chronic illnesses in the province of Anhui in China [10]. According to the first hypothesis put forward by Shamaila Iram et al. (2019), a dramatic increase in energy consumption poses a danger to the sustainability of both the economy and the environment. During the course of this investigation, cutting-edge methods for data exploration and analytics were used to a time series of variables that were associated with energy levels. Heat maps were used to graphically display the results of the data analysis [11]. A variety of contemporary mobile devices were used in the study conducted by Geetanjali Rathee and colleagues (2020) to investigate the ways in which the utilization of multimedia methods in the healthcare industry has enabled the gathering, analysis, and exchange of patient data that is presented in visual, textual, and audio forms [12].

3. Problem Statement

The use of blockchain technology to store information has been the subject of a number of studies that have been carried out in the area of healthcare; nevertheless, it is of the utmost importance that these data be kept safe. The difficulty is that these conventional techniques have poor performance, which is the reason why blockchain has been considered for the goal of securing healthcare data. However, there are traditional ways that have examined blockchain. Conventional research, on the other hand, has taken into account the possible applications of Blockchain technology in the real time system nevertheless, it has been shown that these applications have problems with both inaccuracy and performance. The present effort intends to solve the limitations of previous blockchain systems for healthcare, which include issues with data security, sluggish speed, and a lack of accuracy. As an example, the Tradition approach [3] that examined a MAS-based distributed system to manage sensitive data overlooked the performance problem, while the Med-PPPHIS [10] ignored the accuracy.

4. Proposed Work

The study that has been recommended has concentrated on research concerning block chain security and applications in the health care industry. Additionally, it has investigated the security and performance challenges that are associated with block chain security. In the work that is being recommended, the data set pertaining to real time application is first compressed, and then it is encrypted by using an encryption technique. Before the data is saved in the blockchain once the block has been initiated, it is first compressed and encrypted to ensure its safety. The accuracy and performance of the work that has traditionally been done is then compared to the accuracy and performance of the job that will be proposed. This comparison is then made. Within the context of the current study activity, the function of categorization methods in the safety of the real time system is being considered. Already conducted research in the field of real time system is taken into consideration first.

4.1. Algorithm

1. Input blockchain based data that is compressed and encrypted.

2. Pre-process data to filter less significant information in order to improve accuracy and performance.
3. Initialize LSTM model for deep learning in order to perform data classification.
4. Batch size , learning rate, iteration is set
5. Data splitting is made for training and testing
6. Train the LSTM model considering health care data
7. Testing operation is made in order to find the accuracy parameters such as recall, precision, F1 score

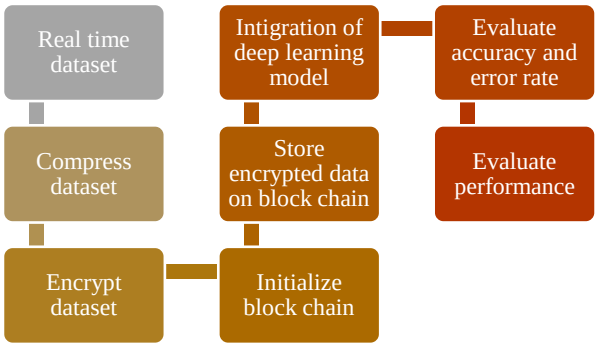


Fig. 1. Proposed Security model

4.2. Evaluation metrics

In the proposed study, accuracy measures like F1Score, precision, and recall value are being taken into consideration. On the other hand, time is being taken into consideration for performance assessment. During the security analysis, the number of blocks that were impacted is taken into consideration when determining the effect of the attack.

4.3. Dataset

The basic information of the client, his sale/purchase history, and the specifics of his disease have been taken into consideration in the data that has been gathered in real time from commercial institutions. The dataset that is being evaluated is considered main data.

4.4. Process flow of work

During the process of data categorization, this section provides a description of the many characteristics and methods that are used to maximize the accuracy, error rate, security, and performance. The efficiency of the system has been optimized via the use of a data compression mechanism, which minimizes the size of the content. On the other hand, data encryption has been used to maximize the security of the data. The LSTM model is initialized after the data compression process, and the batch size is then set. once that, the data is divided into training and testing sets once the iterations have been established. Following training operations, testing is carried out in order to assess the level of correctness.

