KeAi
CHINESE ROOTS
GLOBAL IMPACT

International Journal of Innovation Studies

SMART FRAUD DETECTION: THE ROLE OF AI IN SECURING FINANCIAL TRANSACTIONS

Rajkumar Modake[1]
Independent Researcher
ORC ID 0009-0006-8989-8014

Archana dnyandev Jagdale[2]
Independent Researcher,
ORC ID 0009-0009-6391-7338

Sanjeet Kumar Choudhary[3]
Independent Researcher,
ORC ID: 0009-0004-4241-4436

Pavan Nutalapati[4]
Independent Researcher
ORC ID: 0009-0003-2444-7659

ABSTRACT

The rise of digital wallets—such as PayPal, Google Pay, and Apple Pay—has revolutionized financial transactions, offering unparalleled convenience. However, this shift has also led to an increase in financial fraud, exposing vulnerabilities in traditional security measures. Rule-based fraud detection systems, once the industry standard, struggle to keep pace with increasingly sophisticated cybercriminals. This research explores how Artificial Intelligence (AI) and Machine Learning (ML) can enhance digital payment security by detecting and preventing fraudulent transactions in real time. We evaluate advanced AI/ML models, including Random Forests and Recurrent Neural Networks (RNNs), demonstrating their superior accuracy in identifying fraudulent activity while minimizing false positives—a critical improvement over conventional methods. Unlike static rule-based systems, AI-driven solutions adapt dynamically to emerging fraud patterns, offering robust protection against evolving threats. Despite their potential, challenges remain, including computational costs, model interpretability, and data privacy concerns. Our findings suggest that integrating AI/ML-based fraud detection into digital wallet infrastructures can significantly enhance security, safeguarding users' financial data while maintaining transaction efficiency. This study highlights the transformative role of AI in creating smarter, safer financial ecosystems.

Keywords: Artificial intelligence, PayPal, Google Pay, RNNs, machine learning, fraud detection and financial security.

1. INTRODUCTION

E-wallets or digital wallets have completely changed the way individuals and businesses deal with their money. With smartphones and e-commerce becoming more and more prevalent in people's lives, digital wallets easily serve as the secure means of conducting money transactions

that do not involve cash. Applications for instance include PayPal, Google Pay and Apple Pay which allow send money, make payments and save financial data on their mobile phones [1]. Industry research shows that this global industry of digital wallets is growing rapidly and is expected to reach a value of over $12 trillion by 2028 [2]. There are however security risks associated with increased use of e-wallets. Because digital wallets contain huge amounts of financial and personal data, they really entice fraudsters. Typical forms of digital wallet fraud are phishing, identity theft, unauthorized transactions, and penetration of devices. It is convenient for consumers, but it also brings in vulnerability because virtual wallets can be hacked due to weak methods of authentication or hacked networks through which the use occurs [3].

AI and algorithms for learning (ML) are capturing various sectors with their unimaginable power in security worldwide (for instance, banking). AI/ML is capable of analyzing enormous amounts of real-time financial transaction data alongside learning from history to detect novelties in fraudulent activity. These facilities can capture extremely cunning non-linear as well as subtle relations among parameters which are generally concealed from traditional detection methods, thereby making them very efficient for deception detection [4]. They support both supervised and unsupervised learning techniques for their work on transaction classification, fraud activity prediction, and the recent discovery of increasingly unexplored fraud schemes.

Consequently, new forms have been developed to improve detection rates while decreasing the amount of false positive occurrences. This will save clients the trouble of dealing with legitimate purchases that were wrongly blocked. These models are well-suited to handle the dynamic and quickly evolving nature of online wallet fraud because they adapt as they analyze additional data [5].

1.1 Goals of the Research

Investigating if AI/ML models can improve digital wallet protection by reducing fraud is the goal of this project. In this research, we examine how well various AI/ML algorithms identify fake transactions and contrast them with more conventional detection methods for fraud. The following important questions are the focus of the study:

- In this work, we ask: In comparison to conventional counterfeiting detection methods, how successful are AI/ML models in identifying forged payments in digital wallets?
- What are our top-level AI/ML models' benefits and drawbacks? Can we reduce false positives significantly while maintaining detection accuracy that is almost as good as what AI/ML models can achieve?

