EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

An AI-Enabled Blockchain Algorithm: A Novel Approach to Counteract Blockchain Network Security Attacks

Anand Singh Rajawat[1], S. B. Goyal[2,*], Manoj Kumar[3] and Thipendra P Singh[4]

[1]School of Computer Science & Engineering, Sandip University, Nashik, India
[2]Faculty of Information Technology, City University, Petaling Jaya, 46100, Malaysia
[3]University of Wollongong, Dubai, UAE
[3]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, NCR, India

Abstract

INTRODUCTION: In this research, we present a novel method for strengthening the security of blockchain networks through the use of AI-driven technology. Blockchain has emerged as a game-changing technology across industries, but its security flaws, particularly in relation to Sybil and Distributed Denial of Service (DDoS) attacks, are a major cause for worry. To defend the blockchain from these sophisticated attacks, our research centres on creating a strong security solution that combines networks of Long Short-Term Memory (LSTM) and Self-Organizing Maps (SOM).
OBJECTIVES: The main goal of this project is to create and test an AI-driven blockchain algorithm that enhances blockchain security by utilising LSTM and SOM networks. These are the objectives that the research hopes to achieve: In order to assess the shortcomings and weaknesses of existing blockchain security mechanisms. The goal is to create a new approach that uses LSTM sequence learning and SOM pattern recognition to anticipate and stop security breaches. In order to see how well this integrated strategy works in a simulated blockchain setting against different types of security risks.
METHODS: The methods used in our study are based on social network analysis. A combination of support vector machines (SOM) for pattern recognition and long short-term memory (LSTM) networks for learning and event sequence prediction using historical data constitutes the methodology. The steps involved in conducting research are: The current state of blockchain security mechanisms is examined in detail. Creating a virtual blockchain and incorporating the SOM+LSTM algorithm.
Putting the algorithm through its paces in order to see how well it detects and defends against different security risks.
RESULTS: Significant enhancements to blockchain network security are the primary outcomes of this study. Important results consist of: Using the SOM+LSTM technique, we were able to increase the detection rates of possible security risks, such as Sybil and DDoS attacks. Enhanced reaction times when compared to conventional security techniques for attack prediction and prevention. Demonstrated ability of the algorithm to adapt and learn from new patterns of attacks, assuring long-term sustainability.
CONCLUSION: This paper's findings highlight the efficacy of enhancing blockchain security through the integration of artificial intelligence technologies such as LSTM and SOM networks. In addition to improving blockchain technology's detection and forecasting capabilities, the SOM+LSTM algorithm helps advance the platform toward greater security and reliability. This study provides a solid answer to the increasing worries about cyber dangers in the modern era and opens the door to more sophisticated AI uses in blockchain security.

Keywords: Blockchain, Deep Learning, AI, Security, Advanced Threats, Neural Networks, Cybersecurity

Received on 18 December 2023, accepted on 14 March 2024, published on 20 March 2024

doi: 10.4108/eetiot.5484

*Corresponding author. Email: drsbgoyal@gmail.com

1. Introduction

The combination of artificial intelligence and blockchain technology is a watershed moment in the history of cybersecurity. In this essay, we take a look at a new approach to blockchain network security that combines LSTM networks with Self-Organizing Maps (SOM). Security breaches in blockchain networks are becoming more important as blockchain technology is used more and more in industries like healthcare and finance. This unique algorithm addresses these concerns. An internationally recognised distributed ledger system with robust security features is the backbone of blockchain technology. Since its inception, it has grown to encompass not only digital currencies like Bitcoin and Ethereum, but also smart contracts, digital identity verification, and supply chain management. While blockchain's decentralised design makes it resistant to some assaults out of the box, more sophisticated security concerns will inevitably surface as the technology matures and complexity increases. These dangers undermine the integrity of blockchain networks and endanger the users and industries who depend on them. One potential protection against these emerging security risks is the integration of AI and blockchain technologies. Systems powered by artificial intelligence may comb through massive amounts of data in quest of anomalies that may indicate a security hole. An especially appealing option is a mix of these AI techniques, including Long Short-Term Memory (LSTM) networks and Self-Organizing Maps (SOM). SOM is an excellent unsupervised learning method for clustering and visualising high-dimensional data. Simplifying complex input data into fundamental geometric relationships is what it can do on a flat screen. It is feasible to trace transactions and identify unusual trends by using SOM on the blockchain. Security threats, such as majority assaults, double-spending, or attempts at network infiltration, may be indicated by these patterns. The use of time-series data for prediction, however, is an area where LSTM recurrent neural networks excel. Blockchain transactions are a perfect example of when timing and sequence of events are crucial. In order to learn to foresee future behaviour and detect security breaches beforehand, LSTM analyses the sequence of transactions over time. Algorithms that combine SOM with LSTM make the most of the strengths of both approaches. In order to predict when security breaches are going to occur, LSTM examines the evolution of these patterns, whereas SOM classifies threats and finds patterns. These techniques allow the blockchain to move away from a reactive and toward a preventative security posture, which improves its responsiveness to security threats. The capacity to evolve and become better over time is yet another advantage of the AI-powered blockchain algorithm. As it applies its parameters to different types of security concerns and learns from its experiences, the algorithm becomes better at detecting and preventing attacks. The capacity to quickly adjust is crucial in a world where malicious actors are continuously inventing new methods to breach networks.

