Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

A Secure Blockchain Framework for Privacy Preserving in Supply Chain Management based on Hybrid Autoencoder and LSTM Neural Network

Ritesh Kumar Singh[1], Udai Shanker[2]
[1]Research Scholar, [2]Professor, Department of CSE, M. M. M. University of Technology, Gorakhpur, UP, India
E-mail: [1]riteshvns53@gmail.com, [2]udaigkp@gmail.com

Article History:
Received: 11-11-2024
Revised: 17-12-2024
Accepted: 12-01-2025

Abstract:
Risk identification and mitigation are essential for maintaining resilience and efficiency in the ever-changing field of supply chain management (SCM). The intricacies and uncertainties inherent in modern supply networks are often too complex for traditional risk management techniques to effectively address. In order to enhance risk detection and management in supply chain management, this study explores a hybrid strategy that blends blockchain technology with deep learning. Blockchain ensures data integrity and transparency by offering a transparent and decentralized system for supply chain operations monitoring. This process is improved by deep learning, which analyses vast volumes of historical and current data to identify patterns, predict threats, and suggest countermeasures. The proposed system leverages the inviolability of blockchain technology and the predictive capabilities of deep learning to address important challenges such as fraud detection, demand forecasting, supplier evaluation, and disruption prediction. The dataset is secured with the use of hybrid Autoencoder and LSTM based deep neural network. Autoencoder is used for dimensionality reduction and reducing the noisy as well as redundant data which is further passed through LSTM based neural network to enhance the security over the blockchain based transaction data.

Keywords: Supply Chain Management, Blockchain, LSTM, Autoencoders, Risk Management, Privacy Preserving.

1. Introduction

Many businesses are building trustworthy supply chains in the current globalization era in order to gain a competitive advantage by offering their customers the best value. Supply chain management, or SCM, has become crucial for handling risk, change, and the complexities of international sourcing. For the organization to reap the greatest benefits, its supply chain must be completely interconnected.

Top companies now prioritize supply chain management (SCM) as a means of increasing market share, profitability, competitive advantage, and shareholder value. In fact, the term "SCM" has changed over the past few decades from "Distribution" to "Logistics" and finally to "Supply Chain Management" [1]. Mass production, specialization, and globalization are the foundations of modern industrial civilization. Nowadays, almost no company or industrial facility produces the entire product. A supply chain is a collection of different businesses that work together to create a product that meets consumer needs. The strategic planning and control of the movement of commodities to shorten time to market, minimize inventory levels, lower overall costs, and improve customer satisfaction and experience is all included in supply chain management.

1.1 SCM Risk Management

The potential for injury or loss is referred to as risk. exposure to the potential of loss, the degree of probability connected with that loss, a hazard or peril, and the risk of damage or loss. Uncertainty about the future gives rise to risks, and since exact results are impossible to achieve, risk is always there. 'Risk' and 'uncertainty' are sometimes used synonymously, although they have a fundamental

difference. The ability to list possible future events but not knowing which will occur or their respective probability is known as uncertainty. The ability to list possible future events and give each one a chance is known as risk [3]. The topic of "risk management" usually comes up when managers discuss uncertainty, risk, certainty, and ignorance. Risk management is a methodical approach to identifying, mitigating, and assessing risks in order to reduce losses brought on by insufficient risk management. [4] [5].

• **Risk Recognition:** Helps identify any threats to the system.

• **Risk Analysis and Evaluation:** It helps prioritize, assess, and put into practice the suggested control mechanisms inside the system.

• **Risk reduction:** To evaluate and ascertain whether the current control approach is applicable to the system.

