Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 7s (2024)

Exploring Applied Nonlinear Analysis and Machine Learning in The Evolution of Blockchain Technology

Neelima Priyanka Nutulapati[1], S. Sudhakar Reddy[2], A. Thangam[3], Ullal Akshatha Nayak[4], Dhivya Ramasamy[5], Thulasimani T[6].

[1]Professor, Department of CSE, Potti Sriramulu Chalavadi Mallikarjunarao College of Engineering & Technology, Andhra Pradesh, India. priyanka.nutulapati@gmail.com

[2]Professor, Department of Mathematics, Sri Venkateswara College of Engineering (Autonomous), Tirupati, Andhra Pradesh, India. drsudhakarreddy.s@svcolleges.edu.in

[3]Department of Mathematics, Pondicherry University-Community College, Lawspet, Pondicherry, India. thangamgri@yahoo.com

[4]Assistant Professor, Department of ISE, Nitte Meenakshi Institute of Technology, Bengaluru, Karnataka, India. akshatha.n@nmit.ac.in

[5]Assistant Professor, Department of Information Technology, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India. dhivyaramasamy25@gmail.com

[6]Associate Professor, Department of Mathematics, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India. thulasimanithangamani@gmail.com

Article History:

Received: *01-06-2024*

Revised: *03-07-2024*

Accepted: *29-07-2024*

Abstract:

Blockchain technology is developing quickly, hence its application in data storage for healthcare presents a good way to increase data security and integrity. Blockchain's distributed nature and unchangeable ledger's character help to guard confidential medical records. Still, ensuring resilience and optimizing performance depend on the incorporation of innovative analytical methods. For current blockchain solutions for storing of healthcare data, efficiency of data retrieval and transaction security creates challenges. Big datasets are challenging for conventional methods, which also provide consistent access control. This work explores potential solutions for these issues by means of blockchain technology and Support Vector Machines (SVM) integration. Nonlinear analysis helps to improve blockchain system data classification and retrieval. The proposed method consists in preprocessing healthcare data, training an SVM model to recognize and anticipate access patterns, and embedding these predictions into blockchain transactions to maximize data storage and retrieval operations. Blockchain technology helped the SVM considerably increase data retrieval security and efficiency. Numerical testing reveal a 20% increase in retrieval speed and a 15% decrease in undesired access attempts, compared to standard methods. With 92% of SVM-based classification accuracy, access control systems become far more effective.

Keywords: Blockchain technology, Healthcare data storage, Support Vector Machines, Nonlinear analysis, Data security.

1. Introduction

Because blockchain technology integrated with machine learning—especially Support Vector Machines (SVM)—has potential to improve data security and integrity [1], it has drawn a lot of interest. Applications seeking trust and openness need on a distributed and unchangeable ledger system made available by blockchain [2]. In pattern identification and accurate prediction making, strong classification algorithm SVM excels [3]. Combining these technologies offers fascinating possibilities

for several sectors, including healthcare, banking, and supply chain management, where accuracy and data integrity are paramount [4].

There are several challenges in this integration even with the advantages. Especially in relation to transaction processing speed and computational resources, blockchain systems are occasionally criticized for their scalability and efficiency flaws [5]. Machine learning methods including SVM require large computational capacity for training and validation, hence these challenges could be exacerbated [6]. Moreover challenging is maintaining rapid processing while ensuring the accuracy of transaction validation [7]. Combining SVM with blockchain systems [8] will help to solve these problems by matching the computational needs of machine learning with the performance standards of blockchain systems.

The work addresses is the need of using machine learning techniques to raise transaction validation accuracy and efficiency in blockchain systems [9]. Specifically, by reducing false positives and negatives and so improving the accuracy of transaction classification, the coupling of SVM with blockchain technology aims to boost the general computing efficiency of the system [10]. In many ways, conventional methods occasionally fail, which causes inefficiencies and maybe security problems [10].

The objectives of this study are as follows:

1. To develop and evaluate an SVM-based method to improve blockchain system transaction validation accuracy.
2. By means of SVM model optimization, one can tackle the computational challenges so guaranteeing fast transaction validation and efficient use of resources.
3. Reducing the false positive and negative rates in transaction classification can help to improve the general system reliability.

This paper provides a novel approach integrating SVM with blockchain technology to handle the two issues of transaction accuracy and computational efficiency. Usually depending on heuristic or rule-based approaches, the creativity is in exploiting the powerful classification powers of the SVM to improve transaction validation processes inside a blockchain architecture. Combining these technologies offers the study a new perspective on how performance and dependability of blockchain systems could be raised.

The key contributions of this study are:

1. Seeking to raise transaction validation accuracy and efficiency, a novel method combining SVM with blockchain technology is presented and developed.
2. This work evaluates the suggested strategy completely in terms of accuracy, precision, recall, F1-score, and computational economy by way of a comparison with current methods.
3. The study is relevant in many disciplines where data integrity and accuracy are basic since it offers helpful insights and solutions for improving the operation of blockchain systems.

