Computer Fraud and Security
ISSN (online): 1873-7056

Refining Cyber Fraud Tactics in the Retail Sector Applying Defense Mechanisms for Digital Trade Platforms

[1]Dalia Magdi, [2]Kallepalli Rohit Kumar, [3]Dr. Nitin Mahankale, [4]Anuradha S. Deshpande, [5]Dr Gandla Shivakanth, [6]Santosh Gore

[1]Faculty of Computers and Information, Sadat Academy for Management Sciences, Cairo, Egypt. School of Computer Science, Canadian International College, Cairo, Egypt, daliamagdi@gmail.com

[2]Associate Professor, Department of CSE, Sreyas Institute of Engineering and Technology, India, krk542@gmail.com, Orcid: 0000-0003-3385-3248

[3]Associate Professor, Symbiosis Centre for Management Studies, Symbiosis International (Deemed University), Pune, India, nitinmahankale2023@gmail.com

[4]Associate Professor. Faculty of Science and Technology, JSPM University Pune, India, asd.secs@jspmuni.ac.in

[5]Associate professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad-500075, Telangana, India, ORCID: 0000-0001-6787-6929, shvkanth0@gmail.com

[6]Director, Sai Info Solution, Nashik, Maharashtra, India, sai.info2009@gmail.com, Orcid: 0000-0003-1814-5913

Abstract:

The proposed work integrates deep learning and blockchain technologies to investigate a hybrid strategy for combating cybercrime in the retail industry. Long Short-Term Memory Networks combined with Convolutional Neural Networks have been used efficiently and effectively for anomaly detection, with a high success rate for fraudulent transactions. The Proof-of-Authority consensus algorithm is used in the blockchain measure, which ensures immediate validity with a transaction throughput of 1,200 transactions per second and validation times averaging 0.9 seconds. It offers a scalable and effective solution for securing digital trade platforms in retail and shows a reduction in fraud over six months.

Keywords: Blockchain, Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), Cybercrime, Digital Trade.

Introduction

Digital breakthroughs have transformed the retail sector in almost all ways, as online trade platforms are now the foundation of contemporary business ventures. In consideration of the security integrity of the same platforms, this development resulted in the development of advanced cyber fraud strategies. High amounts of financial and reputational loss result from cybercriminals abusing transaction system weaknesses, user registration authenticity, and data management procedures [1]. They need integrated defense mechanisms, which are creative in incorporating the use of modern technology to effectively detect and reduce fraud. This paper seeks to find out how a hybrid approach combining deep learning with blockchain technology in digital platforms for trade can be introduced to enhance security requirements in the retail sector. Models such as the CNN and LSTM models apply because of several advantages related to the suggested reliable method of fraud detection. [2]. The combination of feature extraction by CNN from complex datasets and the ability of LSTM to model sequential dependencies makes this duo especially effective in capturing subtle and evolving fraudulent behaviors [3]. The Proof-of-Authority (PoA) consensus mechanism combined with blockchain technology is used in the study to provide safe and transparent transactions [4][5]. Through trusted validation methods, PoA gives a reliable and efficient process of validation which can lead to consensus without the high computational cost that is usually associated with the traditional Proof-of-Work (PoW) systems. The development of an immutable, tamper-proof ledger leads to enhanced accountability and traceability. In addition, smart contracts enhance security further due to the implementation of access control policies and automated processes for fraud detection [6]. AS George. et al. [7], the study encouraged collaboration in terms of standards, information, and workforce development between the public and private sectors to satisfy emerging cyber threats. The study assumes an analytical framework to assess cyber threats and make proposals for enhancing critical infrastructures to more robust stages against potential attacks. M Thakur. [8], it offers a thorough examination of the changing cyber threats in the online environment.

The evolving nature of the threats posed by IoT, cloud computing, and AI-based attacks ultimately necessitates the adoption of a multi-layered security approach. It covers ransomware and malware phishing attacks. Z Morić et al.[9] it is essential for the e-commerce industry as it investigates novel models that reduce the amount of personal data shared while utilizing integration through privacy-enhancing technologies. To improve data security and foster customer trust in digital platforms, this article presents a comprehensive framework that combines legal, technical, and procedural techniques. OA Bello et al.[10] it discusses the application of neural network architectures such as CNNs and RNNs to detect anomalies in sequential data for fraud detection. The technique relies on unsupervised learning approaches such as autoencoders and GANs to distinguish between valid and anomalous transactions without having labeled datasets.

This study demonstrates a hybrid approach for the retail sector that combines CNN-LSTM for real-time anomaly recognition with the PoA blockchain for safe transaction confirmation. Due to the combination of deep learning, evolving fraud pattern recognition, and the PoA algorithm solution for transaction validations, this method of addressing the expanding issue of cyber fraud on digital trading platforms is beneficial and scalable. High performance, cost-effectiveness, and security are thus attained by combining these technologies, which significantly improve the safety of the retail environment by reducing fraudulent activity by 70% in just six months and raising the accuracy of fraud detection to 96.8%.