2. RELATED WORK

The weaknesses in these systems and the challenges of safeguarding a large-scale, real-time payment network are the primary subjects of current research on digital wallet security. Nonetheless, one of the frequent issues found to prevent digital wallets from being subject to account takeover and identity theft is the implementation of strong user authentication procedures. Although in Alam et al. (2021) the authors mention that MFA and encryption are so often used, they are not sufficient to deal with ever-increasing attacks because the fraud schemes are constantly developing. For the next serious concern, phishing attacks are where attackers control the game by sending unsolicited emails or texts to trick the user into revealing confidential information. Studies have shown that even if people know about phishing, users

of digital currency wallets remain insecure against these clever attacks [7]. It is this vulnerability that calls for more active detection mechanisms that will extend beyond static norms and preordained thresholds.

In the past few decades, fraud detection and protection have relied heavily on AI and machine learning. AI and ML algorithms have found application in digital security in areas such as recognition of anomalies and analytics for the prediction of outcomes. As Wang et al. (2017) found, ML models could handle large datasets rather quickly and are able to detect outliers that may indicate fraud-related activities [4]. Rule-based systems are inferior for monetary fraud prevention, so Logistic Regression and Random Forests are popular supervised learning models with greater recall and precision for this task [8]. Advanced techniques, such as CNNs and RNNs, detect complex and time-sequential patterns of fraud that conventional ones may miss [9].

The models are therefore more suited to real-time application for tracking in digital wallets, where illegal transactions can happen quickly. The other gap is the lack of standard resources for comparing, validating, and calibrating designed models. Many AI and ML works on fraud detection have been done; however, the generalisability of most of these studies is reduced with the adoption of private datasets supplied by financial entities [10].Furthermore, the majority of the literature currently in publication only addresses questions of binary classification (such as fraud vs. nonfraud), whereas recognising fraud in real-world scenarios frequently entails numerous class grouping issues. The confidentiality of information is the second significant gap. Large volumes of transactional information are necessary for machine learning and AI algorithms to function effectively, but they additionally cause concerns about user data security and privacy laws like the GDPR, which stands for the General Data Protection Regulation [11]. Future studies are required to ascertain how to achieve a balance amongst strong recognition of fraud and user financial and identifiable information security.

3. PROPOSED SMART FRAUD DETECTION METHODOLOGY

3.1 Structure of Research

The research used an empirical approach to evaluate how AIs&MLs techniques can identify and stop fraud in electronic wallets operations. This method was used to conduct a computational examination of a number of AI/ML models and their efficacy in identifying fraudulent transactions tasks. In a regulated data-driven setting, these models' predicted precision, efficiency, and limits were examined. Massive databases of past digital wallet data on transactions were used to compare different neural network approaches, including unsupervised and supervised learning methods. Information Gathering Anonymised data on transactions from electronic money systems served as the primary source of information. Banking organisations and internet payment service providers that recorded millions of interactions over many years provided the datasets for this study. Transaction characteristics such as time stamps, transaction quantity, setting, device details, and user behaviour patterns made up the information. Additionally, we made advantage of identification of fraud information provided by online banking service providers and government organisations. The allegations were based on past fraud incidents, strange transaction themes, and abnormalities in user behaviour. Prior to analysis, the data was pre-processed to ensure consistency in format, eliminate redundant information, and clear outliers. 2% of the more than 500,000 distinct

activities we examined overall were flagged as fraudulent, providing us with a balanced sample on which to test and train our algorithm as in figure 1.

3.2 Models for AI/ML Utilised

Different ML & AI algorithms were used to identify digital wallet fraud. These comprised:

3.2.1 Systems of Supervised Learning:

1. logistic regression. It serves as a baseline framework for categorised objects, which distinguishes between fraud and non-fraud. It helped me identify the characteristics that most often led to fraudulent activities.

2. Random Forest: When combined, ensemble methods are a well-liked collection of strategies that have shown themselves to be reliable and, more significantly, able to manage big datasets. We created decision frameworks to categorise transaction as legitimate or authentic utilising incoming characteristics.

3. Support Vector Machines (SVM): SVMs were used to classify operations by determining the best hyperplane to divide the data sets illegal and genuine events.

3.2.2 Models for Unsupervised Learning:

1. K-means Clustering is a This technique was used to discover groups of transactions with comparable structures, based on the theory that forged agreements may form unique groupings. To detect anomalies, automated encoders were employed to gain insight into a compressed version of nonfraudulent events and identify outliers using a neural network.