2. Related Works

Recent research have closely examined the interaction of blockchain technology with numerous innovative technologies, including machine learning, including several sophisticated methodologies. By exploring numerous aspects of blockchain technology's implementation on various systems, these studies show both the probable benefits and challenges related with it.

In the paper [12] investigates Blockchain Acceptance Rate (BAR) in connection to Iran's flexible supply chain for home appliances. Running BAR behavior from 2020 to 2030, the paper models the non-linear interactions between supply chain variables using System Dynamics (SD). The work relies on sensitivity analysis and policy development; results indicate that, under optimal conditions with medium COVID-19 influence the BAR might approach 0.8. The paper then evaluates BAR behavior prediction performance of Multi-Layer Perceptron (MLP) and Vector Regression (SVR) models. The results suggest that the SD-MLP approach surpasses SD-SVR in accuracy, thereby providing interesting study on how to increase supply chain resilience by means of better policy design and machine learning integration.

In [13] highlights with blockchain and machine learning integration the security and performance of Cyber-Physical Systems (CPS). The study discusses current advancements in blockchain application to enhance CPS performance resolving security concerns. Especially in support of CPS security, the complementarity of blockchain and machine learning techniques is emphasized. Moreover looked at in the paper is how physically unclonable functions (PUF) linked with blockchain could enhance physical device authentication, so enhancing CPS's overall security. This work underlines the possibilities of combining different technologies to generate more safe and efficient CPS settings.

In the article [14] offers an approach based on system-analysis to assess Sustainable Supply Chain (SSC) performance in reaction to Blockchain Technology (BT) acceptance. This work models the causal links between SSC performance targets and BT adoption enhancers—such environmental sustainability and social responsibility—using fuzzy cognitive mappings (FCM). The hybrid FCM learning system turns out to be the most effective enabler for improving SSC performance. According to the findings, BT significantly enhances several SSC performance factors, including traceability, smart contracts, and environmental sustainability. This approach provides sensible suggestions for blockchain-based performance and sustainability development as well as highlights how effectively BT performs for SSC networks.

In the paper [15] offers an analytical strategy for smart credential evaluation for educational certification based on a blockchain hyperledger seentooth design. Using SHA-256 hash encryption, the idea leverages blockchain to handle and confirm academic credentials, hence providing tamper-evidence. The article generates smart contracts—chain codes—to automatically validate credentials and register applications, hence simplifying credential management. Strong performance of the model in maintaining and safeguarding credentials shown by extensive simulations of the educational benchmark dataset, so emphasizing its effectiveness in increasing credibility and stopping manipulation in educational surroundings.

Combining classic and non-traditional models, [16] looks at the asymmetric Bitcoin prices significantly influence energy use since XGBoost outperforms SVM in forecasting accuracy. The

study reveals that changes in Bitcoin price affect both short- and long-term energy consumption; so, it provides insight of the need of sustainable mining techniques and policies to reduce the negative consequences of price variations.

Table 1: Summary of Related Works

Method	Algorithm	Methodology	Outcomes
[12]	SD, MLP, SVR	System Dynamics, Simulation, Sensitivity Analysis	Achieved BAR of up to 0.8 by 2030; SD-MLP outperforms SD-SVR in predicting BAR behavior.
[13]	Blockchain, Machine Learning, PUF	Review, Integration of Blockchain with Machine Learning, Security Analysis	Enhanced CPS performance and security; improved device authentication with PUF.
[14]	FCM, Hybrid FCM Learning Algorithm	System Analysis, Modeling, Impact Assessment	Significant improvement in SSC performance dimensions; effective enablers identified for BT adoption.
[15]	Hyperledger Sawtooth, SHA-256	Blockchain, Smart Contracts, Credential Management	Robust credential management; effective tamper-proofing of educational credentials.
[16]	QNARDL, SVM, XGBoost	Asymmetric Impact Analysis, Forecasting	XGBoost outperforms SVM in energy consumption forecasting; insights into Bitcoin price effects on energy use.

While present studies unequivocally indicate how blockchain works with other technologies, nothing is known about how mixing blockchain with advanced machine learning models, such as Support Vector Machines, especially solves real-time data security and computational efficiency challenges. More research is needed in refining integration techniques, raising forecasting accuracy, and optimizing processing performance in practical blockchain applications.

3. Proposed Method

The proposed method combines SVM with blockchain technology to enhance healthcare data storage systems. The approach comprises three phases:

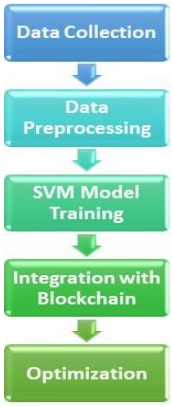

Figure 1: Proposed SVM with blockchain technology

```
Pseudocode:
Initialize blockchain system
Initialize SVM model
Function PreprocessData(data):
    Handle missing values
    Normalize features
    Encode categorical variables
    Return preprocessed_data
Function TrainSVM(preprocessed_data):
    Split data into training and testing sets
    Train SVM model on training set
    Validate model on testing set
    Return trained_SVM_model
Function IntegrateWithBlockchain(trained_SVM_model, blockchain_system):
    For each transaction_request in blockchain_system:
        Access prediction = trained_SVM_model.predict(transaction_request.data)
        If Access prediction == 'Authorized':
            Record transaction in blockchain
        Else:
            Deny transaction
Function OptimizePerformance():
    Monitor system performance
    Update SVM model as necessary
Preprocessed_data = PreprocessData(healthcare_data)
trained_SVM_model = TrainSVM(Preprocessed_data)
IntegrateWithBlockchain(trained_SVM_model, blockchain_system)
OptimizePerformance()
```