4.5. Detailed Deep learning model used in proposed work

Utilizing deep learning models for real-time client information classification stored on a blockchain involves a combination of advanced technologies. Here's a general outline of how this could be implemented:

1. Client Information Classification Model:

- Develop a deep learning model for client information classification. This could involve natural language processing (NLP) techniques for text-based information or computer vision for image-based information.

- Train the model on a diverse dataset that includes various types of client information to ensure robust performance.

2. Integration with Blockchain:

- Utilize a blockchain platform that supports smart contracts and data storage capabilities. Ethereum, for example, is a popular choice for this kind of application.

- Develop a smart contract that defines the rules and conditions for storing and updating client information on the blockchain.

3. Secure Data Transmission:

- Implement secure channels for transmitting client information between the user interface (where the information is entered or uploaded) and the blockchain. This could involve encryption and secure communication protocols.

4. Client Information Storage on Blockchain:

- When new client information needs to be added or updated, the deep learning model processes the information and assigns appropriate classifications.

- The processed information is then stored on the blockchain. The smart contract ensures that only valid and correctly classified information gets added to the blockchain.

5. Decentralized Access Control:

- Implement decentralized access control mechanisms using blockchain-based identity management systems. This ensures that only authorized entities can access and update specific client information.

6. Auditability and Immutability:

- Leverage the immutability and transparency features of blockchain to create an auditable record of all changes made to client information. This is particularly important

for regulatory compliance and accountability.

7. Security Considerations:

- Implement robust security measures to protect both the deep learning model and the blockchain infrastructure. This includes secure model deployment, encryption, and regular security audits.

8. Real-Time Processing:

- Optimize the deep learning model and blockchain interactions to ensure real-time processing of client information. Consider factors such as model inference speed and blockchain transaction confirmation times.

9. User Interface:

- Develop a user-friendly interface for users to interact with the system. This could be a web or mobile application that communicates with the blockchain and displays relevant client information.

10. Compliance with Regulations:

- Ensure that the system complies with data protection and privacy regulations. This may involve implementing features like user consent management and data anonymization.

By combining deep learning models with blockchain technology, you can create a system that not only classifies and stores client information securely but also provides transparency, auditability, and decentralized control over access. This kind of solution could be particularly valuable in industries where client data confidentiality and compliance with regulations are critical, such as finance, healthcare, or legal services.

4.6. Tools/platforms used for implementing the system.

Implementing LSTM-based deep learning using Python typically involves leveraging deep learning libraries and frameworks. Here are tools and platforms that are used in proposed research:

- TensorFlow: TensorFlow is an open-source machine learning framework developed by Google. It has extensive support for deep learning, including LSTM layers.
- Usage: You can use the TensorFlow library along with its high-level API, Keras, to easily build and train LSTM-based models.
- PyTorch: PyTorch is an open-source deep learning library developed by Facebook. It's known for its dynamic computation graph and ease of use.
- Usage: PyTorch provides modules for creating LSTM layers and building sequential models.
- Keras: Keras is a high-level neural networks API written in Python and capable of running on top of TensorFlow, Theano, or Microsoft Cognitive Toolkit.
- Usage: Keras provides a user-friendly interface for building and training LSTM models, and it can be used with TensorFlow as a backend.
- scikit-learn: scikit-learn is a machine learning library that provides simple and efficient tools for data analysis and modeling, including LSTM-based models through its neural network module.
- Google Colab: Google Colab is a free, cloud-based platform provided by Google that allows you to write and execute Python code in a Jupyter Notebook-like environment. It comes pre-installed with popular machine learning libraries.

5. Result and discussion

After compression and encryption of real-time data, suggested deep learning technique was used for simulation, training, and testing. Implementation of suggested deep learning model on blockchain-based real-time commercial dataset yielded results. Conventional method confusion matrix is below.