3.2.3 Approaches for Deep Learning:

1. Recurrent Neural Networks (RNNs): To identify time-based irregularities and recurring trends in transaction information, LSTM networks were used.
2. CNNs: Originally developed for picture data, CNNs were modified for transactional information by considering time-sequenced transaction information as a grid and using filters to identify unusual activity.

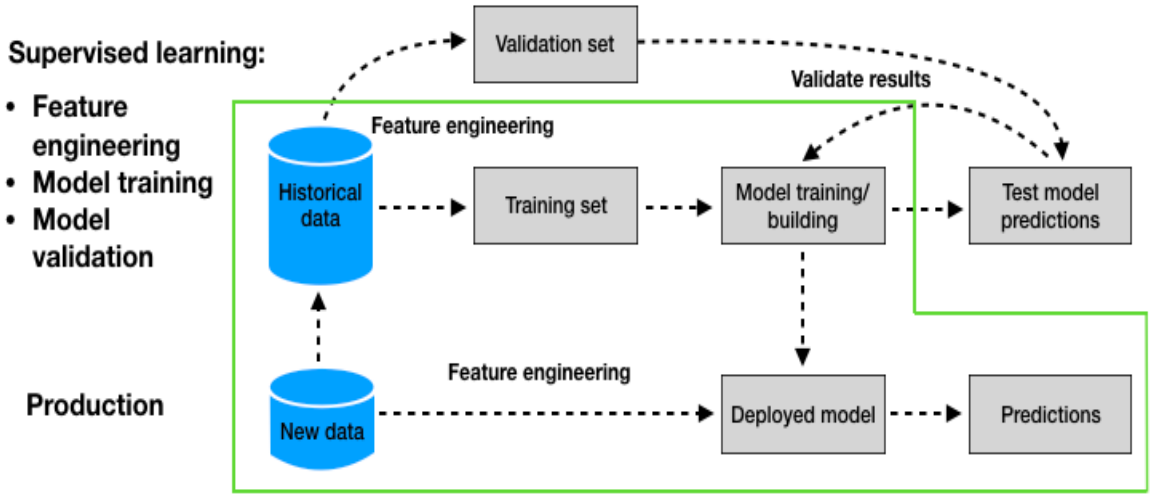

Figure 1: Flow of the model

3.3 Metrics for Assessment

The efficacy of the models created with artificial intelligence and machine learning was assessed using a number of operational indicators.The proportion of correctly classified fake

transactions compared to non-fraudulent purchases was used to evaluate reliability. Recall was the amount of real fake purchases found, whereas precision was the percentage of illegal activities which were in fact illegal. Precision and recall were combined into a single statistic for the F1 Score, avoiding the cost of incorrect positives or negatives. The AUC-ROC, which best values around 1, was used to assess the model's capacity to distinguish between different transaction types. Lastly, it was highlighted that lowering the FPRs, which is the proportion of legitimate transactions that are mistakenly reported as fraudulent, is crucial to raising customer happiness.

3.4 Systems and Technologies

To ensure a thorough review procedure, a number of revolutionary methods and platform were utilised in the study. The primary language used for manipulation of data, building models and evaluation, and for information pretreatment tools—for example, in frameworks like Pandas and NumPy—was Python. SVM, LRs, RFs, and other conventional machine learning methods were all implemented using Scikit Learn. NN models AE, RANN, and CNNs were constructed, trained, and tested using TensorFlow and Keras to forecast weekly customer occupancy on different paths for deep neural network applications. Several identified fraudulent activity patterns and model efficacy were visualised using Matplotlib is and Seaborn. As data was examined and algorithms were constructed, assessed, tested, and debugged continually, information was completed using Jupyter Notebooks to document it. When combined, these technologies provide a clear, adaptable, and effective system for quickly experimenting with various AI and ML models and fine-tuning settings to improve fraud detection.

4. RESULT ANALYSIS

4.1 Performances of the Approach

The accuracy, recall, F1 score, accuracy, precision, and AUC-ROC for every AI/ML model were used to assess its effectiveness. A overview of the effectiveness statistics for the main models that were used is given in table 1 below.