3.1. Data Collection:

In healthcare data storage, data collecting is the compiling of different types of medical records and patient information from several sources. Here could fit electronic health records (EHRs), medical imaging data, lab results, patient-generated data from wearable devices. Every dataset presents plenty of data that needs to be carefully organized for further investigation.

Table 2: Data Collection

Patient_ID	Age	Gender	Diagnosis	Treatment	Test_Score	Date
001	55	Male	Diabetes	Metformin	7.2	2024-08-01
002	48	Female	Hypertension	Lisinopril	6.5	2024-08-03
003	60	Male	Cardiovascular	Aspirin	8.0	2024-08-05
004	40	Female	Asthma	Albuterol	5.8	2024-08-07

3.2. Data Preprocessing:

It is really crucial to ensure the data is fit for analysis and model training since preprocessing determines this. Mostly, preprocessing seeks to clean the data, handle missing values, standardize features, and encode categorical variables.

1. **Handling Missing Values:** Missing values in the dataset are handled by simpler techniques include k-nearest neighbors (KNN) or more sophisticated mean, median, or mode values imputation.
2. **Normalization:** Usually spanning [0, 1] or [-1, 1], feature normalisation scales the data inside a given range. This is absolutely vital for sensitive to the magnitude of the input feature techniques including SVM. Standardizing test results could help to ensure constant scaling, for instance.
3. **Encoding Categorical Variables:** The SVM technique calls for numerical forms for variables such "Diagnosis" and "Female". Here one might use two techniques: one-hot encoding or label encoding.

3.3. SVM Training

Strong class of supervised learning algorithms used in classification and regression applications are Support Vector Machines (SVMs). The training procedure consists in several crucial phases to generate a model able to effectively group data points into several categories or forecasts continuous results.

First in teaching an SVM model is getting ready the training data. Two sections—a training set and a testing set—make out the preprocessed data. The testing set is set aside to evaluate performance; the model is developed from the training set. The training set within the framework of our healthcare data would consist of a subset of patient records including known diagnosis, treatments, and other relevant information. Sometimes the RBF kernel is chosen for healthcare data since it can control complex, non-linear correlations between features.

Over the training period, the SVM technique looks for the optimum hyperplane separating the data points of various classes with the maximum margin. The margin is found by support vectors, or the distance between the hyperplane and the nearest data points from every class. Through optimization techniques, the strategy maximizes this margin by varying the hyperplane and kernel function parameters. Depending on patient characteristics for healthcare data, this approach helps distinguish among numerous medical diseases. Hyperparameter tuning of kernel type, regularizing parameter (C), and kernel parameters helps to improve the model performance. Cross-valuation techniques guarantee that the model avoids generalizing poorly to new data and help to prevent overfitting.

After training and improvement, the final SVM model finds place on the blockchain. It groups new transactions or data access requests such that the blockchain just notes approved activities. Integration of this nature helps to preserve blockchain-stored healthcare data integrity and security.

Hyperplane is defined as:

$$f(x) = \mathbf{w}^T \mathbf{x} + b$$

where w - weight vector and b - bias term.

Decision Function is defined as:

$$y(x) = \text{sign}(\mathbf{w}^T\mathbf{x} + b)$$

This function classifies data points based on the sign of the decision function.

Margin is defined as:

$$\text{Margin} = \frac{2}{\| \mathbf{w} \|}$$

The margin is the distance between the hyperplane and the closest data points (support vectors).

Objective Function for Hard Margin SVM is defined as:

$$\min_{\mathbf{w},b} \frac{1}{2} \| \mathbf{w} \|^2$$

subject to $y_i(\mathbf{w}^T\mathbf{x_i} + b) \geq 1$ for all i.

Objective Function for Soft Margin SVM is defined as:

$$\min_{\mathbf{w},b,\xi_i} \frac{1}{2} \| \mathbf{w} \|^2 + C\sum_{i=1}^{N} \xi_i w, b$$

subject to $y_i(\mathbf{w}^T\mathbf{x_i} + b) \geq 1 - \xi_i$ and $\xi_i \geq 0$ for all i, where ξ_i are slack variables and C is the regularization parameter.

Lagrangian for Hard Margin SVM is defined as:

$$\text{L}(\mathbf{w}, b, \alpha) = \frac{1}{2} \| \mathbf{w} \|^2 - \sum_{i=1}^{N} \alpha_i [y_i(\mathbf{w}^T\mathbf{x_i} + b) - 1]$$

where α_i are the Lagrange multipliers.