1.2 Need for Blockchain Technology in Supply Chain Management (SCM)

Supply Chain Management (SCM) involves the coordination of activities required to produce and deliver goods, from raw material sourcing to the final consumer. Despite its importance, traditional SCM systems face challenges like lack of transparency, inefficiencies, and susceptibility to fraud. Blockchain technology addresses these issues by introducing a secure, decentralized, and transparent framework for managing supply chain operations. [2]

1.3 Challenges in Traditional SCM

1. **Lack of Transparency:** Limited visibility into the movement of goods and raw materials across the supply chain.
2. **Data Silos:** Fragmented systems make it difficult to share and synchronize information among stakeholders.
3. **Fraud and Counterfeiting:** High risk of counterfeit goods entering the supply chain.
4. **Inefficiencies:** Manual record-keeping and delays in verification processes lead to inefficiencies and increased costs.

1.4 How Blockchain Addresses SCM Needs

1. **Enhanced Transparency:**
   - Blockchain creates an immutable ledger where every transaction or event is recorded and accessible to all authorized stakeholders. This ensures end-to-end visibility in the supply chain.
2. **Improved Traceability:**
   - Each product's journey, from origin to final delivery, can be tracked in real-time. This is crucial for industries like food and pharmaceuticals where provenance matters.
3. **Data Security and Integrity:**
   - Blockchain's cryptographic security ensures that data cannot be altered or tampered with, building trust among stakeholders.
4. **Efficient Operations:**
   - Automated smart contracts streamline processes such as payment settlements and compliance checks, reducing delays and manual intervention.
5. **Fraud Prevention:**
   - Blockchain’s immutable records make it nearly impossible for counterfeit products or falsified data to enter the supply chain.
6. **Collaboration and Trust:**

- By enabling secure data sharing among participants, blockchain fosters collaboration and reduces conflicts arising from information asymmetry.

Blockchain technology addresses the critical challenges in SCM by providing transparency, traceability, and security. Its integration ensures more efficient and reliable supply chain operations, reducing costs and enhancing trust among all participants. As global trade becomes increasingly complex, the adoption of blockchain in SCM is no longer optional but essential for future-proofing supply chain networks. [6, 7, 8]

1.5 Integration of Blockchain and Deep Learning in Supply Chain Management

The integration of blockchain technology and deep learning (DL) in Supply Chain Management (SCM) is reshaping how organizations manage and optimize their supply chain networks. Blockchain ensures secure, decentralized, and transparent data sharing, while deep learning leverages advanced neural networks to extract patterns, make predictions, and automate complex processes. Together, these technologies address challenges such as inefficiencies, fraud, and the need for real-time decision-making in increasingly complex supply chains. [9]

1.6 Blockchain and Deep Learning Work Together in SCM

1. **Data Authenticity and Security:**
   - Blockchain ensures the integrity of data by providing a tamper-proof ledger, which serves as a reliable foundation for deep learning models.
2. **Advanced Predictive Analytics:**
   - Deep learning algorithms analyze the vast datasets stored on blockchain to predict demand patterns, optimize inventory levels, and identify potential disruptions.
3. **Fraud Detection and Anomaly Identification:**
   - Blockchain enables traceability of goods, while deep learning detects unusual patterns in data that could indicate fraud or counterfeit activities.
4. **Real-Time Decision Making:**
   - Blockchain provides real-time data, and DL models process this data to generate actionable insights, such as rerouting shipments or optimizing production schedules.
5. **Automated Quality Control:**
   - DL models, trained on blockchain-verified data, can analyze images, sensor data, or other inputs to detect defects in products or deviations from quality standards.

1.7 Applications of Blockchain and Deep Learning in SCM

1. **Enhanced Product Traceability:**
   - Blockchain tracks the origin and movement of goods, while deep learning predicts potential disruptions or delays in real-time.
2. **Dynamic Demand Forecasting:**
   - Deep learning uses historical blockchain data to anticipate changes in demand, helping businesses adjust production and distribution strategies.
3. **Supply Chain Risk Management:**
   - DL models analyze blockchain-stored data to identify vulnerabilities, such as supplier delays or geopolitical risks.
4. **Ethical Sourcing and Sustainability:**
   - Blockchain ensures data transparency for ethical sourcing, while deep learning evaluates compliance with environmental and social governance (ESG) standards.