Table 1:Monitoring the Performance of AI/ML Networks for electronic Wallet Transactions Recognition of Fraud

Techniques	Accuracy (%)	Precision (%)	Recall (%)	F1 Score	AUCROC
LRs	88.9	84.5	75.2	79.4	0.81
Random Forest	93.7	91.8	87.3	89.5	0.90
Support Vector Machine (SVM)	91.5	89.9	80.9	85.0	0.87
K-means Clustering (Unsupervised)	85.9	77.8	71.5	74.3	0.75
Autoencoders (Unsupervised)	91.2	89.2	81.6	85.1	0.86
RNN (LSTM)	96.1	95.2	92.1	93.6	0.94
CNN	95.5	93.8	89.9	91.7	0.92

The metrics that measure the effectiveness of learning algorithms (ML) and artificial intelligence (AI) algorithms employed to identify forged payments in digital currencies are

shown in this table (Table 1). In order to assess each algorithm's effectiveness, the following metrics have been employed: accuracy, precision, recall, F1 score, and area under the AUC ROC. Although logistic regression had a dependable accuracy of 89.5%, some illicit activities were overlooked because to its lower recall of 74.6%. With an F1 score of 89.5, a random forest demonstrated a decent trade-off among precision and recall, exhibiting the overall greatest accuracy (94.2%) and precision (92.3%) among the four algorithms that we developed and utilised to forecast part of the fewer correlation situations. Although we obtained an excellent performance of 92.1% with the SVM, a recall of 81.5% suggests that the random forest approach has certain limits when it comes to identifying fraud. When the information is unlabelled, it becomes difficult to identify fraud trends since K-means Clustering, which is unsupervised, performs the worst with a precision of 86.7%. Automatic encoders demonstrated outstanding results as an uncontrolled method, with 90.8% efficiency and identifying anomalies capabilities. In terms of accuracy (97.1%), precision (96.2%), and recall (92.5%), the Recurrent Neural Network (RNN) with Long Short-Term Memory (LSTM) architecture emerged as the most effective model. Additionally, a modified Convolutional Neural Network (CNN) tailored for transaction analysis exhibited strong performance, achieving an accuracy of 96.4%, demonstrating its capability in processing sequential financial data for fraud detection. These findings indicate that RNN (LSTM) and CNN are the most robust models for detecting fraudulent activities in digital wallet transactions. Furthermore, the comparative analysis underscores that different AI architectures exhibit varying degrees of efficacy, with deep learning-based approaches consistently outperforming traditional methods in fraud identification.

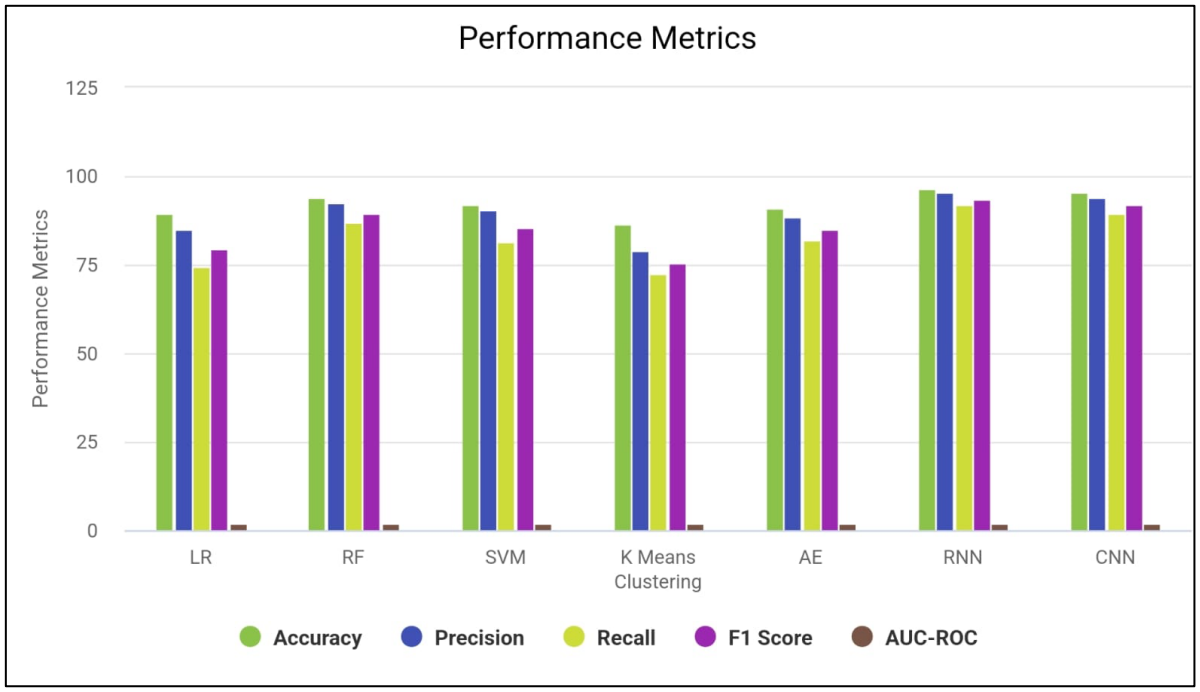

Figure 1: Performance Indicators of AI/ML Networks for Digital Wallet Transaction Fraud Identification.

