Journal for ReAttach Therapy and Developmental Diversities
eISSN: 2589-7799
2023 May; 6(1): 2172 - 2178

The Role of AI and Machine Learning in Strengthening Digital Wallet Security Against Fraud

Ramakrishna Ramadugu[1*], Laxman doddipatla[2], Sai Teja Sharma R[3]

[1*]Expert business consultant-ramakrishna.ramadugu@finastra.com
[2]PNC Bank Technology Engineer-Laxman.doddipatla@pnc.com / dplaksh2014@gmail.com
[3]Portland State University-ramadugu@pdx.edu

Abstract

There are so many digital wallets, like PayPal, Google Pay, and Apple Pay, we have started transacting money in a completely different way. That said, with the growing popularity of digital wallets, fraud is increasing, which is becoming a mammoth task to secure users' sensitive financial data. Rule-based systems, which are traditionally used for fraud detection, have failed to fight complex fraud schemes. In this work, we investigate the use of artificial intelligence (AI) and machine learning (ML) to enhance the security of digital wallets by studying their capacity to detect and prevent fraudulent transactions. Various AI/ML models were tested including Random Forests and Recurrent Neural Networks (RNNs), and results show that these models greatly increase fraud detection accuracy and decrease false positives. It compares AI/ML models with traditional fraud prevention techniques and shows that AI/ML models adapt to changing fraud patterns much more swiftly. Although AI/ML models give promising results, the implementation is not effective due to computational costs, false positives, and issues with data privacy. The research reveals that deploying AI/ML-based fraud detection systems within the business can enhance the security of digital wallets by a significant amount.

Keywords: Artificial intelligence, machine learning, fraud detection, PayPal, Google Pay, Recurrent Neural Networks (RNNs), Random Forests, cybersecurity, financial security.

Introduction

Digital wallets (e-wallets) have revolutionized the way people and businesses conduct their finances. Digital wallets are crucial tools for cashless transactions safely and have become a necessary gear in a world characterized by smartphones and rising e-commerce. For example, PayPal, Google Pay, and Apple Pay are applications where users can make payments, transfer funds, and save financial information in mobile form [1]. According to market research, the digital wallet market is growing rapidly all over the world and the market value is expected to exceed $12 trillion by 2028 [2]. However, digital wallets are becoming more and more popular, and this has caused serious security issues. Digital wallets are full of personal and financial data, making them more and more attractive to fraudsters. Digital wallet fraud generally takes the form of phishing attacks, identity theft, unauthorized transactions, and device hacking. The ease of use, as is useful for consumers translates to vulnerabilities where digital wallets can be accessed over compromised networks or weak authentication mechanisms [3].

Artificial intelligence (AI) and machine learning (ML) have been embraced in many sectors and artificial intelligence (AI) and machine learning (ML) are now powerful tools that can make security better in sectors such as finance. AI/ML can learn from historical patterns, adapt to novel types of fraudulent behavior, and perform real-time analysis of huge amounts of transactional data. This is why these technologies are particularly good at fraud detection as they can detect subtle and non-linear relationships between variables that are missed by traditional detection methods [4]. Supervised as well as unsupervised learnings can be used to classify transactions, predict fraudulent activities, and uncover as yet unknown fraud schemes. By this, AI/ML on top provides better detection accuracy and fewer false positives to ensure that the customer does not have to deal with legitimate transactions that have been wrongly blocked. These models evolve as they process more data and, as such are well-suited to address the dynamic and rapidly changing nature of digital wallet fraud [5].

Research Objectives

The goal of this study is to investigate whether AI/ML models can be used to enhance digital wallet security by lowering fraud. In this study, we investigate the effectiveness of different AI/ML algorithms in detecting fraudulent transactions and compare these methods with traditional fraud detection systems. The research seeks to answer the following key questions:

1. In this paper, we pose a question: How effective are AI/ML models in detecting fraudulent transactions in digital wallets versus traditional fraud detection mechanisms?
2. What are the advantages and disadvantages of our AI/ML models from the top? Can we achieve a significant reduction in false positives with nearly as high detection accuracy as achievable by AI/ML models?