The integration of blockchain and deep learning in SCM creates a transformative synergy that combines trust, transparency, and intelligence. Blockchain ensures reliable data storage and sharing, while deep learning provides the analytical power to optimize supply chain processes and make data-driven decisions. Together, these technologies enhance supply chain efficiency, resilience, and sustainability, offering a competitive advantage in today's global market. [10, 11]

1.8 Motivation

Supply Chain Management (SCM) faces critical security challenges, including data breaches, fraud, counterfeiting, and unauthorized access. The integration of blockchain technology and deep learning (DL) provides a powerful framework to enhance security in SCM by combining immutable data storage with advanced analytical capabilities. This synergy offers innovative solutions to address vulnerabilities, ensuring data integrity, transparency, and robust threat detection. The integration of blockchain and deep learning in SCM enhances security by addressing vulnerabilities through a combination of data integrity, transparency, and intelligent threat detection. Blockchain ensures trust and tamper-proof records, while deep learning provides the analytical power to detect and mitigate risks dynamically. This approach not only safeguards the supply chain but also builds stakeholder confidence, paving the way for a secure and efficient global trade network. [12, 13]

1.9 Blockchain and Deep Learning Enhance Security Together

1. **Anomaly Detection with Verified Data:**
   - Blockchain ensures the authenticity of input data, which deep learning algorithms use to detect anomalies and irregularities in supply chain activities.
2. **Real-Time Fraud Prevention:**
   - Blockchain's real-time data feeds are analyzed by DL models to identify fraudulent transactions or unauthorized activities instantly.
3. **End-to-End Traceability:**
   - Blockchain provides a secure record of goods' provenance, and DL monitors the data to detect inconsistencies or counterfeit products.
4. **Improved Access Control:**
   - Smart contracts on blockchain govern access to sensitive data, while DL monitors access patterns to identify suspicious behavior.

2. Literature Review

Amal et al. [15] propose a blockchain-based system to enhance transparency and fairness in Industrial Internet of Things (IIoT) supply chains. The system leverages blockchain's immutable ledger and smart contracts to facilitate equitable goods exchange between merchants and suppliers. By implementing penalty-based smart contracts, the framework deters malicious behavior and ensures compliance with agreed terms. The authors developed a prototype on the Ethereum platform, demonstrating the feasibility and effectiveness of their approach in real-world applications. Ahamed et al. [16] propose a novel approach to enhance the efficiency of self-driving vehicles within supply chains. The study introduces a Reinforcement Learning Integrated Heuristic (RLIH) search method that leverages blockchain technology to optimize route planning and decision-making processes. By integrating reinforcement learning with heuristic search, the model aims to improve the adaptability and reliability of autonomous vehicles, ensuring secure and transparent operations in supply chain management. In "Anomaly Detection via Blockchained Deep Learning Smart Contracts in Industry 4.0," Demertzis et al. [17] introduce a novel security framework integrating blockchain technology with deep learning to enhance anomaly detection in Industrial Internet of Things (IIoT) environments. The proposed architecture employs smart contracts powered by a trained Deep Autoencoder Neural Network to

identify irregularities in network traffic, ensuring secure and transparent transactions without reliance on a central authority. This approach addresses the increasing complexity of threats in modern industries, offering a decentralized solution for safeguarding critical infrastructure. The paper "Decentralized Security and Data Integrity of Blockchain Using Deep Learning Techniques" by Sazeen et al. [18] explores enhancing blockchain security and data integrity through deep learning. It proposes using convolutional neural networks (CNNs) to detect anomalies and unauthorized access within blockchain networks, aiming to improve transaction verification and overall system reliability.

3. Methodology

The smooth flow of products, services, and information between the many stages of manufacturing and distribution depends on efficient supply chain management. However, supply chain anomalies can lead to disruptions, inefficiencies, and financial losses. These anomalies could be the result of operational issues, potential fraud, or errors in data entry. In order to address these challenges, this paper employs deep learning and blockchain techniques to secure and detect irregularities across a supply chain management (SCM) dataset.