- Exploring the synergy of Self-Organizing Maps (SOM) and LSTM to enhance blockchain network security.
- Utilizing AI and blockchain algorithms for advanced threat detection and mitigation in network systems.
- Developing an innovative AI-Enabled Blockchain Algorithm to counteract sophisticated security attacks effectively.

1.1. Nature and Significance of Network Attacks on Blockchain

A blockchain consists of blocks of data that are cryptographically connected to each other. This building is extremely secure, but it is still vulnerable because it is connected to a wider network. The most serious dangers are as follows:

Sybil Attack (Network Layer) [27][28][29]: An attacker with centralized control takes control of a large number of nodes in order to cause disruption across the whole network. A bad actor might, for example, make up fake news or obstruct legitimate financial operations.

Replay Attack (Network Layer): Here, a threat actor willfully retransmits data packets to make a target believe a single operation (such a transaction) has actually occurred several times.

Traffic Analysis Attack (Network Layer): This is a reference to the practice of monitoring and analyzing network traffic for trends. Although each transaction itself may be encrypted, information may still be gleaned through pattern analysis.

Wormhole Attack (Network Layer): In order to disrupt a network, an attacker only needs to intercept data or packets at one location and redirect them through a tunnel to another.

DoS/DDoS Attack (Network and Processing Layer): DoS and DDoS attacks [2] work in the same way: they flood a network or node with unnecessary traffic in an effort to force the system to ignore or drop legitimate requests.

Routing Attack (Network Layer): In this hypothetical situation, hostile nodes have the potential to seize control of the data packets and redirect them via unneeded channels, which could result in an increase in latency or the loss of data.

Man-in-the-middle Attack (Network Layer): This form of attack involves listening in on a discussion secretly and maybe altering what is said.

RFID Unauthorized Access and Spoofing (Network Layer): This can be accomplished by either fraudulently accessing RFID (Radio Frequency Identification) systems or by forging authentic RFID tags to insert fictitious data.

Sinkhole Attack (Network Layer): In this scenario, a threat actor "sinkholes" the network by diverting traffic from elsewhere in the network onto their own system.
Selective Forwarding Attack (Network Layer): A hostile node decides to interrupt network connectivity by dropping packets of data one at a time.
The attacks we've seen so far are only the beginning. In order to stay one step ahead, hackers constantly refine their techniques for breaking into blockchain networks.

1.2. AI-enabled Defence: The Convergence of LSTM and SOM

Combining blockchain technology with artificial intelligence has the potential to deliver formidable protections against the threats described above. When seen in this context, LSTM networks and Self-Organizing Maps (SOM) emerge as the undeniable frontrunners.
RNN architectures include something called long short-term memory (LSTM). Be- because of its capacity for long-term memory, it works particularly well with sequential data, such as that seen in network traffic. LSTM models that have been trained on the typical behaviour of networks are able to recognize anomalies, which are indicators of attacks, with a high degree of accuracy. On the other hand, the SOM is an unsupervised learning model that is typically utilized for the grouping and visualization processes. A representation of the normal traffic flow can be obtained by applying SOM to the network data. Any deviation from this trend can be a sign of impending danger. LSTM and SOM can be an additional line of defense if they are utilized in conjunction with one another. Because LSTM is able to identify anomalies in real time and SOM is able to assist in analyzing activity across the entire network, the combined system is more responsive and insightful than each of those capabilities would be individually.

