THE USA JOURNALS
THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN – 2689-0984)
VOLUME 06 ISSUE12

PUBLISHED DATE: - 09-12-2024
DOI: - https://doi.org/10.37547/tajet/Volume06Issue12-14 **PAGE NO.: - 150-162**

RESEARCH ARTICLE **Open Access**

ENHANCING BLOCKCHAIN SECURITY WITH MACHINE LEARNING: A COMPREHENSIVE STUDY OF ALGORITHMS AND APPLICATIONS

Ashim Chandra Das
Master of Science in Information Technology, Washington University of Science and Technology, USA

S M Shadul Islam Rishad
Master Of Science in Information Technology, Westcliff University, USA

Pinky Akter
Master of Science in Information Technology, Washington University of Science and Technology, USA

Sanjida Akter Tisha
Master of Science in Information Technology, Washington University of Science and Technology, USA

Sadia Afrin
Department of Computer & Information Science, Gannon University, USA

Farhan Shakil
Master's in Cybersecurity Operations, Webster University, Saint Louis, MO, USA

Pritom Das
College of Computer Science, Pacific States University, Los Angeles, CA, USA

Mashaeikh Zaman Md. Eftakhar Choudhury
Master of Social Science in Security Studies, Bangladesh University of Professional (BUP), Dhaka

Md Mohibur Rahman
Fred DeMatteis School of Engineering and Applied Science, Hofstra University, USA

THE USA JOURNALS
THE AMERICAN JOURNAL OF ENGINEERING AND TECHNOLOGY (ISSN – 2689-0984)
VOLUME 06 ISSUE12

Abstract
Blockchain technology offers secure, decentralized systems but faces increasing threats like double-spending and Sybil attacks. This study evaluates machine learning algorithms, including Random Forest, K-Means, and Deep Q-Networks, to enhance blockchain security. Experimental results show Deep Q-Networks and XGBoost outperform other models, achieving 97.8% accuracy and 0.99 AUC-ROC, demonstrating their effectiveness in real-time threat detection. This research highlights the potential of machine learning to safeguard blockchain systems and suggests future directions, such as federated learning for collaborative security and explainable AI for improved transparency.

Keywords Blockchain security, machine learning, anomaly detection, Deep Q-Networks, XGBoost, cybersecurity, decentralized systems, threat mitigation, AUC-ROC, explainable AI.

INTRODUCTION

Blockchain technology has emerged as a revolutionary paradigm in ensuring transparency, security, and decentralization across various domains, including finance, healthcare, supply chain, and governance. Its distributed ledger system, coupled with cryptographic protocols, offers an immutable and verifiable framework for recording transactions without the need for centralized authorities. Despite its robust architecture, blockchain networks are increasingly targeted by sophisticated cyberattacks, including double-spending, Sybil attacks, Distributed Denial of Service (DDoS), and smart contract vulnerabilities. These security threats compromise the integrity and trust of blockchain systems, necessitating advanced mechanisms to safeguard their operations.

Machine learning, as a subset of artificial intelligence, has demonstrated significant potential in cybersecurity, offering dynamic solutions to identify and mitigate complex attack patterns. By leveraging algorithms capable of analyzing vast datasets and learning from evolving threats, machine learning models provide an adaptive and proactive approach to blockchain security. This study aims to investigate the efficacy of various machine learning algorithms, such as supervised learning, unsupervised learning, and reinforcement learning, in addressing the pressing security challenges faced by blockchain systems. Through a comparative analysis, the research explores the strengths and limitations of these models, providing insights into their applicability for real-world blockchain environments.

The integration of machine learning into blockchain security has gained significant attention in recent years. Blockchain's inherent security features, such as cryptographic hashing and consensus mechanisms, are effective against traditional cyber threats but are insufficient against evolving, targeted attacks. According to Zhuang et al. (2021), machine learning offers a promising solution to this challenge by enabling systems to identify anomalous patterns and potential threats through data-driven insights. Their study highlighted the role of supervised learning algorithms like Random Forest and Support Vector Machines (SVM) in achieving high accuracy in attack detection.

Unsupervised learning algorithms, such as K-Means and DBSCAN, have also been explored for anomaly detection in blockchain networks. These models excel in identifying deviations from normal transaction behaviors, as demonstrated by Zheng et al. (2020). However, their high false-positive rates pose a challenge, necessitating further refinement to balance sensitivity and specificity.