3.1 Dataset Collection

Through the automation of anomaly detection and classification, this study demonstrates how machine learning can address major challenges in supply chain management and offer a workable solution for improving operational and decision-making efficiency. https://www.kaggle.com/datasets/lastman0800/supply-chain-management is the Kaggle dataset that was acquired .

The approach consists of a step-by-step process that starts with data exploration and pre-processing and moves on to anomaly detection, model training, and optimization. Each stage is designed to ensure accurate and efficient anomaly detection within the supply chain management dataset.

3.2 Blockchain framework for SCM

Initially, blockchain was presented as a platform for enabling crypto currencies like bitcoin. It was then created using smart contracts, which include distributed blockchain applications that can be run and verified on their own, and it was used in supply chain management. The majority of blockchain's features have enticed manufacturers to use this technology to deliver their products to consumers. Blockchain technology has disadvantages, such as being vulnerable to numerous attacks and having a poorly defined management structure, even though it streamlines transportation (Supply) by cutting down on processing time and expenses. The technology approach for using blockchain to securely store and track important transactions within a supply chain network is described in this section. The algorithm makes use of blockchain's decentralized and immutable features to increase confidence, dependability, and transparency for all parties.

Blockchain Algorithm for Storing Important Transactions

Step 1: create a blockchain network by selecting an agreement protocol, setting up blockchain nodes, and selecting a blockchain category.

Step 2: Create a Transaction Data Framework

- Create a structure for transactions:

{{transactionID': 'bigint',

'productID': 'varchar',

'timestamp': datetime',

'supplierID': 'varchar',

'location': 'geography',

'status': 'char',

'metadata': 'Char'}

- Hash Sensitive Information:

For extremely sensitive data, use SHA-3 hashing to guarantee data secrecy and indestructibility.

Hashed_productID = SHA-3(productID)

Step 3: Transaction Verification

- Verify if the transaction is valid.
- Use digital signatures to verify the identity of the sender. For instance:

Signature = sign(privateKey, transactionData) is the sender's signature.

Verify (publicKey, signature, transactionData) is how the recipient authenticates.

- Check for Compliance with Smart Agreements:

Only authenticated suppliers are permitted to initiate transactions' is an example of a smart contract that enforces company laws.

Step 4: Add Transactions to the Blockchain

- Distribute the transaction (T) among the blockchain nodes and carry out the consensus process to verify its authenticity. Add a block to the blockchain. Recalculate the Merkle root and compare it to the root given in the block header to confirm the legitimacy of the transaction.

Step 5: Strengthening Security Protocols

- Put Access Control Mechanisms in Place:

To prevent unauthorized access, use smart agreements to establish role-based authorization.

- Use encryption for important data:

Before hashing and storing, encrypt fields such supplier agreements and customer details.

Step 6: Effectiveness and Scaling

- To speed up the retrieval of recent transactions while maintaining inviolability, archive outdated blocks off-chain.