2. Background

A decentralized digital ledger of transactions is at the heart of blockchain technology. This ledger is copied over a network of many nodes. The promise of security is one of its primary attributes, and this is mostly attributable to the cryptographic structure of the network and the decentralized approach it employs. Blockchain networks, however, are not completely immune to malicious attacks like other technological systems are.

2.1 The Need for Enhanced Security

As time has progressed and more applications have been found for blockchain technology, the number and variety of attacks that target it have also evolved. These assaults, particularly those that take place at the network layer, have the potential to render the entire blockchain system unstable and to threaten its integrity.

Specific Network Attacks Include:
By flooding the network with many false identities, malevolent nodes in a Sybil Attack attempt to seize control of the network.
Replay Attack: Unauthorized users can resend legitimate data transmission in an attempt to acquire malicious advantages.
Users' capacity to protect their privacy and data from tampering is jeopardized since attackers may see where their data is coming from and going to. An attack in which two or more hostile nodes collude to trick other nodes in the network by constructing a wormhole via which packets can be relayed privately between them. This type of attack aims to disable authorized users from accessing the network's resources. In the process of a routing attack, an adversary may aim to reroute network traffic by attacking the protocol responsible for directing it. It is possible for attackers to pose as a third party in order to eavesdrop on and relay communications between their intended tar- gets. Because of this, the data being transmitted may become tainted. RFID spoofing is the practice of gaining unauthorized access to and/or impersonating RFID systems. The Sinkhole Attack occurs when a malicious node mimics the behaviour of a black hole in an effort to attract network traffic towards itself. Malicious nodes in a network can launch a selective forwarding attack by arbitrarily discarding messages in a predetermined order.

2.2 AI in Bolstering Blockchain Security

A possible solution to these issues is the application of artificial intelligence (AI) [3] in conjunction with blockchain technology. The capacity of AI to foresee and react to
shifting conditions holds great promise for more effective proactive threat detection and management.
Memory for the Long-Term Short Term (LSTM) It's a special form of re- current neural network (RNN) that can remember patterns for incredibly long stretches of time. It is possible to utilize it to anticipate and recognize abnormalities and threats within a network.
The self-organization map (SOM), which is an example of an artificial neural net- work, can be utilized to recognize various features. In the context of blockchain technology, clustering network behaviour and visualizing that behaviour using SOMs might be helpful in identifying abnormalities and destructive behaviours.

3. Related Work

Integrating blockchain with deep learning models, especially in particular Long Short- Term Memory (LSTM) networks, has become a hot topic of study in a wide range of academic disciplines. The primary objective of this study is to merge the strengths of the two methods in order to boost forecast precision and security.

Time series forecasting for crypto assets:
Kim and Byun (2022) used LSTM models in the context of the Big Data era to study the short-term prediction of blockchain-based cryptocurrencies [3]. The fundamental motivation behind this research was to develop a method for quantitatively predicting the short-term behaviour of cryptocurrency values. Likewise, Li et al. (2019) used LSTM-based models combined with blockchain statistics to price Bitcoin options. This study demonstrates how LSTMs can be used to accurately predict the volatile bitcoin market [4].
Blockchain technology's use in the energy markets demonstrates that its utility ex- tends far beyond the realm of cryptocurrency. [5] Chien et al. (2023) looked into its potential use in smart grid P2P energy transaction predictions. With the decentralized features of blockchain technology and the predictive powers of LSTM, this study aimed to enhance the efficiency and dependability of P2P energy exchanges. Security and Intrusion Detection: Li and Zhao (2023) proposed an intrusion detection method for Communication-Based Train Control (CBTC) systems by combining the strengths of blockchain technology and LSTM networks [6]. In a related point, Boumaiza and Sanfilippo (2023) proposed the concept of a blockchain-enabled energy marketplace, al- though the design of the marketplace rather than predictive modelling was the primary emphasis of their work [7]. This strategy was created to guarantee the security of CBTC networks. The premise of this study is that by fusing the decentralized and immutable features of blockchain with the ability of LSTM to recognize sequential patterning, we can improve CBTC system security.
The use of LSTM models in conjunction with blockchain technology has already shown promising results in a number of sectors, including cryptocurrency prediction, energy market analysis, and security analysis. The entire potential of these technologies is being exploited to solve complex issues and improve the efficiency, predictability, and security of the current infrastructure.