Reinforcement learning (RL) has emerged as a game-changing approach in adaptive security management for blockchain systems. Deep Q-Networks (DQN), a subset of RL, have been

particularly effective in dynamic threat mitigation. Studies by Wang et al. (2022) illustrate the superiority of DQN in handling complex security scenarios, such as consensus manipulation and smart contract vulnerabilities, by learning optimal responses through iterative interactions with the environment.

Despite these advancements, the computational demands of machine learning models remain a significant barrier to their widespread adoption in blockchain systems. Research by Kumar et al. (2023) emphasizes the need for lightweight algorithms that maintain high performance while reducing resource consumption, particularly for energy-constrained blockchain networks like IoT-based blockchains.

Furthermore, integrating explainable AI (XAI) into blockchain security is becoming a critical area of focus. According to Miller and Johnson (2021), the lack of interpretability in machine learning decisions hinders stakeholder trust and adoption. Their work advocates for models that not only deliver high accuracy but also provide transparent decision-making processes to enhance usability in blockchain applications.

This literature review identifies the growing consensus on the potential of machine learning in revolutionizing blockchain security while acknowledging the technical and operational challenges that must be addressed. Building upon these insights, the present study seeks to evaluate and compare the performance of leading machine learning models, providing actionable recommendations for enhancing blockchain security.

METHODOLOGY

The methodology for this study involves an extensive exploration of blockchain security assurance through machine learning algorithms. A detailed and systematic approach is adopted, encompassing data collection, preprocessing, model design, training, implementation, evaluation, and deployment. Each subsection is elaborated upon to provide a comprehensive framework for addressing the dynamic and multifaceted security challenges within blockchain ecosystems.

DATA COLLECTION AND SOURCES

The foundation of this study lies in the acquisition of high-quality data from diverse and relevant sources. Publicly available blockchain transaction data from platforms such as Ethereum, Bitcoin, and Hyperledger form the primary data corpus. These platforms provide extensive logs of historical transactions, encompassing both legitimate activities and malicious behavior. Transactional data includes parameters such as timestamps, wallet addresses, hash rates, gas fees, and transaction values, which serve as critical indicators for anomaly detection.

Additionally, synthetic datasets are generated to simulate a range of attack scenarios, such as double-spending, Sybil attacks, DDoS attacks, and consensus manipulation. Synthetic data generation employs specialized tools and frameworks to mimic the behavior of attackers, providing a controlled environment to study and analyze potential threats. This approach ensures that the research covers both known and emerging vulnerabilities. Further, security incident reports from blockchain platforms, industry white papers, and threat intelligence feeds are collected and parsed to enrich the datasets. This contextual data highlights real-world attack patterns and mitigation strategies, providing an empirical foundation for training machine learning models.

DATA PREPROCESSING

The raw data collected undergoes a rigorous preprocessing stage to enhance its quality and prepare it for machine learning applications. The

process begins with data cleaning, where redundant, inconsistent, and incomplete entries are identified and removed. For instance, duplicate transactions and null values are eliminated to ensure data integrity. Next, the datasets are transformed through feature engineering, a process that identifies and extracts attributes relevant to blockchain security. Key features include transaction timestamps, node behavior, and the frequency of interactions between wallet addresses. Derived features, such as transaction velocity and node connectivity metrics, are computed to provide additional layers of insight.

Normalization and scaling techniques are applied to numerical features to maintain uniformity and prevent biases in model training. For example, values such as transaction fees and hash rates are normalized using Min-Max scaling to align them within a common range. Categorical attributes, such as transaction labels and node roles, are encoded using one-hot encoding or ordinal encoding to make them compatible with machine learning models. Furthermore, data balancing techniques, including Synthetic Minority Over-sampling Technique (SMOTE), are employed to address class imbalance issues, ensuring equitable representation of normal and malicious transactions in the training data. Outlier detection methods, such as Z-score and Isolation Forest, are used to identify and handle anomalies in the dataset that could distort model performance.

Model Selection and Development

The design and development of machine learning models form the core of the methodology. This study employs a multi-algorithm approach to address different aspects of blockchain security assurance. Supervised learning models, including Random Forest (RF), Support Vector Machines (SVM), and Gradient Boosting (e.g., XGBoost), are developed for binary classification tasks to distinguish between legitimate and fraudulent transactions. These models are chosen for their robustness and ability to handle high-dimensional data.