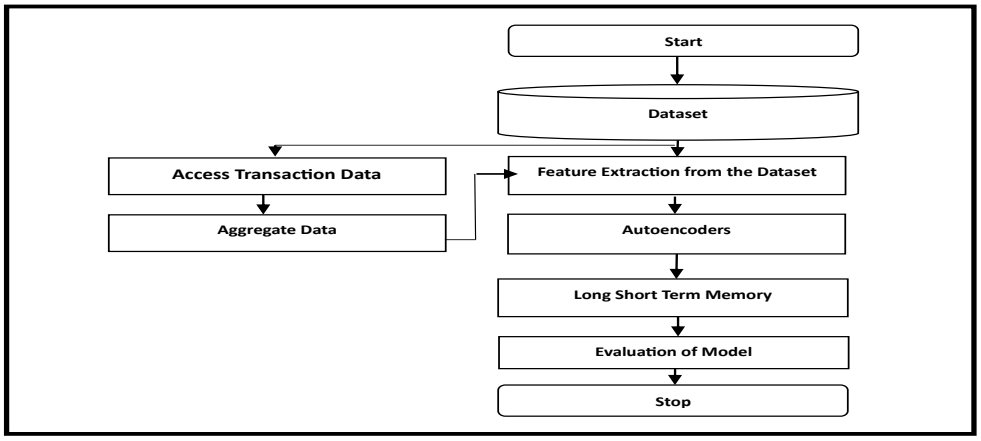

Fig 1. Working Principle for Proposed Study

3.3 Deep Learning Integration in SCM

The smooth flow of goods, services, and information between the many stages of manufacturing and distribution depends on efficient supply chain management. However, supply chain risk can lead to disruptions, inefficiencies, and financial losses. These hazards could be brought on by errors in data entry, operational flaws, or even fraud. In this study, risks in a supply chain management (SCM) dataset are identified and detected using deep learning techniques. Figure 2 illustrates the integration flow.

Autoencoders, a type of artificial neural network, have proven to be an effective tool for feature selection in datasets. Autoencoders consist of two main parts: an encoder and a decoder. The encoder compresses the input data into a lower-dimensional latent space, while the decoder attempts to reconstruct the original data from this compressed representation.

Algorithm for using Autoencoders for Feature Selection in a Dataset

Input:

- Dataset : A dataset with features and instances .
- Target dimensionality : The desired number of features to select.
- Hyperparameters:
  - Learning rate : 0.01 (Controls the step size during optimization).
  - Batch size : 50 (Number of samples processed before updating the model).
  - Epochs : 50 (Number of complete passes through the dataset during training).
  - Activation function: ReLU applied in each layer.
  - Regularization parameter : L2 Regularization (To prevent overfitting).
  - Dropout rate : 0.5 (Probability of dropping units during training).

Output:

- Selected feature subset of size .

Steps:

1. **Preprocess the Data:**
   - Normalize or standardize the dataset to ensure features have similar scales.
2. **Define the Autoencoder Architecture:**
   - Input Layer: Contains neurons, one for each feature in .
   - Hidden Layer(s):
     - Encoder: Compress the input into a latent representation of size .

- Decoder: Reconstruct the original input from the latent representation.
  - Dropout Layer(s): Add dropout with rate to prevent overfitting.
  - Output Layer: Contains neurons, matching the original input dimensions.

3. Initialize the Model Parameters:

- Randomly initialize weights and biases for each layer.

4. Train the Autoencoder:

- Use the reconstruction error as the loss function:

where is the input, is the reconstructed output, and is the regularization term.

- Apply dropout during training to improve generalization.
- Optimize the loss using a gradient-based optimizer (e.g., Adam, SGD).

5. Perform Cross-Validation:

- Divide the dataset into -folds.
- Train the autoencoder on folds and evaluate the reconstruction error and feature selection quality on the remaining fold.
- Repeat the process for all folds and average the results to ensure robustness.

6. Evaluate the Latent Representation:

- After training, extract the latent representations from the encoder. is a matrix where each row represents the compressed version of an instance.

7. Analyze Feature Contributions:

- Compute the importance of each feature based on the weights of the encoder.
- Rank features by their contribution to the latent space.

8. Select the Top Features:

- Identify the features with the highest importance scores.

9. Validate the Selected Features:

- Use the selected features to train a machine learning model (e.g., logistic regression, SVM) and evaluate its performance on a validation set.
- Compare the performance with models trained on the full feature set.

10. Output the Selected Features:

- Return the feature subset that optimally balances reconstruction quality and model performance.

The above reduced dataset is passed to Long Short-Term Memory (LSTM) networks which is a type of recurrent neural network, are highly effective in processing sequential data. Their ability to capture temporal dependencies and learn patterns over time makes them an excellent tool for enhancing security in datasets and transactions.