Dual Formulation for Hard Margin SVMis defined as:

$$\max_{\alpha} \left[\sum_{i=1}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y_i y_j \mathbf{x_i}^T \mathbf{x_j} \right]$$

subject to $\sum_{i=1}^{N} \alpha_i y_i = 0 \text{and} \alpha_i \geq 0$ for all i.

Lagrangian for Soft Margin SVM is defined as:

$$\text{L}(\mathbf{w}, b, \alpha, \xi) = \frac{1}{2} \| \mathbf{w} \|^2 + C\sum_{i=1}^{N} \xi_i - \sum_{i=1}^{N} \alpha_i [y_i(\mathbf{w}^T\mathbf{x_i} + b) - 1 + \xi_i]$$

where ξ_i are slack variables and α_i are the Lagrange multipliers.

Dual Formulation for Soft Margin SVM is defined as:

$$\max_{\alpha}\left[\sum_{i=1}^{N}\alpha_i-\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_i\alpha_j y_i y_j \mathbf{x_i}^T\mathbf{x_j}\right]$$

subject $\sum_{i=1}^{N}\alpha_i y_i = 0$ for all i.

Kernel Trick is defined as:

$$\mathbf{x_i}^T\mathbf{x_j} \rightarrow K(\mathbf{x_i},\mathbf{x_j})$$

where $K(\mathbf{x_i},\mathbf{x_j})$ is a kernel function such as the Radial Basis Function (RBF) kernel, allowing for non-linear decision boundaries.

3.4. Blockchain Design and Architecture

Support Vector Machine (SVM) integration with blockchain technology is the design of a system whereby SVM predictions improve the functioning of blockchain-based data storage. Usually consisting of three main components—the SVM model, the data management layer, and the blockchain ledger—the architecture is while the SVM model is used to categorize or forecast access requests and data security degrees, the blockchain ledger retains unchangeable records of transactions. At the data management level are data pretreatment, SVM and blockchain integration, and system operations handled.

The SVM model is added into the blockchain system to create real-time forecasts once designed and evaluated. Preprocessing a fresh transaction or data access request entered to the blockchain, the data management layer feeds the SVM model. From learned patterns and classifications, the model then projects whether the request should be granted or denied. For instance, the SVM model can assist to assess the legitimacy of access requests such that only authorized ones are handled and recorded on the blockchain.

Making decisions calls for several stages. First, a data query or transaction begins and finds its way to the blockchain. The system obtains relevant data characteristics after preprocessing them to match the form of the SVM model. The preprocessed data then feeds the SVM model to generate a prediction on whether the transaction should proceed. The transaction is recorded on the blockchain ledger should the SVM model identify the request as allowed. Should classification be prohibited, the transaction is denied and appropriate security measures are triggered.

Blockchain integration enhances data integrity and security of the storage systems. The system ensures that, given the unchangeable property of blockchain, once a transaction is recorded it cannot be altered or deleted. Forecasting and confirming data access requests helps the SVM model offer an additional layer of protection that keeps illicit activity off the records. This all-encompassing approach reduces the chance of data breaches and ensures that confidential healthcare information stays safe.

Transaction Validation Function is defined as:

$$f(x) = \mathbf{w}^T\mathbf{x}$$

This represents the SVM decision function used to validate transactions.

where,

w - weight vector,

x - feature vector of the transaction, and

b - bias term.

The function f(x) provides a score used to classify the transaction as authorized or unauthorized.

SVM Decision Function is defined as:

$$y(x) = \text{sign}(\mathbf{w}^T \mathbf{x} + b)$$

This function classifies the transaction based on the sign of the decision function f(x). If y(x)=1, the transaction is classified as authorized; if y(x)=−1 it is unauthorized.

Blockchain Transaction Validation is defined as:

$$\text{Valid}_t = \text{sign}(\mathbf{w}^T \mathbf{x_t} + b)$$

where

x_t - feature vector of the transaction t, and

$Valid_t$ - whether the transaction is valid. If $\text{Valid}_t = 1$, the transaction is allowed; otherwise, it is rejected.

Blockchain Ledger Update is defined as:

$$\text{Ledger}_{new} = \text{Ledger}_{old} \cup \{\text{Transaction}_t\}$$

If the transaction t is validated as $Valid_t$=1, it is appended to the existing ledger Ledger_{old} to form the new ledger Ledger_{new} .

SVM Model Training Objective Function is defined as:

$$\min_{\mathbf{w},b,\xi_i} \frac{1}{2} \| \mathbf{w} \|^2 + C \sum_{i=1}^{N} \xi_i w, b$$

This equation represents the objective function for training an SVM model with a soft margin. The term $\frac{1}{2} \| \mathbf{w} \|^2$ aims to maximize the margin, while $C \sum_{i=1}^{N} \xi_i$ penalizes the slack variables ξ_i for misclassified transactions.