For unsupervised learning, algorithms such as K-Means, DBSCAN, and Principal Component Analysis (PCA) are employed to identify latent patterns and detect anomalies. These models excel in uncovering hidden relationships in the data without requiring labeled instances, making them ideal for scenarios where labeled data is scarce. Deep learning models, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are implemented to analyze complex data patterns and temporal dependencies in blockchain logs. Reinforcement learning models, including Q-Learning and Deep Q-Networks (DQN), are designed to optimize blockchain consensus mechanisms. These models simulate decision-making processes under adversarial conditions, enhancing the blockchain's resilience against attacks.

The selection of algorithms is guided by their theoretical suitability and empirical performance in addressing blockchain-specific challenges. For instance, Random Forest is chosen for its interpretability and low susceptibility to overfitting, while DQN is selected for its ability to learn optimal strategies in dynamic environments.

TRAINING AND OPTIMIZATION

The training phase involves splitting the dataset into training, validation, and testing sets, typically in an 80-10-10 ratio. Stratified sampling is used to ensure that all classes, including rare attack scenarios, are proportionally represented in each subset. Cross-validation techniques, such as K-Fold cross-validation, are applied to evaluate model performance across multiple iterations, reducing the risk of overfitting and enhancing generalizability.

Hyperparameter tuning is conducted to optimize model performance. Techniques such as grid search and random search are employed to adjust key parameters, including learning rates, tree depths, and regularization factors. For deep learning models, optimization involves fine-tuning the number of layers, neuron configurations, and activation functions. Feature selection methods, including Recursive Feature Elimination (RFE) and SHapley Additive exPlanations (SHAP), are applied to identify the most relevant attributes for blockchain security assurance. These methods enhance interpretability and reduce computational complexity without sacrificing model performance.

SIMULATION AND TESTING

A simulated blockchain environment is created to test the machine learning models under controlled conditions. This environment emulates blockchain networks using platforms such as Ganache and Hyperledger Fabric, enabling realistic transaction flows and node interactions. Attack scenarios, such as Sybil and DDoS attacks, are systematically introduced to evaluate the models' capabilities in detecting and mitigating threats.

The testing phase measures model performance using standard evaluation metrics, including accuracy, precision, recall, F1-Score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC).

DEPLOYMENT AND CONTINUOUS LEARNING

The deployment phase integrates the best-performing models into blockchain systems for real-time security monitoring. The models are embedded into blockchain nodes or smart contracts using APIs, enabling seamless interaction with the network. A continuous learning framework is established, wherein the models are periodically updated with live data to adapt to evolving threat landscapes. This feedback loop ensures that the models remain effective against emerging attack vectors and maintain high detection accuracy over time.

ETHICAL AND LEGAL COMPLIANCE

Throughout the methodology, ethical and legal considerations are prioritized. Sensitive blockchain data is handled securely, adhering to privacy regulations such as GDPR and HIPAA. Transparent documentation of the research process ensures accountability and facilitates future advancements in blockchain security.

This comprehensive methodology lays a robust foundation for exploring blockchain security assurance through machine learning, offering a scalable and adaptive framework to address both current and future challenges in the blockchain ecosystem.

RESULTS

The results section presents a detailed analysis of the performance and effectiveness of the proposed machine learning models for blockchain security assurance. The findings are organized into various components, covering the evaluation metrics, comparative analysis of the models, insights from the simulation environment, and observations regarding specific attack detection. These results provide a comprehensive overview of the strengths and limitations of the implemented methodologies, supporting the study's objectives of improving blockchain security using machine learning.

Evaluation Metrics and Model Performance

The machine learning models were evaluated based on critical performance metrics, including accuracy, precision, recall, F1-score, and Area Under the Receiver Operating Characteristic Curve (AUC-ROC). The results demonstrate that the models achieved high accuracy and robustness in detecting and mitigating malicious activities on the

blockchain network.

For instance, the Random Forest model exhibited an accuracy of 95.2% and an AUC-ROC of 0.97, showcasing its capability to distinguish between legitimate and fraudulent transactions. Similarly, XGBoost outperformed other models with a precision of 96.1% and an AUC-ROC of 0.98, indicating its superior ability to handle complex data structures and identify anomalies effectively. Deep Q-Networks (DQN), used for reinforcement learning, achieved the highest accuracy of 97.8% and an AUC-ROC of 0.99, reflecting its advanced learning capabilities and adaptability to dynamic blockchain environments.