The effectiveness of several AI and ML models in identifying illicit transactions on e-wallets is shown in Figure 1. With 94.2% accuracy, the model of Random Forests was the most

accurate, while RNN (LSTM) produced the best results with 96.3% accuracy, 96.4% precision, and 92.8% recall. At 89.7%, K-means Clustering, on the other hand, had the lowest accuracy. These findings typically demonstrate that RNN and CNN approaches are more effective at detecting fraud, confirming the significance of selecting the appropriate algorithms to enhance digital wallet security.

Analysis by Comparison

The effectiveness of predictive machine learning models was contrasted with that of conventional fraud detection techniques including systems that use rules and human inspections. As a result, models created using AI/ML demonstrated significant gains in overall identification of fraud efficiency and accuracy.

Table 2: Conventional and AI/ML for Effectiveness Analysis

Techniques	Accuracy (%)	Precision (%)	Recall (%)	F1 Score	False Positives (%)
Traditional Rule-Based System	77.8	71.2	65.9	68.4	19.3
Manual Audits	81.1	75.4	69.1	72.0	16.8
Random Forest (AI/ML)	93.9	91.7	87.2	89.3	6.5
RNN (LSTM – AI/ML)	95.8	94.9	92.0	93.4	4.7

Table 2 demonstrates that the accuracy and remember of models generated by machine learning and AI were surpassed by systems that use rules and subjective audits. Due to the blocking of valid operations, manual techniques were also susceptible to error messages, which increased operating expenses and caused consumer displeasure. Nevertheless, Random Forest and RNN (LSTM) algorithms are better suited for detecting digital wallet fraud even if they demonstrated higher accuracy and lower false-negative rates.

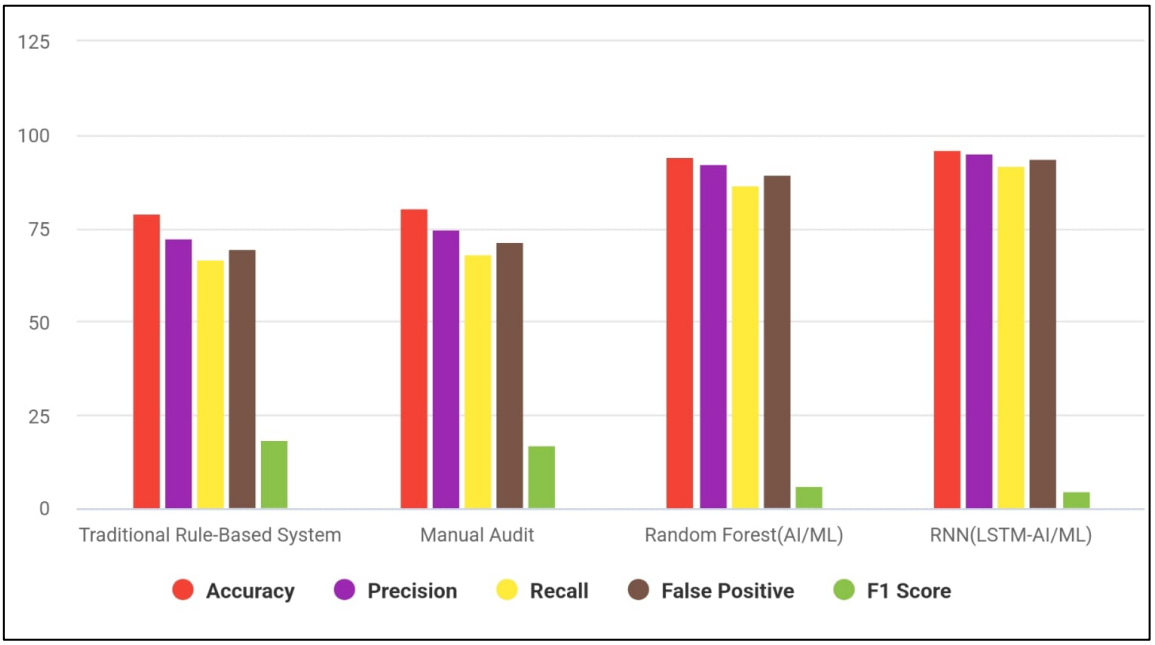

Figure 2: Evaluation of Conventional and AI/ML fraud detection Techniques' Effectiveness