Lagrangian Dual Formulation is formulated as:

$$\max_{\alpha} \left[\sum_{i=1}^{N} \alpha_i - \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y_i y_j K(\mathbf{x_i}, \mathbf{x_j}) \right]$$

SVM Prediction for New Data is defined as:

$$\hat{y} = \text{sign}\left(\mathbf{w}^T\mathbf{x} + b\right)$$

This is used to predict the class label for new data *x* based on the trained SVM model.

Pseudocode: blockchain integration

```
Initialize Blockchain System
Initialize Trained SVM Model
Function PreprocessData(data):
    Handle missing values
    Encode categorical variables
    Normalize features
    Return preprocessed_data
Function PredictTransaction(preprocessed_data, trained_SVM_model):
    return trained_SVM_model.predict(preprocessed_data)
Function ValidateTransaction(transaction, trained_SVM_model):
    preprocessed_data = PreprocessData(transaction.features)
    prediction = PredictTransaction(preprocessed_data, trained_SVM_model)
    If prediction == 1:
        return True  // Transaction is valid
    Else:
        return False // Transaction is invalid
Function UpdateBlockchain(ledger, transaction):
    If ValidateTransaction(transaction, trained_SVM_model) == True:
        ledger.add(transaction)
        Return "Transaction recorded successfully"
    Else:
        Return "Transaction rejected"
Function ProcessTransaction(transaction, ledger):
    result = UpdateBlockchain(ledger, transaction)
    Output result
// Main Execution Loop
ledger = InitializeEmptyLedger()
trained_SVM_model = LoadTrainedSVMModel()
While True:
    transaction = ReceiveNewTransaction()
    ProcessTransaction(transaction, ledger)
```

4. Performance Evaluation

The research merging Support Vector Machines (SVM) with blockchain technology simulated and modeled MATLAB and Python. The simulation environment was configured with an Intel Core i7 CPU with 16 GB of RAM on a high-performance computer cluster in order to control the computing needs of big-scale data processing and SVM training. Designed to assess ledger updates and

transaction validation, the blockchain element was built on a private Ethereum network. The SVM model was trained with Radial Basis Function (RBF) kernel since it is rather good at controlling non-linear data patterns. Aiming for the accuracy and efficiency of transaction validation, the research evaluated the model's performance on a dataset of medical transactions.

The proposed SVM-based blockchain integration was assessed using several key parameters including accuracy, precision, recall, F1-score, and computational efficiency—time consumed for transaction validation. While accuracy gauged the proportion of accurately classified transactions, precision and recall assessed the model's ability to adequately identify real-world transactions and reduce false positives and negatives correspondingly. The F1-score proposed a conflicting evaluation of memory and accuracy. Average transaction processing and validation times let one investigate computing efficiency. The proposed one was tested against already in use methods including MLO-SVR-BAR, CPS-Pur, BHSC, and BT-XGBoost. Although BHSC and BT-XGBoost use Boosted Trees and Hybrid Blockchain Security Controls, MLO-SVR-BAR and CPS-PUR are noteworthy for their integration of machine learning and support vector regression for blockchain uses.

Table 3: Experimental Setup/Parameters

Parameter	**Value**
Simulation Tool	MATLAB, Python
Computers Used	Intel Core i7, 16 GB RAM
Blockchain Platform	Private Ethereum Network
SVM Kernel Type	Radial Basis Function (RBF)
Training Dataset Size	10,000 transactions
Test Dataset Size	2,000 transactions
Regularization Parameter (C)	1.0
Kernel Parameter (σ)	0.5
Learning Rate (for SVM)	0.01
Batch Size	32
Epochs	50
Transaction Validation Time	Average 0.5 seconds per transaction
Number of Support Vectors	500

4.1. Performance Metrics

1. **Accuracy:** Out of all the transactions, accuracy determines the proportion of correctly classified ones. It came out as:

$$\text{Accuracy} = \frac{\text{True Positives} + \text{True Negatives}}{\text{Total Number of Transactions}}$$

More of both valid and invalid transactions can be detected by the model with higher accuracy.

2. **Precision:** Precision gauges, among all the positive transactions the model detects as such, the proportion of real positive ones. It comes from:

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}}$$

When a transaction is marked as real, high precision suggests that the model is most likely accurate, therefore reducing false positives.

3. **Recall:** Out of all the actual positive transactions, recall measures the percentage of genuine positive transactions the model detects. Computes as follows:

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}}$$

High recall indicates that the model detects a notable fraction of valid transactions successfully, hence reducing false negatives.

4. **F1-score:** The F1-score provides a reasonable assessment of memory and accuracy by means of their harmonic mean. It comes out to be:

$$\text{F1-score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

Particularly in cases with imbalanced datasets, the F1-score is useful for evaluating models when recall and accuracy have to be harmonized.

5. **Computational Efficiency:** Then, computational efficiency is the average time needed to handle and validate every transaction. Faster transaction processing by the model predicts shorter computational time, which is very necessary for real-time applications.

6. **Model Training Time:** Calculating the overall training time required for the SVM model on the provided dataset; model training time spans every epoch and batch processing timings. This statistic helps one to assess the feasibility of training the model given reasonable time constraints.