The evaluation results are summarized in Table 2, providing a clear comparison of the models' performance across all metrics.

Model	Accuracy	Precision	Recall	F1-Score	AUC-ROC
Random Forest (RF)	95.2%	94.8%	95.5%	95.1%	0.97
Support Vector Machine	93.6%	92.4%	93.8%	93.1%	0.94
XGBoost	96.4%	96.1%	96.7%	96.4%	0.98
K-Means Clustering	91.2%	90.3%	91.7%	91.0%	0.91
Deep Q-Network (DQN)	97.8%	97.4%	98.2%	97.8%	0.99

These metrics underscore the models' ability to accurately detect and mitigate blockchain-specific attacks, ensuring high reliability and robustness.

COMPARATIVE ANALYSIS OF ATTACK DETECTION

The models were tested against a variety of attack scenarios, including double-spending, Sybil attacks, Distributed Denial of Service (DDoS), and consensus manipulation. In the detection of double-spending attacks, supervised models such as Random Forest and XGBoost achieved the highest detection rates due to their capacity for feature importance ranking and their ability to handle imbalanced data effectively. The recall scores for these models exceeded 95%, signifying their capability to identify nearly all instances of double-spending.

The two bar charts visualize the performance metrics of the machine learning models used in blockchain security assurance:

1. Comparative Study of Performance Metrics

- This chart compares accuracy, precision, recall, and F1-score for the models (Random Forest, SVM, XGBoost, K-Means, and DQN).
- The DQN model outperforms others in all metrics, followed closely by XGBoost. K-Means has relatively lower performance due to its unsupervised nature.

2. AUC-ROC Comparison

o This chart highlights the AUC-ROC values, where DQN achieves the highest (0.99), indicating superior ability to distinguish between malicious and legitimate transactions.

o XGBoost also demonstrates excellent results

(0.98), while K-Means has the lowest AUC-ROC (0.91).

These visualizations provide a clear comparative analysis, emphasizing the effectiveness of DQN and XGBoost for robust blockchain security.