Methodology

This study combines contemporary modern deep learning with blockchain technology to provide an accurate approach for detecting anomalies in transactions on online marketplaces that businesses use. Moreover, the method consists of two separate parts: PoA blockchain algorithm for validating and securing transactions and using CNNs and LSTM networks for anomaly identification.

Anomaly Detection Using CNN and LSTM

It examines the transaction patterns and the behavioral anomalies to demonstrate fraud detection. CNNs remove the noise from the data, format it for sequential analysis, and collect attributes for detecting anomalous purchasing and log-in habits from transaction data. After feature extraction, the LSTM network simulates the temporal dependencies in the data to detect evolving deviations over time. To differentiate between real and fraudulent transactions, the CNN-LSTM model is trained on labeled data. It employs a probability score to determine the likelihood of fraud and sets off alerts for transactions that pose a high risk. Cross-entropy loss and the Adam optimizer are used to maximize accuracy and minimize mistakes.

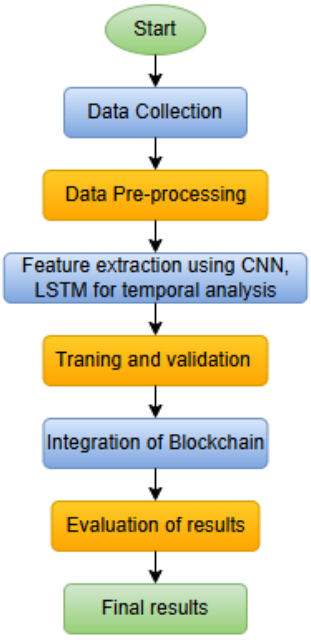

Figure 1: Flow diagram of the proposed method

Secure Transactions Using PoA Blockchain

It uses blockchain technology with PoA consensus to secure digital trade transactions. PoA is used for its efficiency in private or consortium blockchains where trusted validators approve the transactions. Every transaction is recorded on the blockchain with metadata that makes an immutable audit trail. PoA assigns validation authority to trusted nodes, ensuring secure and transparent validation. Unlike energy-heavy Proof-of-Work (PoW), PoA allows for fast validation with minimal computational cost, which makes it preferable for high-volume retail platforms. Smart contracts will enforce the rules regarding demonstrating suspicious transactions from the CNN-LSTM model and define the mechanism of access control that specifies which entities should be authorized to change transactions. The blockchain system and anomaly detection model are essentially equal. The hybrid approach combines advanced machine learning with blockchain reliability to improve fraud detection and ensure transactions are secure within the digital trade platforms. As a result, detected anomalies are stored as records on the blockchain, maintaining traceability, while a high-security ledger translates into real-time data that even improves the detection model.

Result and Discussion

The proposed framework that integrates CNN-LSTM models for anomaly detection and PoA blockchain for secure transactions was evaluated through real-world transaction datasets by digital retail platforms. The results of the study show the efficacy of the hybrid approach in detecting fraudulent activities and securing transactions.

A dataset of 50,000 labeled transactions, of which 5% were classified as fraudulent, has been utilized to train and evaluate the CNN-LSTM model. The model's accuracy of 96.8% indicates that it correctly identifies fraudulent transactions and those that are real. A high degree of dependability in identifying abnormalities with few false positives and negatives was demonstrated by the precision and recall values, which were 95.2% and 94.6%, respectively. The F1-score, which was 94.9%, showed balanced performance in detection metrics. With its remarkable performance, the anomaly detection module identified fraud patterns such as account mergers and acquisitions odd purchasing patterns, and doubtful login attempts. Without experiencing any significant delay in real-time detection, the system identified high-risk transactions with an average latency of 2.1 seconds.