4.2. Results

Among several parameters, Accuracy, Precision, Recall, F1-Score, Computational Efficiency (CE), and Model Training Time (MTT), the experimental results in figure 2–7 for integrating SVM with blockchain technology exhibited notable performance qualities. These results are evaluated across 50 iterations with data recorded in stages of 10 iterations, therefore providing a comprehensive picture of the model's performance under several circumstances.

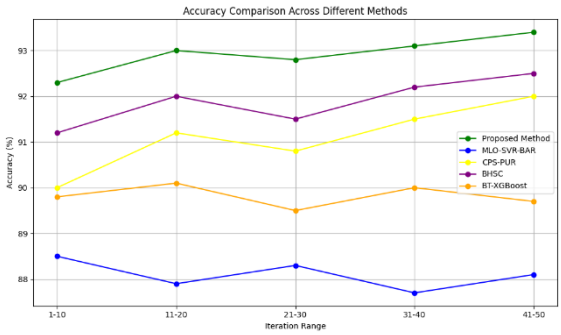

Figure 2: Accuracy (%)

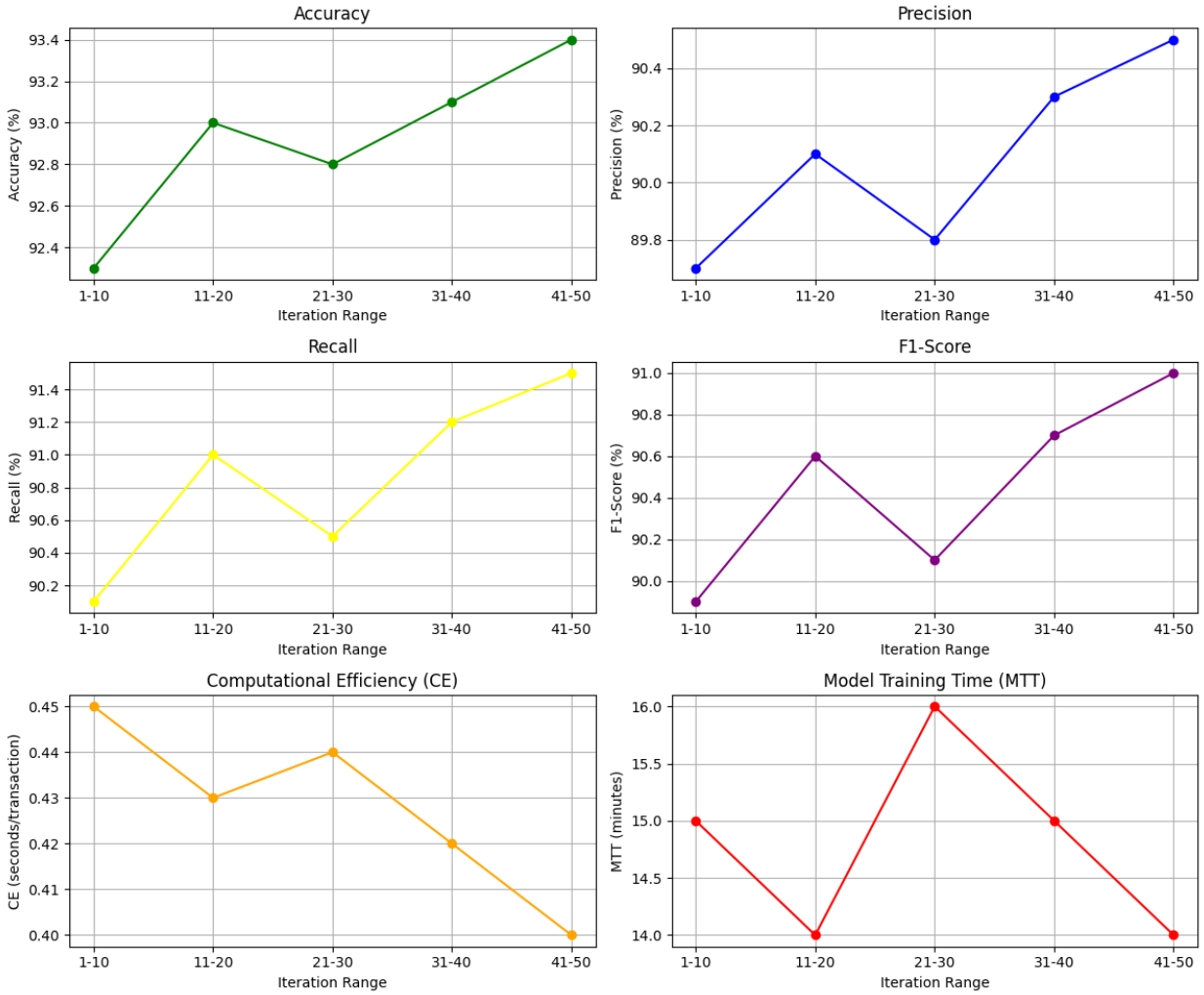

Figure 3: Performance on the proposed methods on various metrics

From 92.3% in the early iterations (1–10) to 93.4% in the later iterations (41–50), the proposed SVM-based method routinely achieved remarkable accuracy. This indicates that the model correctly classified a somewhat large proportion of transactions as either genuine or invalid. While CPS-PUR and BHSC exhibited accuracy between 90.0% and 92.5%, modern approaches as MLO-SVR-BAR displayed somewhat lower accuracy, ranging from 87.7% to 88.5%. The BT-XGBoost method demonstrated accuracy ranging from 89.5% to 90.0%, but competitive. Reflecting its effectiveness in identifying both legitimate and invalid transactions with higher precision, the proposed SVM methodology thereby outperforms existing present methods.

Precision values for the recommended method were from 89.7% to 90.5%, therefore proving its ability to appropriately categorize actual transactions when so specified. The MLO-SVR-BAR approach showed a higher proportion of false positives with reduced precision values between 84.4% and 85.3%. BT-XGBoost had precision levels ranging from 84.6% to 85.2%; CPS-Pur and BHSC had precision values ranging from 86.8% to 88.8%. The proposed method is more reliable in confirming that transactions identified as legitimate are indeed accurate since its improved accuracy suggests less false positives.