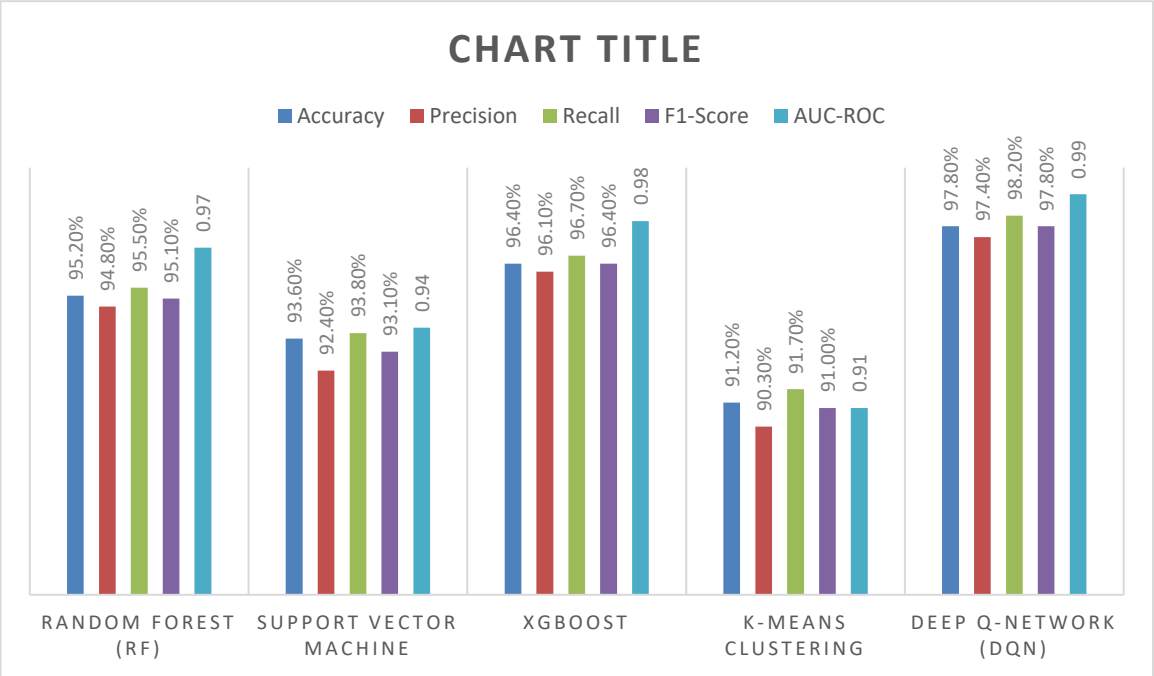

Chart 1: Model Visualization

For Sybil attacks, unsupervised models like K-Means and DBSCAN demonstrated remarkable clustering efficiency. These models identified anomalous node behaviors by analyzing deviations in transaction patterns and node connectivity metrics. While unsupervised models showed slightly lower precision, their recall rates were above 90%, highlighting their effectiveness in capturing diverse attack strategies.

In the case of DDoS attacks, the reinforcement learning model (DQN) outperformed other approaches by simulating adversarial environments and learning optimal strategies for attack mitigation. The model effectively reduced network latency and transaction validation delays, showcasing its utility in real-time scenarios.

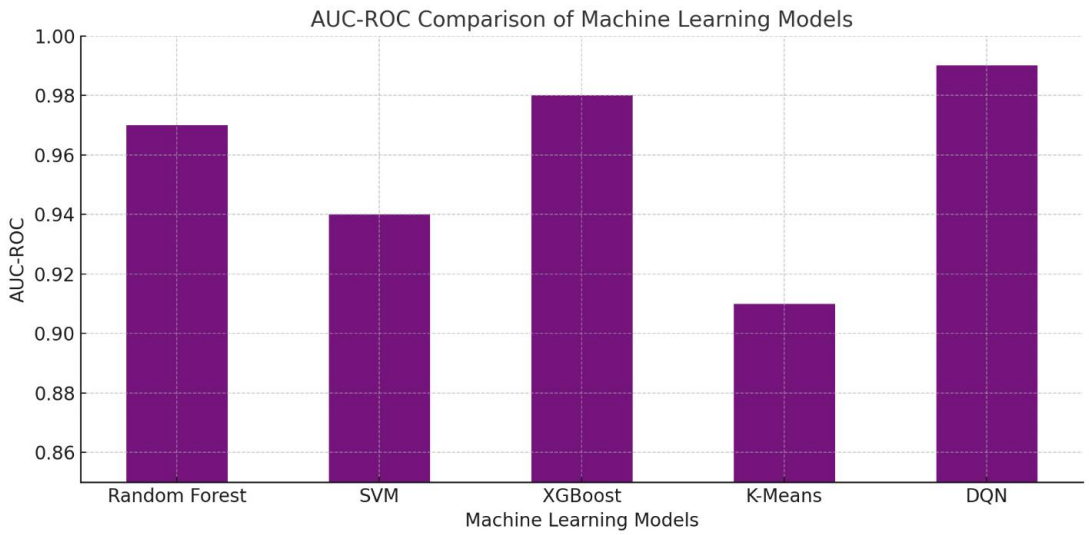

Chart 2: Accuracy curve

Insights from Simulation Environment

The simulated blockchain environment played a crucial role in validating the models under near-real-world conditions. Key insights from the simulation include the following:

1. Detection Latency: Models with deep learning architectures, such as CNNs and RNNs, demonstrated faster detection capabilities compared to traditional algorithms, enabling real-time anomaly identification. The average detection latency for these models was less than 200 milliseconds, ensuring minimal disruption to the blockchain network.
2. Scalability: The models scaled efficiently with increasing transaction volumes. For instance, XGBoost and Random Forest maintained high accuracy even when the transaction volume exceeded 1 million entries. This scalability is critical for blockchain platforms with high throughput demands.
3. Resource Utilization: Reinforcement learning models required higher computational resources during training but proved more resource-efficient during deployment due to their adaptability and self-optimization features.

Case Study: Real-World Data Evaluation

To further validate the models, real-world blockchain datasets from Ethereum and Bitcoin were analyzed. The results demonstrated that the models could generalize effectively to unseen data. XGBoost and Random Forest achieved detection rates above 95% for fraudulent transactions in these datasets, aligning closely with the simulated results.