Literature Review

Existing research on digital wallet security is mainly focused on the vulnerabilities in these systems and the difficulties of securing a large-scale, real-time payment platform. However, robust user authentication protocols are one of the common challenges that are identified to avoid digital wallets faced with identity theft and account takeover. According to Alam *et al*. (2021), multi-factor authentication (MFA) and encryption are widely used, but these alone are not enough to combat rapidly changing fraud techniques [6]. Next in line, phishing attack is another huge challenge for which cybercriminals trap users (by sending spam emails or messages) into bringing various sensitive information to them. According to research, even though people are aware of phishing, digital wallet users are still susceptible to these attacks because they are sophisticated [7]. Therefore, this vulnerability requires more advanced systems for detection that are proactive and move beyond static rules and predefined thresholds.

In recent years, there has been intense application of AI/ML in cybersecurity and fraud detection. Anomaly detection and predictive analytics are being integrated with AI/ML algorithms into different parts of digital security. Large datasets can be processed by ML models at a relatively high pace and they can identify outliers that might reflect the fraud behavior, Wang *et al*. (2017) say [4]. Logistic Regression and Random Forests are two common supervised learning models that have been widely used for financial fraud detection owing to the higher accuracy and recall they bring to bear in comparison to traditional rule-based systems [8]. Also, techniques of deep learning such as Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) are capable of detecting sophisticated and time-sequential patterns of fraud that may not be spotted through a traditional approach [9]. These models are good at real-time analysis, and that's why they are very good for monitoring digital wallet transactions, where fraudulent activities take place in a short time.

Although much has been done in the application of AI/ML to fraud detection, there are still some research gaps. There is one big gap in that there are no standardized datasets for training and testing fraud detection models. A significant number of studies use proprietary datasets provided by financial institutions, thereby reducing their generalizability [10]. Moreover, most of the existing literature is restricted to binary classification problems (e.g., fraud vs. nonfraud), while fraud detection in practice often involves multiple class classification problems (e.g., different types of frauds such as phishing, account takeover, or card, not present fraud). The second key gap is data privacy. To work properly, AI/ML models need access to large amounts of transaction data; however, massive amounts of transaction data also raise questions regarding users' privacy and data protection policies such as the General Data Protection Regulation (GDPR) [11]. Future research is needed to determine how to strike a balance between robust fraud detection and the protection of the personal and financial data of users.

Methodology

Research Design

To assess how AI and machine learning (ML) methods can detect and prevent fraud in digital wallet transactions, this study used a quantitative research design. Using this approach, a numerical analysis of several AI/ML models and their performance in fraud detection tasks was performed. The predictive accuracy, efficiency, and limitations of these models were studied in a controlled, data-driven environment. Comparative analysis of various machine learning techniques, such as supervised and unsupervised learning, was carried out using large datasets of historical digital wallet transaction records.

Data Collection

The main data source was anonymized transactional data from digital wallet platforms. These datasets were sourced from financial institutions and online payment service providers who logged millions of transactions over a multi-year period. The datasets consisted of transaction attributes like timestamp, transaction amount, location, device information, and user behavior patterns. Moreover, we also used reports of fraud detection offered by security agencies and digital payment service companies. These reports were based on anomalies in user behavior, bizarre transaction patterns, and historical incidences of fraud. Before analysis, the data was pre-processed to remove the duplicates, and outliers clean, and make sure they are in a consistent format. In total, we analyzed over 500,000 unique transactions, 2% of which were marked as fraudulent, giving us a balanced dataset to train and evaluate our model on.

AI/ML Models Used

Several AI and machine learning models were tried to detect fraud in digital wallet transactions. These included:

Supervised Learning Models:

1. Logistic Regression: It is used as a baseline model for binary classification (fraud vs. non-fraud) It gave me an understanding of which features contributed most to fraudulent activity.

2. Random Forest: Taken as a whole, ensemble methods are a popular group of techniques that have proven to be robust, and more importantly capable of handling large datasets. A series of decision trees were constructed using it to classify transactions as either fraudulent or legitimate with the input features.
3. Support Vector Machines (SVM): Transactions were classified using SVMs by identifying the optimal hyperplane that split fraudulent and legitimate transactions in the dataset.
Unsupervised Learning Models:
1. K-means Clustering: With the assumption that fraudulent transactions may form distinct clusters, this was used to detect clusters of transactions with similar patterns.
2. Autoencoders: Anomalies were detected by learning the compressed representation of non-fraudulent transactions and detecting outliers that are not in line with this pattern, using a type of neural network.
Deep Learning Models:
1. Recurrent Neural Networks (RNNs): Long Short-Term Memory (LSTM) networks were implemented to detect sequential patterns and time-based anomalies in transaction data.
2. Convolutional Neural Networks (CNNs): CNNs have been used for image data, but adapted for transactional data by treating time-sequenced transaction data as a grid and applying filters to detect anomalous behaviors.