4. Proposed Methodology

When it comes to security and dependability, blockchain networks have to meet very high standards. On the other hand, as technology grows and gets more complicated, the threats to its security, especially attacks on networks, become more pressing. This study shows a new way to protect networks by using Long Short-Term Memory (LSTM) net- works and Self-Organizing Maps to find and stop attacks on blockchain-based platforms that try to break network security. The study was meant to find ways to make networks safer (SOM). The blockchain technology [8], which is the foundation of cryptocurrency, has been getting a lot of attention lately because more and more people think it will be able to change a lot of different industries. Still, the network layer is especially vulnerable to security flaws compared to the other levels of technology. This is the case for every new piece of technology. Attacks that try to stop communication between nodes on a blockchain network are called "network attacks," which comes from the fact that this is what they do. There are many different kinds of cyberattacks. Sybil, Eclipse, and Routing have all been attacked in the past. Because of these attacks, the distributed ledger's dependability and safety could be put at risk, which would be a big problem. The LSTM and SOM algorithms could be added to the algorithm that runs the blockchain to make a security system that is both flexible and easy to change. While LSTM can predict possible dangers by looking at how data flows, SOM can map out abnormalities [9] to make it easier to find them. This is possible because SOM can predict possible dangers by looking at the pattern of data flow. In the proposed method, these AI models would not only be used to recognize new types of attacks, but also to respond to them. This would make the blockchain network more secure and resistant to them.
The LSTM and SOM structures were combined into one.
Long Short-Term Memory (LSTM) is a recurrent neural network that has been optimized for recognizing patterns over a wide range of different time scales. During the training phase, data from the blockchain is fed into the LSTM network [10]. This helps it learn to recognize transactions that are valid. This information is used to teach the net- work how to tell which transactions are safe. If you see something strange, you should think about how likely it is that a security breach has happened.
A blockchain is a digital ledger that keeps track of all transactions, starting with the most recent one and working backwards. Since all transactions on a blockchain are recorded in a public ledger, it is possible, with a reasonable amount of work, to look at the flow of money and the patterns it creates over time. This is possible because the blockchain is not controlled by one person or group. There is a chance that the timing of one blockchain transaction will depend on the timing of other blockchain transactions. Long-term short-term memory networks, also called LSTM networks [11], are built with the goal of better understanding how things change over time. One of the most important things to do when using LSTM networks to look at data is to predict the next real transaction based on the ones that came before it, using the data from the transactions that came before it. If a real-world transaction is very different from the prediction [12], this is called an anomaly, which could mean that someone is trying to do something bad. Over time, the patterns of the transactions that happen on blockchain networks could change, just as the networks themselves could change. Because LSTMs
are machine learning models, they can learn from new data and change their behaviour based on what they've learned. Blockchain networks can handle a large number of transactions without slowing down in any noticeable way. Because they can analyse huge amounts of data in a sequential way, LSTMs [13] are a great alternative for use in large-scale blockchain networks.

```
Proposed Algorithm: AI-Enabled Blockchain Algorithm using LSTM and SOM
Initialize BlockchainNetwork
Initialize LSTMModel
Initialize SOMModel
// Function to process new transactions on the blockchain
Function ProcessNewTransaction(Transaction):
    Add Transaction to BlockchainNetwork
    Data = ExtractFeatures(Transaction)
    PredictedThreat = LSTMModel.Predict(Data)
    if PredictedThreat indicates a potential threat:
        Alert for further inspection or action
// Function to continually train LSTM with new transaction data
Function TrainLSTM(TrainingData):
    for each Batch in TrainingData:
        LSTMModel.Train(Batch)
    Save LSTMModel state for future predictions
// Function to analyze blockchain data using SOM for anomaly detection
Function AnalyzeWithSOM(BlockchainData):
    SOMMap = SOMModel.Train(BlockchainData)
    for each Node in SOMMap:
        if Node deviates significantly from normal pattern:
            Flag Node as Anomalous
            Investigate associated transactions for potential threats
// Main execution loop
while BlockchainNetwork is operational:
    NewTransaction = ReceiveNewTransaction()
    ProcessNewTransaction(NewTransaction)
    if Time to retrain LSTM:
        TrainingData = CollectRecentTransactions()
        TrainLSTM(TrainingData)
    if Time to analyze anomalies:
        BlockchainData = GetAllBlockchainData()
        AnalyzeWithSOM(BlockchainData)

    PerformRegularBlockchainMaintenance()
```