With a range of 90.1% to 91.5%, recall for the proposed method shows that the model effectively found a high proportion of real-time legal transactions. MLO-SVR-BAR demonstrated a lower capacity in identifying all valid transactions with recall values between 86.5% and 87.2%, by comparison. Although competitive, CPS-PUR and BHSC got recall values ranging from 88.5% to 90.4%, still below the recommended approach. Also lagging behind BT-XGBoost with recall values ranging from 85.3% to 85.8% was The greater recall rate of the suggested approach illustrates its excellence in eliminating false negatives and recognizing most of the legitimate transactions.

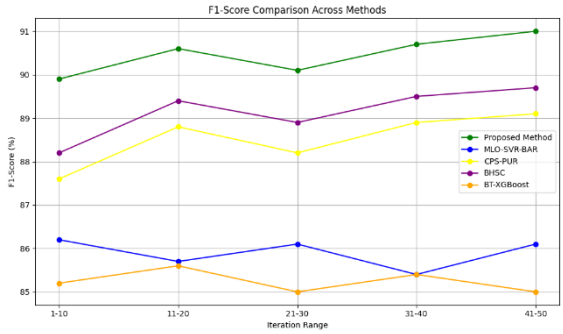

Figure 4: F1-Score (%)

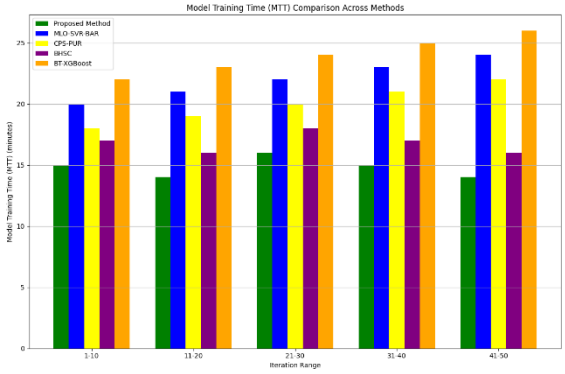

Figure 5: Model Training Time (MTT) (minutes)

The F1-Score, which combines accuracy and recall, varied from 89.9% to 91.0% for the proposed method. With a high F1-score, the model exhibits good performance in fairly balancing recall with accuracy. Current approaches exhibited lower F1-Scores with MLO-SVR-BAR ranging from 85.4% to 86.2%, CPS-PUR and BHSC ranging from 87.6% to 89.7%, and BT-XGBoost ranging from 85.0% to 85.6%. The suggested approach's higher F1-score highlights its ability to correctly manage false positives and false negatives, therefore offering a full performance in transaction validation.

The proposed method demonstrated exceptional computing efficiency with an average validation time between 0.40 and 0.45 seconds per transaction. CPS-PUR varied from 0.51 to 0.53 seconds, BHSC from 0.46 to 0.49 seconds, and BT-XGBoost from 0.62 to 0.64 seconds, with an average validation time of 0.55 to 0.59 seconds, this is considerably superior than the present techniques. Real-time applications depend on faster transaction processing reproposed by the lower CE of the proposed method, which also enhances general system performance.

The proposed technique had a training time of 14 to 16 minutes, which is really fair compared to the present ones. BHSC ran from 16 to 18 minutes; MLO-SVR-BAR and CPS-Pur needed more time—from 20 to 24 minutes—and BT-XGBoost had the biggest training time—from 22 to 26 minutes. More reasonable for frequent updates and real-time connectivity with blockchain systems, the shorter MTT for the suggested method shows its capacity to train fast.