Table 1 Confusion matrix for conventional Conventional

	Class 1	*Class 2*
Class 1	284	21
Class 2	25	1912

In case of proposed work, confusion matrix obtained is shown below

Table 2 Confusion matrix for Proposed work

	Class 1	*Class 2*
Class 1	289	16
Class 2	5	1932

5.1. Comparison of overall accuracy

Considering outcome of conventional an proposed accuracy, Table 3 is presenting overall accuracy of both model on the bases of accuracy.

Table 3 Accuracy in case of proposed and conventional work

Conventional work	*Proposed work*
97.95	99.06

Considering table 3, accuracy in case of proposed and conventional work is shown below.

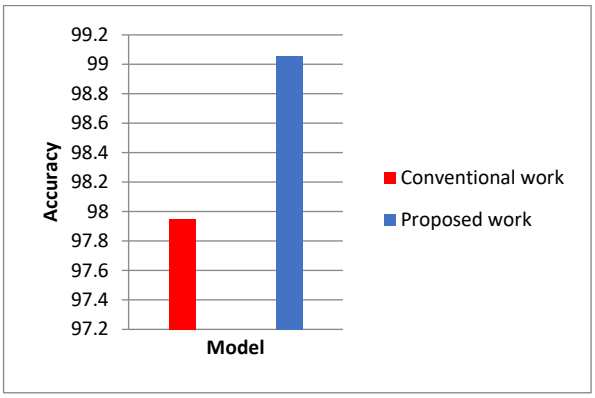


Fig. 2. Comparison of accuracy

5.2. Performance comparison

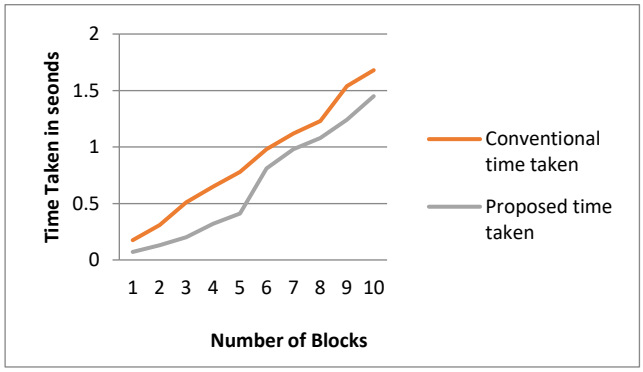
A simulation illustrating the time needed for block processing is provided in this section for your examination. Research has shown that the processing time required for a block is much less compared to the processing time required for traditional methods. When comparing the two, this is the situation. When quantifying the quantity of blocks, it is advisable to do division by 10 at regular intervals. The results of a comparison study between the suggested work processing times and the typical work processing times are shown in Table 4.

Table 4 Comparative analysis of performance

Number of blocks	Conventional time taken	Proposed time taken
1	0.175	0.071
2	0.31	0.13
3	0.51	0.20
4	0.65	0.32
5	0.78	0.41
6	0.98	0.81
7	1.12	0.98
8	1.23	1.08
9	1.54	1.24
10	1.68	1.45

Fig. 3. Comparative analysis of performance

Based on the data presented in Table 4, Figure 7 provides a comparative assessment of the performance of the proposed design in comparison to the conventional configuration.



5.3. Comparative analysis security

The text has included a specific section that presents a model of the effects resulting from external attacks on blocks. Upon examining the quantities of blocks at regular intervals of 5, it was seen that the amount of blocks that have been compromised due to an external assault is notably lower compared to traditional methods. The discovery was made by a comparative analysis of the compromised blocks against the overall number of blocks. The findings of a comparison study on the Blocks impacted by external assaults are shown in Table 5. This study aims to analyze and evaluate the processing durations of both standard and suggested labor methods.

Table 5 Security comparison

Block	Conventional	Proposed
1	0	0
5	1	0
10	2	1
15	4	2
20	6	3
25	9	4
30	11	7
35	17	9
40	21	12
45	28	15

The following picture compares Block impacted by external assaults in the present system versus the suggested approach, using table 5.