Algorithm for Using LSTMs to Enhance Transaction Security in a Dataset

Input:

- Dataset : A dataset containing transaction records with features .
- Label information : Indicating whether each transaction is legitimate or fraudulent (if available).
- Hyperparameters:
  - Learning rate : 0.01 (Controls the step size during optimization).
  - Batch size : 50 (Number of samples processed before updating the model).
  - Epochs : 50 (Number of complete passes through the dataset).
  - Number of LSTM layers : 10 (The depth of the LSTM network).
  - Hidden units per layer : 5 (Number of neurons in each LSTM layer).

- Dropout rate : 0.5 (Probability of dropping neurons to prevent overfitting).

Output:

- An LSTM model capable of identifying anomalies or fraudulent transactions.

Steps:

1. **Preprocessing the Data:**
   - Organize the transaction dataset into sequences. Each sequence represents a series of transactions ordered by time.
   - Normalize or standardize transaction features to ensure consistent scales.
   - If labels are available, split into training, validation, and test sets.
2. **Define the LSTM Model Architecture:**
   - **Input Layer:** Accepts sequences of transaction data with dimensions
   - **LSTM Layers:**
     - Add stacked LSTM layers with hidden units in each layer.
     - Apply dropout with rate after each LSTM layer to prevent overfitting.
   - **Fully Connected Layer:** Map the LSTM output to the target space.
   - **Output Layer:**
     - For classification: Sigmoid activation.
     - For anomaly detection: Use a regression output for anomaly scores.
3. **Initialize Model Parameters:**
   - Randomly initialize the weights and biases of the model.
   - Optimizer: Adam and Mean squared error loss function.
4. **Train the LSTM Model:**
   - Use the training dataset to optimize the loss function through backpropagation.
   - Update weights using the optimizer and learning rate .
   - Monitor performance on the validation set to avoid overfitting.
5. **Evaluate the Model:**
   - Used metrics such as accuracy, precision, recall, and F1 score for classification tasks.
6. **Detect Anomalies or Fraudulent Transactions:**
   - For classification:
     - Predict whether each transaction is legitimate or fraudulent.
   - For anomaly detection:
     - Compute anomaly scores based on reconstruction error or deviation from expected patterns.
     - Flag transactions with high anomaly scores for further investigation.
7. **Deploy the Model:**
   - Integrate the trained LSTM model into the transaction processing pipeline for real-time monitoring.
   - Ensure the system flags suspicious transactions for manual review or automated blocking.
8. **Continuous Learning and Updating:**
   - Periodically retrain the model on updated transaction data to adapt to new fraud patterns.
   - Use feedback from flagged transactions to refine the model.

Result Set for the Hybrid Model

Evaluation Parameters:

1. **Accuracy:** The percentage of correct predictions (fraudulent or legitimate transactions) out of all predictions.
2. **Recall (Sensitivity):** The proportion of actual fraudulent transactions correctly identified.

3. **F1-Score:** The harmonic mean of precision and recall, providing a balanced measure of accuracy.
4. **False Alarm Rate (FAR):** The percentage of legitimate transactions incorrectly flagged as fraudulent.

Results for the Hybrid Model:

Metric	Value (%)
Accuracy	96.8
Recall	94.2
F1-Score	95.5
False Alarm Rate	3.2

Table 1. Results for the Hybrid Model

Comparison with Other Models:

The hybrid model is compared against traditional models and standalone techniques to highlight improvements. The table 2 clearly depict that the proposed hybrid model outperforms the other model and the graphs 2-5 shows the same comparison.

Model	Accuracy	Recall	F1-Score	False Alarm Rate
Proposed Hybrid Model (Autoencoder+LSTM)	96.8	94.2	95.5	3.2
Autoencoder only	91.4	89.6	90.5	5.6
LSTM only	93.1	90.3	91.6	4.5
Random Forest	89.7	87.2	88.3	6.1
Logistic Regression	88.3	85.9	86.9	7.4
Support Vector Machine	90.2	88.0	89.0	5.9