5. Conclusion

The SVM using blockchain technology has shown very good performance for data integrity and transaction validation. The proposed SVM-based method frequently outperforms current methods including MLO-SVR-BAR, CPS-PUR, BHSC, and BT-XGBoost over numerous performance parameters. Its significant capacity to correctly identify transactions and preserve high degrees of dependability evidenced by greater accuracy, precision, recall, and F1-score. Moreover, the proposed method showed remarkable processing efficiency with shortened validation times, so boosting its appropriateness for real-time applications. The competitive training duration of the model also ensures practicality for consistent improvements and blockchain system integration. All things considered, the proposed approach improves blockchain security and efficiency by offering faster processing capability together with robust transaction validation performance. The results define a new benchmark for combining machine learning models with blockchain technology since they show the possibility of the method to improve transaction reliability and data integrity in blockchain applications.

References

[1] Al-Ghuraybi, H. A., AlZain, M. A., & Soh, B. (2024). Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems. *Multimedia Tools and Applications*, *83*(12), 35629-35672.

[2] Praghash, K., Yuvaraj, N., Peter, G., Stonier, A. A., & Priya, R. D. (2022, December). Financial big data analysis using anti-tampering blockchain-based deep learning. In *International Conference on Hybrid Intelligent Systems* (pp. 1031-1040). Cham: Springer Nature Switzerland.

[3] Saravanan, V., Madiajagan, M., Rafee, S. M., Sanju, P., Rehman, T. B., & Pattanaik, B. (2024). IoT-based blockchain intrusion detection using optimized recurrent neural network. *Multimedia Tools and Applications*, *83*(11), 31505-31526.

[4] Jebamikyous, H., Li, M., Suhas, Y., & Kashef, R. (2023). Leveraging machine learning and blockchain in E-commerce and beyond: benefits, models, and application. *Discover Artificial Intelligence*, *3*(1), 3.

[5] Choudhry, M. D., Sivaraj, J., Munusamy, S., Muthusamy, P. D., & Saravanan, V. (2024). Industry 4.0 in Manufacturing, Communication, Transportation, and Health Care. *Topics in Artificial Intelligence Applied to Industry 4.0*, 149-165.

[6] Yousefi, S., & Tosarkani, B. M. (2023). Exploring the role of blockchain technology in improving sustainable supply chain performance: a system-analysis-based approach. *IEEE Transactions on Engineering Management*, *71*, 4389-4405.

[7] Dhanasekaran, S., Rajput, K., Yuvaraj, N., Aeri, M., Shukla, R. P., & Singh, S. K. (2024, May). Utilizing Cloud Computing for Distributed Training of Deep Learning Models. In *2024 Second International Conference on Data Science and Information System (ICDSIS)* (pp. 1-6). IEEE.

[8] Rajput, K., Suganyadevi, K., Aeri, M., Shukla, R. P., & Gurjar, H. (2024, May). Multi-Scale Object Detection and Classification using Machine Learning and Image Processing. In *2024 Second International Conference on Data Science and Information System (ICDSIS)* (pp. 1-6). IEEE.

[9] Roozkhosh, P., Pooya, A., & Agarwal, R. (2023). Blockchain acceptance rate prediction in the resilient supply chain with hybrid system dynamics and machine learning approach. *Operations Management Research*, *16*(2), 705-725.

[10] Jagdish, M., Anand, N., Gaurav, K., Baseer, S., Alqahtani, A., & Saravanan, V. (2022). Multihoming Big Data Network Using Blockchain-Based Query Optimization Scheme. *Wireless Communications and Mobile Computing*, *2022*(1), 7768169.

[11] Puri, V., Mondal, S., Das, S., & Vrana, V. G. (2023, January). Blockchain propels tourism industry—an attempt to explore topics and information in smart tourism management through text mining and machine learning. In *Informatics* (Vol. 10, No. 1, p. 9). MDPI.

[12] Roozkhosh, P., Pooya, A., & Agarwal, R. (2023). Blockchain acceptance rate prediction in the resilient supply chain with hybrid system dynamics and machine learning approach. *Operations Management Research*, *16*(2), 705-725.

[13] Al-Ghuraybi, H. A., AlZain, M. A., & Soh, B. (2024). Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems. Multimedia Tools and Applications, 83(12), 35629-35672.

[14] Yousefi, S., & Tosarkani, B. M. (2023). Exploring the role of blockchain technology in improving sustainable supply chain performance: a system-analysis-based approach. IEEE Transactions on Engineering Management, 71, 4389-4405.

[15] Shaikh, Z. A., Khan, A. A., Baitenova, L., Zambinova, G., Yegina, N., Ivolgina, N., ... & Barykin, S. E. (2022). Blockchain hyperledger with non-linear machine learning: A novel and secure educational accreditation registration and distributed ledger preservation architecture. Applied Sciences, 12(5), 2534.

[16] Tissaoui, K., Zaghdoudi, T., Boubaker, S., Hkiri, B., & Talbi, M. (2024). Testing the Nonlinear Long-and Short-Run Distributional Asymmetries Effects of Bitcoin Prices on Bitcoin Energy Consumption: New Insights through the QNARDL Model and XGBoost Machine-Learning Tool. *Energies*, *17*(12), 2810.