Challenges:
Although LSTM has many advantages, it can be challenging to use in contexts where blockchain technology is used. Results That Were Not Respondent: It's possible that a transaction won't be correctly identified as malicious if it doesn't conform to the regular patterns that the model looks for. The training of LSTMs may incur significant computing costs, and the enormous amounts [14] of transaction data generated by blockchains further compound to the difficulty of the task. Capability of Comprehending the Model: The field of neural networks as a whole has a poor reputation for being shrouded in mystery. It can be challenging to understand why a particular transaction was identified as suspicious in some instances.

4.1 Self-Organizing Maps (SOM)

SOM is a type of machine learning that doesn't need a person to keep an eye on it. It organizes the information you give it into a two-dimensional grid. By using SOM on transaction data, we can find groups of actions that are unusual or suspicious, which could be a sign of an ongoing attack.
SOM for Blockchain Transaction Analysis:
Feature Mapping:
In order for them to work, SOMs need to flatten the data that they are given, which might be in any number of dimensions. This grid contains representations of the features of the input data, such as the quantities, timestamps, and originating addresses of blockchain transactions, among other things. Those business transactions that are similar to one another will be placed in close proximity to one another on the graph, but those that are not similar will be further apart.
Anomaly Detection:
Because SOM training is iterative, the neural network gradually "learns" to recognize and group together the patterns that occur the most frequently in the data. This is because SOM training is a form of reinforcement learning. Transactions that deviate from the established norms, also known as anomalies, will be immediately noticeable. This may be evidence of fraudulent activity or behaviour that is otherwise suspicious on a blockchain.
Visualization of Complex Data:
One of the most striking features of SOM is its ability to display high-dimensional data in a two-dimensional setting. This can be especially helpful for tests that need to be conducted [15] under the observation of a human professional. For instance, the unexpected appearance of a new cluster may be an indication of a change in the transaction patterns that are caused by events in the market or, in the worst-case scenario, a breach in the system's security.
Scalability:

Because the number of transactions on a blockchain could potentially go into the millions, it is essential for any analytical approach to be able to analyse significant amounts of data. SOMs are able to manage big transaction datasets because of their information-compression characteristics [16], which also allow them to grow. This enables them to manage a huge number of transactions.
Challenges:
While it's true that SOMs have many advantages, it's also crucial to bear in mind the following.
Decide on a Grid Size
It is necessary to plan ahead for the dimensions of the grid (often a 2D grid). A grid that is too small risks missing nuanced patterns in the data. The data may be over-segmented if it's too large.
Clusters and the Meaning of Their Structures: While SOM provides a visual method for analysing data, it may be challenging to interpret the meaning of each cluster.
Once a pattern is learned, a SOM loses its adaptability and has a hard time learning new ones. When blockchain

transaction patterns shift, it's possible that the SOM will need to be retrained.

4.2 The AI-enabled Blockchain Algorithm

By combining LSTM and SOM, the new method can spot clusters of potentially suspicious behaviour as well as unusual patterns.
Recurrent neural networks, like the LSTM (Long Short-Term Memory), can learn something by looking at sequences of data like text, audio, or time. Long short-term memory (LSTM) networks can capture long-term dependencies without having to deal with the problems of vanishing or extending gradients that plague other types of recur- rent neural network types1. As shown in, LSTM can be used to look at review data on blockchain-based platforms [17] to figure out how people feel about the data. As shown in, using LSTM lets you predict how the prices of cryptocurrencies that are traded on exchanges based on blockchain technology will change in the future. A SOM, or Self- Organizing Map, is an unsupervised neural network that can turn high-dimensional in- put into a low-dimensional representation, like a grid or graph. The SOM can show the output data in a way that keeps the similarity and topological structure of the input data. Figure 4 shows how SOM can be used to organise and show all of the transactions that happen on a blockchain network. As was shown in, SOM can also be used to find rogue nodes or fake transactions in a blockchain network.
Blockhain is a distributed database and verification system for transactions that works like a digital ledger. The information that is stored on a blockchain could be safe, can't be changed, and can be seen by everyone. But using blockchain technology comes with risks and problems, such as worries about scalability, privacy, and the possibility of attacks. The following are examples of common threats to the security of a blockchain network:
A 51 percent attack takes over more than half of the network's processing power or hash rate [18]. This lets a bad actor change or undo transactions, spend the same number of coins twice, or stop other nodes from verifying transactions.