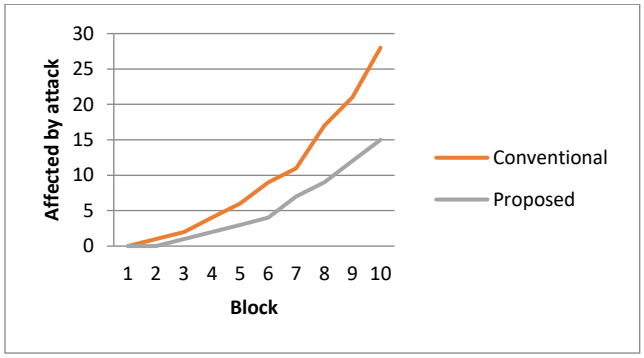


Fig. 4. Investigation of the Blocks that are influenced by attacks

6. Conclusion

Proposed work is 99% accurate, whereas traditional work is 97%. Proposed work improves significantly. Results following suggested contribution show error rate lowered from 11% to 14%. The probability of external assaults drops from 11% to 21%. Thus, suggested work overcomes traditional work's restriction. However, security and accuracy may be improved. Future studies may use hybrid technique with optimization for improvement.

7. Scope Of Research

In real-world blockchain applications, this research will improve accuracy, performance, and security. The approach considers external assaults that affect blocks as security flaws. Because transaction optimization may minimize mistake, future study may examine optimization mechanisms to increase accuracy and security.

References

[1] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring,” J. Med. Syst., vol. 42, no. 7, pp. 1–7, 2018, doi: 10.1007/s10916-018-0982-x.

[2] I. Radanović and R. Likić, “Opportunities for Use of Technology based on blockchain in Medicine,” Appl. Health Econ. Health Policy, vol. 16, no. 5, pp. 583–590, 2018, doi: 10.1007/s40258-018-0412-8.

[3] D. Calvaresi, A. Dubovitskaya, J. P. Calbimonte, K. Taveter, and M. Schumacher, Multi-agent systems and blockchain: Results from a systematic literature review, vol. 10978 LNAI. Springer International Publishing, 2018.

[4] A. Zhang and X. Lin, “Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain,” J. Med. Syst., vol. 42, no. 8, 2018, doi: 10.1007/s10916-018-0995-5.

[5] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, Towards decentralized accountability and self-sovereignty in healthcare systems, vol. 10631 LNCS. Springer International Publishing, 2018.

[6] M. H. Miraz and M. Ali, Blockchain enabled enhanced IoT ecosystem security, vol. 200. Springer International Publishing, 2018.

[7] A. Firdaus, N. B. Anuar, M. F. A. Razak, I. A. T. Hashem, S. Bachok, and A. K. Sangaiah, “Root Exploit Detection and Features Optimization: Mobile Device and Blockchain Based Medical Data Management,” J. Med. Syst., vol. 42, no. 6, 2018, doi: 10.1007/s10916-018-0966-x.

[8] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-Based Data Preservation System for Medical Data," J. Med. Syst., vol. 42, no. 8, pp. 1–13, 2018, doi: 10.1007/s10916-018-0997-3.

[9] G. Epiphaniou, H. Daly, and H. Al-Khateeb, "Blockchain and healthcare," Adv. Sci. Technol. Secur. Appl., pp. 1–29, 2019, doi: 10.1007/978-3-030-11289-9_1.

[10] T. Zhou, X. Li, and H. Zhao, "Med-PPPHIS: Blockchain-Based Personal Healthcare Information System for National Physique Monitoring and Scientific Exercise Guiding," J. Med. Syst., vol. 43, no. 9, 2019, doi: 10.1007/s10916-019-1430-2.

[11] S. Iram, T. Fernando, and R. Hill, Connecting to smart cities: Analyzing energy times series to visualize monthly electricity peak load in residential buildings, vol. 880, no. 3. Springer International Publishing, 2019.

[12] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using technology based on blockchain," Multimed. Tools Appl., vol. 79, no. 15–16, pp. 9711–9733, 2020, doi: 10.1007/s11042-019-07835-3.

[13] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, "The benefits and threats of technology based on blockchain in healthcare: A scoping review," Int. J. Med. Inform., vol. 142, no. February, p. 104246, 2020, doi: 10.1016/j.ijmedinf.2020.104246.