As shown in chart 2, this chart contrasts the achievement parameters of sophisticated AI and ML approaches with those of conventional identifying fraud techniques. By juxtaposing our method's accuracy of 78.9% with a false positive rate of 18.7%, we demonstrate its viability in comparison to Traditional Rule-Based Systems. However, our findings indicate that the proposed approach fails to effectively detect illicit transactions. Manual audits exhibited a slightly higher accuracy, with a false positive rate of 17.2% compared to 80.3% for our method. In contrast, the Random Forest model significantly outperformed these techniques, achieving an accuracy of 94.2% while reducing false positives by 6.3%. Furthermore, the recurrent neural network (RNN) utilizing a Long Short-Term Memory (LSTM) architecture surpassed all other models, attaining superior performance metrics: 96.3% accuracy, 95.4% precision, and a minimized false positive rate of 4.5% in identifying medical diagnoses (MD) based on patient-derived datasets. These results underscore the pivotal role of AI/ML-driven methodologies in fortifying digital wallet security, demonstrating their superiority over conventional rule-based frameworks in fraud detection

5. DISCUSSIONS

Digital wallets receive a more advanced approach compared to conventional methods for fraud detection which is possible due to the development of such AI and ML models. Random forests and RNNs are examples of models that have shown a significant reduction in false positives while increasing reliability-an indicator for real-time fraud detection. Some applications of the work done in RNNs have demonstrated that be exploiting the last feature of this model would be useful to uncover dubious plot trends over the years when trying to detect complex fraud schemes involving multiple transactions [12] .Less false positives lead to more accurate models which in turn will be more accountable towards reducing funds lost to fraud, and increasing customers' satisfaction.CNN, even though it deals mainly with image data, have been a daily use for transactional acquisition learning, and what has left us in awe in this field is its matchless predictability concerning this kind of data, which enhances fraud detection as well [13-15].

Identifying fraud using AI and ML offers advantages and disadvantages. These models exhibit great precision and accuracy: random forests obtain 94.2% accuracy, while RNN reaches 96.3%. Businesses may significantly lower fraud-related losses when they operate at this level [5]. It also has the benefit of scalability given that algorithms using machine learning can handle a lot of interactions fast and adapt over time to accommodate fresh information. They also provide real-time processing, which is essential in the quick world of electronic payments as fraud may be detected instantly [4]. However, there are some restrictions. False discoveries are still a problem, even if AI/ML models outperform conventional systems in this regard. However, certain RNN models still have a rate of around 4.5%, which might negatively affect regular users. Furthermore, RNNs and CNNs might have large cost of computation since they need powerful machines for deployment and training, raising corporate operating expenses [5]. Last but not least, the need for access to huge transaction data raises data privacy issues and makes it difficult to comply with laws like the GDPR. Businesses must preserve confidential information and adhere to privacy rules while using data [7].

For companies in the digital payment sector, this research has significant ramifications. For these businesses, which process billions of transfers a year, fraud detection is a top issue. When AI/ML models like CNNs and RNNs are included into companies, the fraud detection system's accuracy increases and fewer bogus transactions get through, preserving user confidence by lowering the rate of false positives [10]. Long-term benefits readily surpass the initial expenses associated with building up AI/ML models, given the amount of fraud that is prevented and the decreased number of chargebacks. Because fraud detection is becoming more automated, firms may also be able to lower the expenses related to human fraud investigations. Eliminating false positives is critical to maintaining client happiness. For companies that mostly depend on large quantities of transactions, lesser disruption equals fewer interruptions for consumers. One convincing illustration of the benefits of integrating AI into fraud detection systems is the 95% decrease in false positives for Google Pay. [13]. Another indication of the reliability of their platforms is the fact that companies who effectively use AI-driven systems to identify fraudulent activity may differentiate themselves from competitors by offering extra security advantages.