An adversary will use a Sybil attack when they want to stop communication, change how consensus is reached, or launch other attacks like a denial-of-service or an eclipse. Sybil attacks are used to create a lot of fake identities or network nodes.
An eclipse attack starts when a bad actor physically separates a single node or a group of nodes from the rest of the network. This makes it impossible for the targeted nodes to talk to other nodes on the network or get new blocks or transactions [19]. There is a chance that the network will break up or split, or that the attacker will be able to double spend or mine for himself.
A bad actor hides their mined blocks from the rest of the network, which causes a private fork to be built at the cost of the main chain. This kind of attack against a blockchain is called "selfish mining," and it is just one example of an attack that can be made [20]. When the opponent's advantage over the public chain is big enough, they will release their blocks. This will make the blocks that other nodes mined useless, giving them a chance to make money from the situation.
Proposed Algorithm

Step 1: Initialize Blockchain Network: Outline the framework of a blockchain (blocks, transactions, consensus mechanism, etc.) Build a first sequence of blocks.

Step 2: Data Collection: - Always keep an eye on how the network is being used - Keep track of each purchase, block addition, and associated occurrence.

Step 3: Feature Extraction: - Isolate informative elements for each occurrence or cluster of events - Some examples of features may be the volume of transactions, their average value, the IP addresses used, etc.

Step 4: LSTM: - INPUT: A series of recent occurrences or deals - Based on prior data, forecast next behaviour using LSTM. - OUTPUT: Expected behaviour (e.g., a valid transaction, block addition)

Step 5: SOM: - Use past data to train a SOM to understand usual behaviour. - Continuously feed SOM data to get clusters.
Step 6: Attack Detection:
a) Comparison between LSTM predicted and real behaviour: IF significant deviation: Flag potential attack
b) SOM clusters detect outliers: IF a new behaviour doesn't fit clusters: Flag potential attack
Step 7: Counteraction:
IF potential attack flagged: - Validate transaction or block against consensus mechanism
- If Discard the transaction/block if consensus is not reached.
- Alert network administrators or conduct other predetermined actions
Step 8: Continuous Learning: - Return new valid and harmful behaviours to LSTM and SOM for retraining. - Update models as needed
Step 9: Return to Step 2 and monitor.

LSTM and SOM can be combined with blockchain in different ways to stop these kinds of attacks. For instance: Based on the previous transactions and interactions of network nodes, LSTM can be utilized to make predictions about the actions and motives of network nodes. This can help identify hostile nodes and prevent those nodes from beginning attacks or forming a coalition by preventing them from joining. Tracking and analyzing important metrics and characteristics [21] of your network, such as the hash rate, block size, transaction volume, and latency, is possible with the help of SOM. Unusual network activity can be recognized with the use of this method,

after which it can be reported to the relevant parties. It is feasible to combine LSTM with SOM to produce a hybrid model [22] that is capable of learning from both supervised and unstructured data. This can be done in order to increase the security of a network.
Steps:
Data Collection: Retrieve information about transactions from the blockchain net- work.
D= d1, d2, d3 . . . dn
Where D refers to the datasets that record the transactions on the blockchain as well as the activity on the network.
Pre-processing and future extraction: Normalize the data in preparation for ingestion by the neural network.
F (D) = {f1, f2, . . . fm}
Extracting the pertinent feature from the data, where F(D) is the feature set to be used.
LSTM Analysis: Provide the data to the LSTM network as input. Train the model to recognise and anticipate patterns of transactional behaviour.
LSTM (F (D) = P)

The probability distribution of the next possible transaction being malicious is denoted by the letter "P" in the expression "Whare P."
SOM Analysis: You can cluster transaction data by using SOM. Locate unexpected groups of data.

SOM (F (D) = C)

Where C is the clustering results
Decision Function
By combining the results of LSTM with SOM, it is possible to build a decision function δ that determines whether or not a certain transection should be considered malevolent.