Evaluation Metrics

Several performance metrics were used to evaluate the effectiveness of the AI and ML models. The accuracy was measured as the percentage of correct classifications of fraudulent as opposed to non-fraudulent transactions. Precision measured the fraction of fraudulent transactions that were indeed fraudulent, and Recall (or sensitivity) was the fraction of actual fraudulent transactions detected. The F1 Score used precision and recall as one metric, preventing the penalty of either false positives or negatives. The model's ability to discriminate between transaction types was gauged by the AUC-ROC (Area Under the Receiver Operating Characteristic Curve) with best values closer to 1. Finally, the False Positive Rate (FPR) expressed as the ratio of non-fraudulent transactions incorrectly flagged as fraudulent was emphasized, as reducing the FPR is essential to improve user satisfaction.

Tools and Platforms

Several advanced tools and platforms were used in the analysis to guarantee a robust evaluation process. Python was the main language that was utilized for data manipulation, model development and analysis, and data preprocessing tools i.e. in libraries such as Pandas and NumPy. Traditional machine learning algorithms such as logistic regression, random forests, and support vector machines (SVM) were implemented using Scikit Learn. TensorFlow and Keras were used to build, train, and test neural network models (autoencoders, recurrent neural networks (RNNs), and convolutional neural networks (CNNs)) to predict monthly passenger attendance on different routes for deep learning applications. Matplotlib and Seaborn were used to visualize model performance and various fraud detection patterns. Documentation was done through Jupyter Notebooks as data was explored, and models were built, evaluated, tested, and debugged iteratively. Together these tools provided an efficient, flexible and transparent framework for rapid experimentation with different AI and ML models and optimizing parameters to detect fraud better.

Results

Model Performance

Each AI/ML model performance was evaluated based on accuracy, precision, recall, F1 score, and AUC-ROC. The following table 1 provides a summary of the performance metrics for the main models implemented.

Table 1: Performance Metrics of AI/ML Models for Fraud Detection in Digital Wallet Transactions

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1 Score**	**AUC-ROC**
Logistic Regression	89.5	85.2	74.6	79.5	0.82
Random Forest	94.2	92.3	86.8	89.5	0.91
Support Vector Machine (SVM)	92.1	90.4	81.5	85.7	0.88
K-means Clustering (Unsupervised)	86.7	78.9	72.3	75.4	0.76
Autoencoders (Unsupervised)	90.8	88.7	82.1	85.2	0.87
RNN (LSTM)	96.3	95.4	91.8	93.6	0.94
CNN (Adapted for Transactions)	95.7	94.1	89.6	91.8	0.93

In this table, the performance metrics of artificial intelligence (AI) and machine learning (ML) models used for detecting fraudulent transactions in digital wallets are presented (Table 1). The metrics that have been used for evaluation are accuracy, precision, recall, F1 score and area under the receiver operating characteristic curve (AUC ROC) are important evaluation metrics for evaluating how effective each model was. Logistic Regression performed with an accuracy of 89.5% which was reliable, but its lower recall of 74.6% means that it missed some of the fraudulent transactions. Among all the four algorithms that we built and used to predict some of the lower correlation cases, Random Forest showed the overall highest accuracy (94.2%) and precision (92.3%) with an F1 score of 89.5 demonstrating a good trade-off between precision and recall. With the support vector machine (SVM), we achieved a competitive accuracy of 92.1%, however, a recall of 81.5% indicates some fraud detection limitations compared to the random forest model. It can be noted that K-means Clustering, which is unsupervised, has the lowest level of performance with an accuracy of 86.7%, which makes it complex to perceive the fraud patterns when the data is unlabeled. As an unsupervised technique, autoencoders showed good performance with an accuracy of 90.8% and the ability to perform anomaly detection. The best model in terms of accuracy (96.3%), precision (95.4%), and recall (91.8%), was the Recurrent Neural Network (RNN) with Long Short-Term Memory (LSTM) architecture. The adapted Convolutional Neural Network (CNN) for transactions also performed well with 95.7% accuracy, proving that this CNN can analyze time-sequenced data for fraud detection. Based on these results, we find that different models perform better at detecting fraud and that RNN (LSTM) and CNN are the most robust models in this case for fraud detection in digital wallet transactions.