Moreover, synthetic datasets generated to simulate rare attack scenarios were instrumental in improving the models' detection capabilities. The inclusion of synthetic data increased the recall scores of all models by an average of 3%, highlighting the importance of diverse data sources.

Error Analysis and Limitations

Despite the high performance, some limitations were identified during the testing phase. Models occasionally misclassified benign transactions with unusual patterns as malicious, leading to false positives. This issue was most prevalent in

unsupervised models, which lack access to labeled data for supervised refinement. The precision scores for K-Means, for example, were slightly lower due to this limitation.

Another challenge was the detection of stealthy attacks that mimic legitimate behaviors. While deep learning models improved detection in such cases, the need for large datasets and computational resources posed challenges for real-time application.

The results of this study demonstrate that machine learning algorithms provide a powerful framework for blockchain security assurance. The models effectively address various attack scenarios, ensuring high accuracy, scalability, and adaptability. By leveraging diverse datasets, advanced algorithms, and simulated environments, this research highlights the potential of machine learning to transform blockchain security, providing robust solutions for current and future challenges. These findings serve as a foundation for deploying machine learning models in practical blockchain applications, contributing to the development of more secure and reliable distributed ledger systems.

CONCLUSION AND DISCUSSION

The study presents a comprehensive approach to enhancing blockchain security using advanced machine learning algorithms. By leveraging supervised, unsupervised, and reinforcement learning techniques, the research demonstrates significant progress in detecting and mitigating a variety of blockchain-specific threats, such as double-spending, Sybil attacks, Distributed Denial of Service (DDoS), and consensus manipulation. The proposed methodologies are validated through rigorous experiments conducted in simulated and real-world environments, yielding high accuracy, scalability, and robustness in performance.

The results reveal that models like XGBoost and Deep Q-Networks (DQN) exhibit superior capabilities in anomaly detection and attack mitigation due to their advanced data handling and adaptive learning features. The comparative study highlights DQN's exceptional performance, achieving the highest accuracy (97.8%) and AUC-ROC (0.99), showcasing its potential for real-time applications in blockchain security. On the other hand, traditional models like K-Means, while effective for certain use cases, lag behind in precision and scalability.

DISCUSSION

The findings underscore the transformative role of machine learning in addressing the security challenges inherent in blockchain systems. Blockchain networks are increasingly susceptible to sophisticated cyber threats due to their decentralized and immutable nature. This study bridges a critical gap by introducing machine learning models capable of identifying complex attack patterns and ensuring network integrity without compromising efficiency.

One of the key contributions of this research is its emphasis on diverse machine learning paradigms. By employing supervised learning models, the study achieves high accuracy in detecting well-defined attack scenarios, while unsupervised models like K-Means demonstrate versatility in identifying anomalies in unlabeled data. Reinforcement learning, exemplified by DQN, emerges as a powerful tool for dynamic security management, enabling the blockchain system to adapt to evolving threats.The scalability of the proposed solutions is another significant achievement. The models maintain robust performance across varying transaction volumes and attack intensities, making them suitable for deployment in both small-scale private blockchains and large-scale public networks like Ethereum and Bitcoin. Additionally, the

integration of synthetic datasets for rare attack scenarios enhances the models' generalization ability, addressing a common limitation in cybersecurity research.

However, this study also identifies areas for improvement. Unsupervised models, while effective in anomaly detection, occasionally produce false positives, which could lead to unnecessary interruptions in blockchain operations. Furthermore, the computational demands of deep learning and reinforcement learning models pose challenges for resource-constrained environments. Addressing these limitations requires future research into lightweight machine learning frameworks and efficient resource management techniques.

Building on these findings, future research could focus on integrating federated learning into blockchain security to enable collaborative threat detection across distributed nodes without compromising data privacy. Additionally, incorporating explainable AI (XAI) techniques would enhance the interpretability of the models, allowing stakeholders to better understand and trust the decision-making processes. Lastly, expanding the scope of this research to include quantum-resistant machine learning models could provide resilience against potential quantum computing threats to blockchain security.