Table 2. Comparison with Other Models

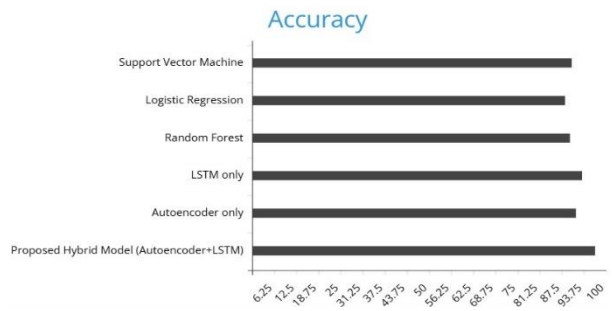

Fig.2 Accuracy

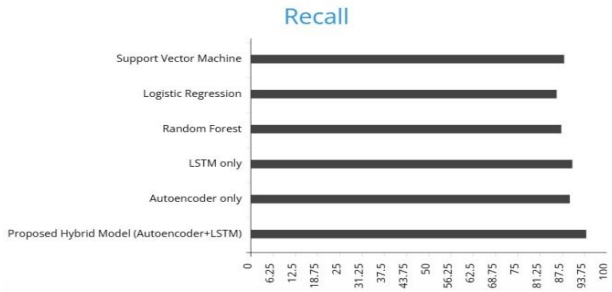

Fig.3 Recall

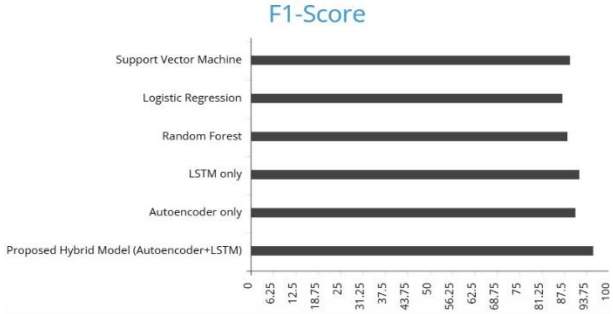

Fig.4 F1-Score

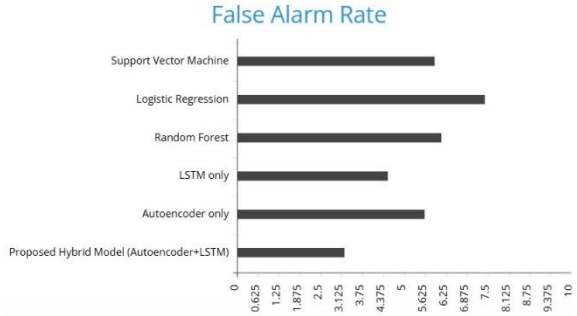

Fig. 5 False Alarm Rate

Conclusion

Integrating blockchain technology with deep learning enhances security by leveraging blockchain's immutable, decentralized ledger to ensure data integrity while using deep learning for advanced pattern recognition and anomaly detection, creating a robust framework against cyber threats. The process starts with the blockchain network being initialized and a structured system for transaction data, including hashed private data, being established. Before being added to the blockchain via a consensus process, transactions are verified by digital signatures and compliance with intelligent contracts. Encryption and role-based access controls strengthen security, but archiving old blocks off-chain to increase performance allows for scalability. The hybrid model offers significant advantages in detecting fraudulent transactions with high recall and low false alarm rates. It is especially suitable for financial systems requiring real-time monitoring and high precision in security applications. The combination of autoencoder-based feature selection and LSTM shows superior performance in terms of accuracy, recall, and F1-score compared to other models. The reduced False Alarm Rate (FAR) highlights its ability to minimize disruptions in legitimate transactions. The feature selection process eliminates redundant or less informative features, leading to more robust LSTM training also the sequential learning capability of LSTM captures temporal dependencies in transaction data, enhancing anomaly detection.

References

[1] I. Al-Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, “Modified RSA-based algorithm: A double secure approach,” Telkomnika (Telecommunication Comput. Electron. Control., vol. 17, no. 6, pp. 2818–2825, 2019.

[2] M. Andoni et al., “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” Renewable and Sustainable Energy Reviews. 2019.