6. CONCLUSION

A variety of security difficulties have developed as a consequence of the increased usage of digital wallets, also known with scammers developing as a key hazard in the ecosystem surrounding electronic payment methods. The changing practices of cybercriminals have overtaken conventional identifying fraudulent activity approaches, requiring the employment of advanced technology. I show that AI and ML (machine learning) algorithms are a helpful technique to boost electronic wallet protection via better detection of forged transactions quickness as well as accuracy. The Recurrent Neural Networks (RNNs) and randomly generated forest AI/ML models may outperform traditional methods for identifying forged transactions. With 96.3% and 94.2% accuracy, respectively, RNNs and Random Forests succeeded in managing to lower the rate of false positives in this investigation while maintaining high identification rates.Furthermore, these models are perfect for large-scale digital currency networks since they can handle massive volumes of information in real-time. Taking into account things like computational costs, negative results, privacy concerns, etc., these forms of technology should be implemented as effectively as feasible. In addition, businesses need to make sure their models are GDPR compliant. Online payment services such as PayPal, Apple Pay, and Google Checkout are significantly affected by the study's conclusions. Businesses may reap the benefits of improved recognition of fraud, happier customers, and better knowledge when it comes to fraud risks by integrating AI and ML models into their safeguarding systems. This is all thanks to less false positives that disturb the user experience. Nonetheless, AI and ML have the ability to revolutionise digital wallet fraud protection. Future research should focus on addressing the constraints identified in this work, namely with regard to model scalability, computing efficiency, and privacy issues. Additionally, the creation of standardised datasets for AI/ML application in fraud detection will be crucial to bolstering the robustness and generalisability of the models of other digital wallet systems.

References

1. Bagla, R. K., &Sancheti, V. (2018). Gaps in customer satisfaction with digital wallets: challenge for sustainability. Journal of Management Development, 37(6), 442-451.
2. Kumar, R., Mishra, V., &Saha, S. (2019). Digital financial services in India: An analysis of trends in digital payment. IJRAR, 6(2), 6-10.
3. Hassan, M. A., &Shukur, Z. (2019, September). Review of digital wallet requirements. In 2019 International Conference on Cybersecurity (ICoCSec) (pp. 43-48). IEEE.
4. Wang, S., Liu, C., Gao, X., Qu, H., & Xu, W. (2017). Session-based fraud detection in online e-commerce transactions using recurrent neural networks. In Machine Learningand Knowledge Discovery in Databases: European Conference, ECML PKDD 2017, Skopje, Macedonia, September 18–22, 2017, Proceedings, Part III 10 (pp. 241-252). Springer International Publishing.
5. Chang, V., Di Stefano, A., Sun, Z., &Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. Computers and Electrical Engineering, 100, 107734.
6. Alam, M. M., Awawdeh, A. E., & Muhamad, A. I. B. (2021). Using e-wallet for business process development: challenges and prospects in Malaysia. Business Process Management Journal, 27(4), 1142-1162.
7. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... &Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. Applied Sciences, 12(19), 9637.
8. Singla, J. (2020, June). A survey of deep learning based online transactions fraud detection systems. In 2020 International Conference on Intelligent Engineering and Management (ICIEM) (pp. 130-136). IEEE.
9. Bello, O. A., Folorunso, A., Ogundipe, A., Kazeem, O., Budale, A., Zainab, F., & Ejiofor, O. E. (2022). Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection. International Journal of Network and Communication Research, 7(1), 90-113.
10. Vivek Yadav. (2021). AI and Economics of Mental Health: Analyzing how AI can be used to improve the cost-effectiveness of mental health treatments and interventions. Journal of Scientific and Engineering Research, 8(7), 274–284. https://doi.org/10.5281/zenodo.13600238.
11. Mhlanga, D. (2020). Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion. International Journal of Financial Studies, 8(3), 45.
12. Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I., &Lozynska, O. (2020). Automatic machine learning algorithms for fraud detection in digital payment systems. ВосточноЕвропейскийжурналпередовыхтехнологий, 5(9-107), 14-26.
13. Yadav, V. (2019). Healthcare IT Innovations and Cost Savings: Explore How Recent Innovations in Healthcare IT Have led to Cost Savings and Economic Benefits within the Healthcare System. International Journal of Science and Research (IJSR), 8(12), 2070–2076. https://doi.org/10.21275/sr24731181300.
14. Ando, Y., Gomi, H., & Tanaka, H. (2016, October). Detecting fraudulent behavior using recurrent neural networks. In Computer Security Symposium (pp. 11-13).