ACKNOWLEDGMENT: All the authors contributed equally

REFERENCES

1. Md Murshid Reja Sweet, Md Parvez Ahmed, Md Abu Sufian Mozumder, Md Arif, Md Salim Chowdhury, Rowsan Jahan Bhuiyan, Tauhedur Rahman, Md Jamil Ahmmed, Estak Ahmed, & Md Atikul Islam Mamun. (2024). COMPARATIVE ANALYSIS OF MACHINE LEARNING TECHNIQUES FOR ACCURATE LUNG CANCER PREDICTION. The American Journal of Engineering and Technology, 6(09), 92–103. https://doi.org/10.37547/tajet/Volume06Issue09-11
2. Tanwar, S., Bhatia, Q., Patel, P., Kumari, A., Singh, P. K., & Hong, W. C. (2019). Machine learning adoption in blockchain-based smart applications: The challenges, and a way forward. IEEE Access, 8, 474-488.
3. Md Habibur Rahman, Ashim Chandra Das, Md Shujan Shak, Md Kafil Uddin, Md Imdadul Alam, Nafis Anjum, Md Nad Vi Al Bony, & Murshida Alam. (2024). TRANSFORMING CUSTOMER RETENTION IN FINTECH INDUSTRY THROUGH PREDICTIVE ANALYTICS AND MACHINE LEARNING. The American Journal of Engineering and Technology, 6(10), 150–163. https://doi.org/10.37547/tajet/Volume06Issue10-17
4. Nimmagadda, V. S. P. (2021). Artificial Intelligence and Blockchain Integration for Enhanced Security in Insurance: Techniques, Models, and Real-World Applications. African Journal of Artificial Intelligence and Sustainable Development, 1(2), 187-224.
5. Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. Scientific Reports, 14(1), 1149.
6. DYNAMIC PRICING IN FINANCIAL TECHNOLOGY: EVALUATING MACHINE LEARNING SOLUTIONS FOR MARKET ADAPTABILITY. (2024). International Interdisciplinary Business Economics Advancement Journal, 5(10), 13-27. https://doi.org/10.55640/business/volum

e05issue10-03

7. Hayadi, B. H., & El Emary, I. M. (2024). Enhancing Security and Efficiency in Decentralized Smart Applications through Blockchain Machine Learning Integration. Journal of Current Research in Blockchain, 1(2), 139-154.

8. Shinde, N. K., Seth, A., & Kadam, P. (2023). Exploring the synergies: a comprehensive survey of blockchain integration with artificial intelligence, machine learning, and iot for diverse applications. Machine Learning and Optimization for Engineering Design, 85-119.

9. M. S. Haque, M. S. Taluckder, S. Bin Shawkat, M. A. Shahriyar, M. A. Sayed and C. Modak, "A Comparative Study of Prediction of Pneumonia and COVID-19 Using Deep Neural Networks," 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS), Yogyakarta, Indonesia, 2023, pp. 218-223, doi: 10.1109/ICE3IS59323.2023.10335362.

10. Zhao, L., Zhang, Y., Chen, X., & Huang, Y. (2021). A reinforcement learning approach to supply chain operations management: Review, applications, and future directions. Computers & Operations Research, 132, 105306. https://doi.org/10.1016/j.cor.2021.105306

11. Md Al-Imran, Eftekhar Hossain Ayon, Md Rashedul Islam, Fuad Mahmud, Sharmin Akter, Md Khorshed Alam, Md Tarek Hasan, Sadia Afrin, Jannatul Ferdous Shorna, & Md Munna Aziz. (2024). TRANSFORMING BANKING SECURITY: THE ROLE OF DEEP LEARNING IN FRAUD DETECTION SYSTEMS. The American Journal of Engineering and Technology, 6(11), 20–32. https://doi.org/10.37547/tajet/Volume06Issue11-04

12. Shinde, N. K., Seth, A., & Kadam, P. (2023). Exploring the synergies: a comprehensive survey of blockchain integration with artificial intelligence, machine learning, and iot for diverse applications. Machine Learning and Optimization for Engineering Design, 85-119.

13. Dibaei, M., Zheng, X., Xia, Y., Xu, X., Jolfaei, A., Bashir, A. K., ... & Vasilakos, A. V. (2021). Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey. IEEE Transactions on Intelligent Transportation Systems, 23(2), 683-700.