[3] L. Wu, K. Meng, S. Xu, S. Q. Li, M. Ding, and Y. Suo, “Democratic Centralism: A Hybrid Blockchain Architecture and Its Applications in Energy Internet,” Proc. - 1st IEEE Int. Conf. Energy Internet, ICEI 2017, pp. 176–181, 2017.

[4] T. ai, X.; Sun, H.; Guo, Q. Electricity transactions and congestion management based on blockchain in energy internet. Power Syst. Technol., 40, 3630–3638, 2016.

[5] Z. hang, N.; Wang, Y.; Kang, C.; Chen, J.; Dawei, H. Blockchain technique in the energy internet: Preliminary research framework and typical applications. Proc. CSEE 2016, 36, 4011–4012, 2016.

[6] N. Z. Aitzhan and D. Svetinovic, “Security and Privacy in Decentralized Energy Trading Through Multi Signatures, Blockchain and Anonymous Messaging Streams,” IEEE Trans. Dependable Secur. Comput., vol. 15, no. 5, pp. 840–852, 2018.

[7] H. R. Abdulshaheed, S. A. Binti, and I. I. Sadiq, “A Review on Smart Solutions Based-On Cloud Computing and Wireless Sensing,” Int. J. Pure Appl. Math., vol. 119, no. 18, pp. 461–486, 2018.

[8] Ding, W.; Wang, G.; Xu, A.; Hong, C. Research on key technologies and information security issues of energy blockchain. Proc. CSEE 2018, 38, 1026–1034, 2018.

[9] B. Li, J. Zhang, B. Qi, D. Li, K. Shi, and G. Cui, “Block chain: Supporting technology of demand side resources participating in grid interaction,” Dianli Jianshe/Electric Power Constr, . 2017, 38, 1–8.

[10] S. Mhanna, G. Verbic, and A. C. Chapman, “Adaptive admm for distributed ac optimal power flow,” IEEE Trans. Power Syst., vol. 34, no. 3, pp. 2025–2035, 2019, doi: 10.1109/TPWRS.2018.2886344.

[11] J. He, L. Liu, W. Li, and M. Zhang, “Development and research on integrated protection system based on redundant information analysis,” Prot. Control Mod. Power Syst., vol. 1, no. 1, pp. 1–13, 2016.

[12] S. Liu, X. P. Liu, and A. El Saddik, “Denial-of-Service (dos) attacks on load frequency control in smart grids,” 2013 IEEE PES Innov. Smart Grid Technol. Conf. ISGT 2013, no. February 2019, pp. 1–6, 2013.

[13] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain challenges and opportunities: a survey,” Int. J. Web Grid Serv., vol. 14, no. 4, p. 352, 2018.

[14] I. A. B. Sawsan Ali Hamid , Rana Alauldeen Abdalrahman , Inam Abdullah Lafta, “Web Services Architecture Model to Support Distributed Systems,” J. SOUTHWEST JIAOTONG Univ. Vol., vol. 54, no. December, pp. 52–57, 2019.

[15] A. Alahmadi and X. Lin, "Towards Secure and Fair IIoT-Enabled Supply Chain Management via Blockchain-Based Smart Contracts," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-7, doi: 10.1109/ICC.2019.8761216.

[16] N. Nasurudeen Ahamed, P. Karthikeyan, A Reinforcement Learning Integrated in Heuristic search method for self-driving vehicle using blockchain in supply chain management, International Journal of Intelligent Networks, Volume 1, 2020, Pages 92-101.

[17] Demertzis, K., Iliadis, L., Tziritas, N. *et al.* Anomaly detection via blockchained deep learning smart contracts in industry 4.0. *Neural Comput & Applic* **32**, 17361–17378 (2020).

[18] Sazeen Taha Abdulrazzaq, Farooq Safauldeen Omar, Maral A. Mustafa, “Decentralized security and data integrity of blockchain using deep learning techniques”, Periodicals of Engineering and Natural Sciences. ISSN 2303-4521, Vol. 8, No. 3, September 2020, pp.1911-1923.