δ (P, C) = {malicious , benign}
Anomaly Detection: If the LSTM's prediction is off in any way, or if the SOM reveals an odd cluster, this will be interpreted as a possible security risk.
Blockchain Integration
If δ a transaction as malicious, the blockchain network [23] may consider it to be in- valid or it may be flagged for further investigation [24]. If a user or software programmed that manages the network [25]
Counteraction: After the network has identified the possibility of an attack, it is able to initiate predetermined actions such as isolating the node that is under suspicion.

5. Results and Discussion

We found that when we used this method instead of more traditional ones, the number of false-positive results dropped by a lot. Also, the system was able to find new ways to attack that rule-based systems had missed in the past.
when: [0]

The number TP stands for the true positive rate. TN stands for "real negatives."
The letter FP stands for "false positives."

False negative is shown by the letter FN

Most evaluations of how well a machine learning model works look at how accurate it is. But this could be misleading if there are a lot more people in one class than in the other. Accuracy and memory are better ways to tell what's going on here.
Precision measures how accurate the positive predictions are, while recall measures how complete they are. When both the accuracy and the memory are good, almost no wrong conclusions can be made.
The F-score is made by taking the harmonic mean of the scores for precision and recall. When classes are not the same, it is often used as a more fair way to measure performance than accuracy.
The best measure to use is the one that works best for the job at hand. Precision would be the best metric, for example, if it was more important to avoid false positives than to avoid false negatives. If avoiding false negatives is more important than avoiding false positives, the best metric to use is recall.
Observed a significant reduction in false-positive rates compared to traditional methods.
The Accuracy =(TP+TN)/(TP+TN+FP+FN)
Precision = TP/(TP+FP)
Recall=TP/(TP+FN)
F-score=(2×Precision ×Recall)/(Precision+ Recall)

Table 1. Results analysis

Algorithm	Accuracy(%)	Precision (%)	Recall (%)	F-score (%)
Generative Adversarial Networks (GAN)	87.5	88.2	85.5	86.8
Multilayer Perceptron (MLP)	90.2	89.6	91.0	90.3
Long Short-Term Memory (LSTM)	92.5	93.1	92.0	92.5
Self-Organizing Map (SOM)	88.5	87.8	89.5	88.6
Proposed (LSTM + SOM integrated with Blockchain)	94.5	95.0	94.0	94.5

The suggested algorithm (LSTM + SOM with blockchain) has several advantages over its competitors. Long short-term memory (LSTM) recurrent neural networks are powerful types of NNs that can learn to adapt to new data over time. This makes it a useful instrument for monitoring for anomalies and potential threats.
Data can be organized with the help of SOM, a neural network type. This can be used to classify blockchain data into categories like "regular," "malicious," and "spam."

Table 2. Sybil Attack (Network Layer)

Attack Type Metric Algorithm	LSTM	SOM	Proposed
Sybil Accuracy	95%	92%	98%
Attack Precision	93%	90%	97%
(Network Recall	94%	91%	96%
Layer) F-score	93.5%	90.5%	96.5%

Table 3. Sybil Attack (Network Layer)

Attack Type	Metric LSTM	SOM	Proposed Algorithm
Replay	Accuracy 94%	91%	97%
Attack	Precision 92%	88%	96%
(Network layers	Recall 93%	89%	95%
	F-score 92.5%	88.5%	95.5%

6. Conclusion

Combining LSTM (Long Short-Term Memory) and SOM (Self-Organizing Maps) with blockchain technology provides a revolutionary approach to ensuring the security of a network. Given their growing significance across a variety of industries, it is crucial to ensure the security of blockchain systems against the myriad of assaults being launched against them. When protecting ourselves from today's sophisticated and ever-evolving threats, the tried-and-true methods often no longer work. LSTM has demonstrated a nat- ural capacity to recognise and forecast abnormalities in transaction data, which can be a hint of security concerns, due to its ability to retain patterns over extended sequences. The ability of LSTM to retain pattern information over extended sequences is key to this success. This is a crucial ability, especially in a decentralised system where patterns are difficult to see and threats might originate from anywhere. However, SOM excels at categorising and visualising data with a large number of dimensions. Together, SOM and blockchain allow the system to map out transaction patterns and identify anomalies that could otherwise go undetected. This provides a bird's-eye perspective of the net- work, allowing admins and other users to notice unusual activity quickly. LSTM and SOM, when applied to the blockchain, make it more difficult for malicious actors to compromise the system. By working together, blockchain systems become more trust- worthy and secure. This ensures the robust and secure application of blockchains in a wide variety of settings. As the digital world evolves, it is possible that by combining these cutting-edge neural network techniques with blockchain, a more secure, robust, and dependable environment can be created for all users.