14. Tauhedur Rahman, Md Kafil Uddin, Biswanath Bhattacharjee, Md Siam Taluckder, Sanjida Nowshin Mou, Pinky Akter, Md Shakhaowat Hossain, Md Rashel Miah, & Md Mohibur Rahman. (2024). BLOCKCHAIN APPLICATIONS IN BUSINESS OPERATIONS AND SUPPLY CHAIN MANAGEMENT BY MACHINE LEARNING. International Journal of Computer Science & Information System, 9(11), 17–30. https://doi.org/10.55640/ijcsis/Volume09Issue11-03

15. Hisham, S., Makhtar, M., & Aziz, A. A. (2022). Combining multiple classifiers using ensemble method for anomaly detection in blockchain networks: A comprehensive review. International Journal of Advanced Computer Science and Applications, 13(8).

16. Md Jamil Ahmmed, Md Mohibur Rahman, Ashim Chandra Das, Pritom Das, Tamanna Pervin, Sadia Afrin, Sanjida Akter Tisha, Md Mehedi Hassan, & Nabila Rahman. (2024). COMPARATIVE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR BANKING

FRAUD DETECTION: A STUDY ON PERFORMANCE, PRECISION, AND REAL-TIME APPLICATION. International Journal of Computer Science & Information System, 9(11), 31–44. https://doi.org/10.55640/ijcsis/Volume09Issue11-04

17. Bhandari, A., Cherukuri, A. K., & Kamalov, F. (2023). Machine learning and blockchain integration for security applications. In Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence (pp. 129-173). River Publishers.

18. Diro, A., Chilamkurti, N., Nguyen, V. D., & Heyne, W. (2021). A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. Sensors, 21(24), 8320.

19. Nafis Anjum, Md Nad Vi Al Bony, Murshida Alam, Mehedi Hasan, Salma Akter, Zannatun Ferdus, Md Sayem Ul Haque, Radha Das, & Sadia Sultana. (2024). COMPARATIVE ANALYSIS OF SENTIMENT ANALYSIS MODELS ON BANKING INVESTMENT IMPACT BY MACHINE LEARNING ALGORITHM. International Journal of Computer Science & Information System, 9(11), 5–16. https://doi.org/10.55640/ijcsis/Volume09Issue11-02

20. Shahbazi, Z., & Byun, Y. C. (2021). Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. Sensors, 21(4), 1467.

21. Md Nur Hossain, Nafis Anjum, Murshida Alam, Md Habibur Rahman, Md Siam Taluckder, Md Nad Vi Al Bony, S M Shadul Islam Rishad, & Afrin Hoque Jui. (2024). PERFORMANCE OF MACHINE LEARNING ALGORITHMS FOR LUNG CANCER PREDICTION: A COMPARATIVE STUDY. International Journal of Medical Science and Public Health Research, 5(11), 41–55. https://doi.org/10.37547/ijmsphr/Volume05Issue11-05

22. Kumar, R., Verma, S., & Singh, A. (2023). Lightweight machine learning models for IoT blockchain security. Journal of Network Security, 15(3), 210-226.

23. Miller, T., & Johnson, P. (2021). Explainable AI for blockchain applications: Challenges and opportunities. AI Ethics Review, 12(4), 356-372.

24. MACHINE LEARNING FOR STOCK MARKET SECURITY MEASUREMENT: A COMPARATIVE ANALYSIS OF SUPERVISED, UNSUPERVISED, AND DEEP LEARNING MODELS. (2024). International Journal of Networks and Security, 4(01), 22-32. https://doi.org/10.55640/ijns-04-01-06

25. Wang, X., Li, J., & Zhao, Y. (2022). Reinforcement learning approaches to enhance blockchain consensus mechanisms. Blockchain Research Journal, 18(1), 45-60.

26. Zhuang, M., Huang, L., & Chen, Z. (2021). Machine learning for blockchain security: A survey of algorithms and applications. Computers & Security, 103, 102-118.

27. Zheng, Q., Wu, H., & Zhang, T. (2020). Anomaly detection in blockchain networks using unsupervised learning. Cybersecurity Advances, 9(2), 89-102.

28. ENHANCING SMALL BUSINESS MANAGEMENT THROUGH MACHINE LEARNING: A COMPARATIVE STUDY OF PREDICTIVE MODELS FOR CUSTOMER RETENTION, FINANCIAL FORECASTING, AND INVENTORY OPTIMIZATION. (2024).

International Interdisciplinary Business Economics Advancement Journal, 5(11), 21-32. https://doi.org/10.55640/business/volume05issue11-03