[14] D. J. Munoz, D. A. Constantinescu, R. Asenjo, and L. Fuentes, Clinicappchain: A low-cost blockchain hyperledger solution for healthcare, vol. 1010. Springer International Publishing, 2020.

[15] R. M. Amir Latif, K. Hussain, N. Z. Jhanjhi, A. Nayyar, and O. Rizwan, "A remix IDE: smart contract-based framework for healthcare sector by using Technology based on blockchain," Multimed. Tools Appl., 2020, doi: 10.1007/s11042-020-10087-1.

[16] A. Mubarakali, "Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN(SRHB)Approach," Mob. Networks Appl., vol. 25, no. 4, pp. 1330–1337, 2020, doi: 10.1007/s11036-020-01551-1.

[17] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-health records using keyless signature infrastructure technology based on blockchain in cloud," Neural Comput. Appl., vol. 32, no. 3, pp. 639–647, 2020, doi: 10.1007/s00521-018-3915-1.

[18] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences—A scoping review," Int. J. Med. Inform., vol. 134, no. May 2019, p. 104040, 2020, doi: 10.1016/j.ijmedinf.2019.104040.

[19] R. Casado-Vara, F. De la Prieta, S. Rodriguez, J. Prieto, and J. M. Corchado, Cooperative algorithm to improve temperature control in recovery unit of healthcare facilities, vol. 802. Springer International Publishing, 2020.

[20] M. P. McBee and C. Wilcox, "Technology based on blockchain: Principles and Applications in Medical Imaging," J. Digit. Imaging, vol. 33, no. 3, pp. 726–734, 2020, doi: 10.1007/s10278-019-00310-3.

[21] I. A. Omar, R. Jayaraman, K. Salah, I. Yaqoob, and S. Ellahham, "Applications of Technology based on blockchain in Clinical Trials: Review and Open Challenges," Arab. J. Sci. Eng., vol. 46, no. 4, pp. 3001–3015, 2021, doi: 10.1007/s13369-020-04989-3.

[22] T. Veeramakali, R. Siva, B. Sivakumar, P. C. Senthil Mahesh, and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using technology based on blockchain with an optimal deep learning model," J. Supercomput., vol. 77, no. 9, pp. 9576–9596, 2021, doi: 10.1007/s11227-021-03637-3.

[23] J. A. Santos, P. R. M. Inácio, and B. M. C. Silva, "Towards Use of Blockchain in Mobile Health Services and Applications," J. Med. Syst., vol. 45, no. 2, 2021, doi: 10.1007/s10916-020-01680-w.

[24] A. Rejeb, H. Treiblmaier, K. Rejeb, and S. Zailani, "Blockchain research in healthcare: a bibliometric review and current research trends," J. Data, Inf. Manag., vol. 3, no. 2, pp. 109–124, 2021, doi: 10.1007/s42488-021-00046-2.

[25] Ratkovic, Nada. "Improving Home Security Using Blockchain." International Journal of Computations, Information and Manufacturing (IJCIM) 2, no. 1 (2022).

[26] Liu, Yiying, Guangxing Shan, Yucheng Liu, Abdullah Alghamdi, Iqbal Alam, and Sujit Biswas. "Blockchain bridges critical national infrastructures: E-healthcare data migration perspective." IEEE Access 10 (2022): 28509-28519.

[27] Odeh, A., I. Keshta, and Q. A. Al-Haija. "Analysis of Blockchain in Healthcare Sector: Application and Issues. Symmetry 2022, 14, 1760." (2022).

[28] Mahajan, Hemant B., Ameer Sardar Rashid, Aparna A. Junnarkar, Nilesh Uke, Sarita D. Deshpande, Pravin R. Futane, Ahmed Alkhayyat, and Bilal Alhayani. "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems." Applied Nanoscience (2022): 1-14.

[29] Xi, Peng, Xinglong Zhang, Lian Wang, Wenjuan

Liu, and Shaoliang Peng. "A review of Blockchain-based secure sharing of healthcare data." Applied Sciences 12, no. 15 (2022): 7912.

[30] Attaran, Mohsen. "Technology based on blockchain in healthcare: Challenges and opportunities." International Journal of Healthcare Management 15, no. 1 (2022): 70-83.