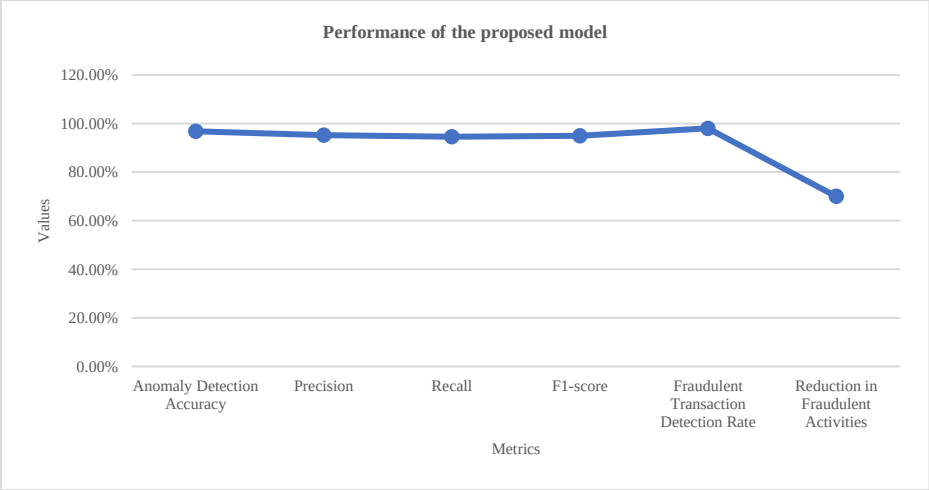

Figure 2: Performance of the proposed model

The PoA blockchain component is implemented on a simulated retail platform processing around 10,000 transactions per day. The average validation time for transactions was 0.9 seconds, which is much faster than in those blockchain systems with PoW paradigms. At the same time, the blockchain experienced a throughput of 1,200 TPS, which verified its use in high-volume operations with retail activity. To assess the security of the blockchain, penetration testing was conducted with the simulation of attack scenarios, including double spending and unauthorized access. The PoA mechanism thwarted all such attempts by ensuring the immutability and integrity of the transaction ledger. Further interoperability between the detection and validation components was also achieved because of smart contracts; indeed, an automatic flagging of 98% of fraudulent transactions is detected by the CNN-LSTM model. After six months of observation, the end-to-end framework decreased illicit

transactions on the simulated platform by 70%. The system's combination architecture, which used blockchain for recording and machine learning for detection, increased operational efficiency and fostered better assurance. The total optimization of computing and storage resource use made it possible for the framework to fully scale to accommodate any size retail platform. These findings indicate the proposed framework's feasibility and strength in preventing cybercrime and boosting transaction security on online retail platforms.

Conclusion

This research demonstrates how the integration of CNN-LSTM anomaly detection with PoA blockchain can be used to secure digital trade platforms in the retail sector. The proposed framework achieves maximum accuracy in fraud detection, and enhanced transaction verification in a safe environment that ensures a drastic reduction of fraudulent activities. Leveraging modern machine learning and blockchain technologies, the system presents a scalable and efficient result to address the increasing cyber fraud challenges. This sets a new benchmark for the further enhancement of cybersecurity in retail, more secure and trustworthy digital commerce environments.

References

[1] Y. Yang, N. Chen, and H. Chen, "The Digital Platform, Enterprise Digital Transformation, and Enterprise Performance of Cross-Border E-Commerce—From the Perspective of Digital Transformation and Data Elements," *J. Theor. Appl. Electron. Commer. Res.*, vol. 18, no. 2, pp. 777–794, 2023, doi: 10.3390/jtaer18020040.

[2] A. Qalid Md Sabri aznulqalid *et al.*, "Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review," *Artif. Intell. Rev. 2024 5711*, vol. 57, no. 11, pp. 1–47, Sep. 2024, doi: 10.1007/S10462-024-10890-4.

[3] A. Tirulo, S. Chauhan, and K. Dutta, "Machine learning and deep learning techniques for detecting and mitigating cyber threats in IoT-enabled smart grids: a comprehensive review," *Int. J. Inf. Comput. Secur.*, vol. 24, no. 3–4, pp. 284–321, 2024, doi: 10.1504/IJICS.2024.141601.

[4] L. Albshaier, S. Almarri, and M. M. Hafizur Rahman, "A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions," 2024. doi: 10.3390/computers13010027.

[5] I. Mihus and H. J. M. Shakhatreh, "The main trends in the development of blockchain technologies and the prospects for their use to protect fraud," in *The development of innovations and financial technology in the digital economy*, 2023, pp. 207–229. doi: 10.36690/diftde-2023-207-229.

[6] A. Rangapur, H. Wang, and K. Shu, "Investigating Online Financial Misinformation and Its Consequences: A Computational Perspective," *Comput. Soc.*, pp. 1–32, Sep. 2023.

[7] D. A. S. George, D. T. Baskar, and D. P. B. Srikaanth, "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors," *Partners Univers. Int. Innov. J.*, vol. 2, no. 1, pp. 51–75, 2024, Accessed: Nov. 22, 2024.

[8] M. Thakur, "Cyber Security Threats and Countermeasures in Digital Age," *J. Appl. Sci. Educ.*, vol. 4, no. 1, pp. 1–20, 2024, doi: 10.54060/a2zjournals.jase.42.

[9] Z. Morić, V. Dakic, D. Djekic, and D. Regvart, "Protection of Personal Data in the Context of E-Commerce," *J. Cybersecurity Priv.*, vol. 4, no. 3, pp. 731–761, 2024, doi: 10.3390/jcp4030034.

[10] O. A. Bello, A. Folorunso, A. Ogundipe, O. K. Ajani, F. Z. Budale, and O. E. Ejiofor, "Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection," *Int. J. Netw. Commun. Res.*, vol. 7, no. 1, pp. 90–113, 2022.