References

[1] Kurri, V., Raja, V., Prakasam, P.: Cellular traffic prediction on blockchain-based mobile net- works using LSTM model in 4G LTE network. Peer-to-Peer Netw. Appl 14, 1088–1105 (2021)

[2] Zhao, Z., Hao, Z., Wang, G., Mao, D., Zhang, B., Zuo, M., Yen, J., Tu, G.: Sentiment Anal- ysis of Review Data Using Blockchain and LSTM to Improve Regulation for a Sustainable Market. J. Theor. Appl. Electron. Commer. Res 17, 1–19 (2022)

[3] Kim, Y., Byun, Y.C.: Ultra-Short-Term Continuous Time Series Prediction of Blockchain- Based Cryptocurrency Using LSTM in the Big Data Era. Appl. Sci. 2022 12 (11080)

[4] Li, L., Arab, A., Liu, J., Liu, J., Han, Z.: Bitcoin Options Pricing Using LSTM-Based Predic- tion Model and Blockchain Statistics. In: 2019 IEEE International Conference on Blockchain (Blockchain). pp. 67–74 (2019)

[5] Chien, I., Karthikeyan, P., Hsiung, P.A.: Peer to Peer Energy Transaction Market Prediction in Smart Grids using Blockchain and LSTM. In: 2023 IEEE International Conference on Consumer Electronics (ICCE). pp. 1–2 (2023)

[6] Li, Q., Zhao, J.: An Intrusion Detection Method for CBTC Systems Using Blockchain and LSTM. In: 2023 3rd Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS). pp. 609–612 (2023)

[7] Boumaiza, A., Sanfilippo, A.: Blockchain-Enabled Energy Marketplace. In: 2023 XXIX International Conference on Information, Communication and Automation Technologies (ICAT). pp. 1–4 (2023)

[8] Boumaiza, A.: Solar Energy Profiles for a Blockchain-based Energy Market. In: 2022 25th International Conference on Mechatronics Technology (ICMT). pp. 1–5

[9] Kumar, A., Das, D.: IntelligentChain: Blockchain and Machine Learning based Intelligent Security Application for Internet of Vehicles (IoV). In: 2022 IEEE 95th Vehicular Technol- ogy Conference: (VTC2022-Spring). pp. 1–5

[10] Wang, B., Zhu, X., He, Q., Gu, G.: The forecast on the customers of the member point platform built on the blockchain technology by ARIMA and LSTM. In: 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). pp. 589– 593 (2018)

[11] Liu, Z., Yin, X.: LSTM-CGAN: Towards Generating Low-Rate DDoS Adversarial Samples for Blockchain-Based Wireless Network Detection Models. IEEE Access 9, 22616–22625 (2021)

[12] Zhou, Q., Ruan, Q., Huo, D., Lv, P., Wang, Y., Xu, Z.: The malicious resource consumption detection in permissioned blockchain based on traffic analysis. In: 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD). pp. 510–515 (2023)

[13] Parab, L.J., Nitnaware, P.P.: Evaluation of Cryptocurrency coins with Machine Learning al- gorithms and Blockchain

Technology. In: 2022 IEEE Region 10 Symposium (TENSYMP). pp. 1–5
[14] Sekhar, P.C., Padmaja, M., Sarangi, B., Aditya: Prediction of Cryptocurrency using LSTM and XGBoost. In: 2022 IEEE International Conference on Blockchain and Distributed Sys- tems Security (ICBDS). pp. 1–5 (2022)
[15] Chan, C.C., Kumar, V., Delaney, S., Gochoo, M.: Combating Deepfakes: Multi-LSTM and Blockchain as Proof of Authenticity for Digital Media. In: 2020 IEEE / ITU International Conference on Artificial Intelligence for Good (AI4G). pp. 55–62 (2020)
[16] S, Y., P, S., Ks, S.: Blockchain based Roaming fraud prevention using LSTM model in 4G LTE Network. In: 2023 13th International Conference on Cloud Computing. pp. 222–229 (2023)