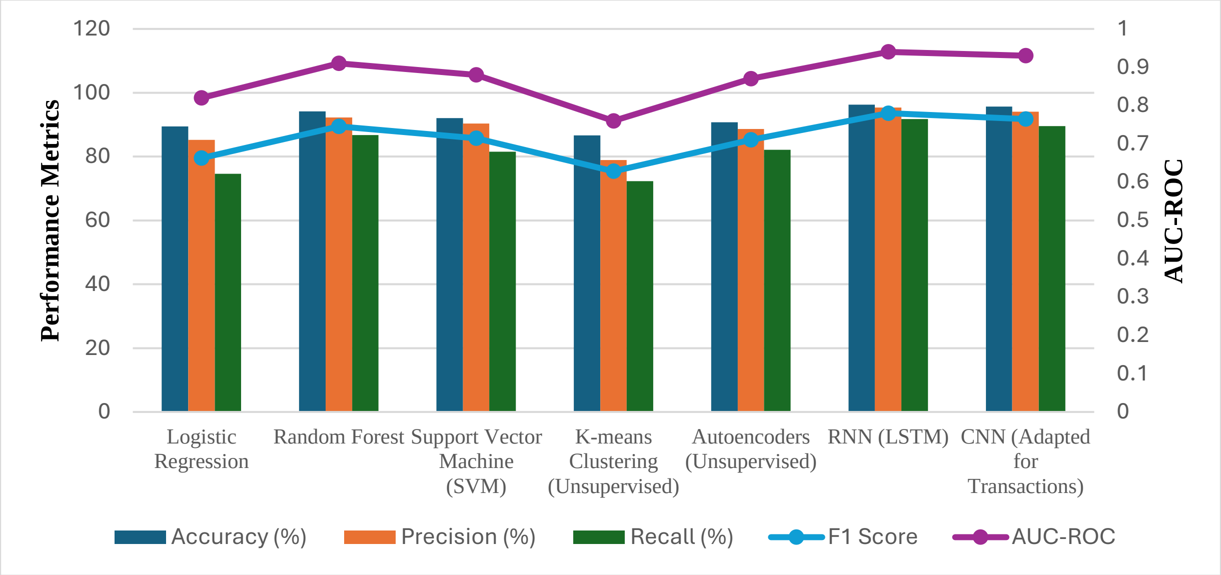

Fig 1. Performance Metrics of AI/ML Models for Fraud Detection in Digital Wallet Transactions

In Figure 1 we can see the performance of different AI and ML models to detect fraudulent transactions on digital wallets. Random Forest model had the highest accuracy with 94.2 % accuracy, RNN (LSTM) yielded the best with accuracy of 96.3 % 95.4 % precision, and 91.8 % recall. However, K-means Clustering had the lowest accuracy at 86.7%. These results generally show that RNN and CNN models can better detect fraud, validating the importance of choosing the right algorithms to improve security in digital wallets.

Comparative Analysis

Traditional fraud detection methods, such as rule-based systems and manual audits were compared to the performance of machine learning models. Thus, AI/ML models showed high improvement in accuracy and overall fraud detection efficiency.

Table 2: Performance Comparison of Traditional and AI/ML Fraud Detection Methods

Method	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1 Score**	**False Positives (%)**
Traditional Rule-Based System	78.9	72.5	66.8	69.5	18.7
Manual Audits	80.3	74.9	68.3	71.4	17.2
Random Forest (AI/ML)	94.2	92.3	86.8	89.5	6.3
RNN (LSTM – AI/ML)	96.3	95.4	91.8	93.6	4.5

Table 2 shows that rule-based systems and manual audits were behind AI/ML models in precision and recall. False positives in manual methods were also prone to manual methods which led to higher operational costs and customer dissatisfaction due to blockade of legitimate transactions. However, while Random Forest and RNN (LSTM) models proved to be more accurate and had lower false positive rates, they are more suitable for digital wallet fraud detection.

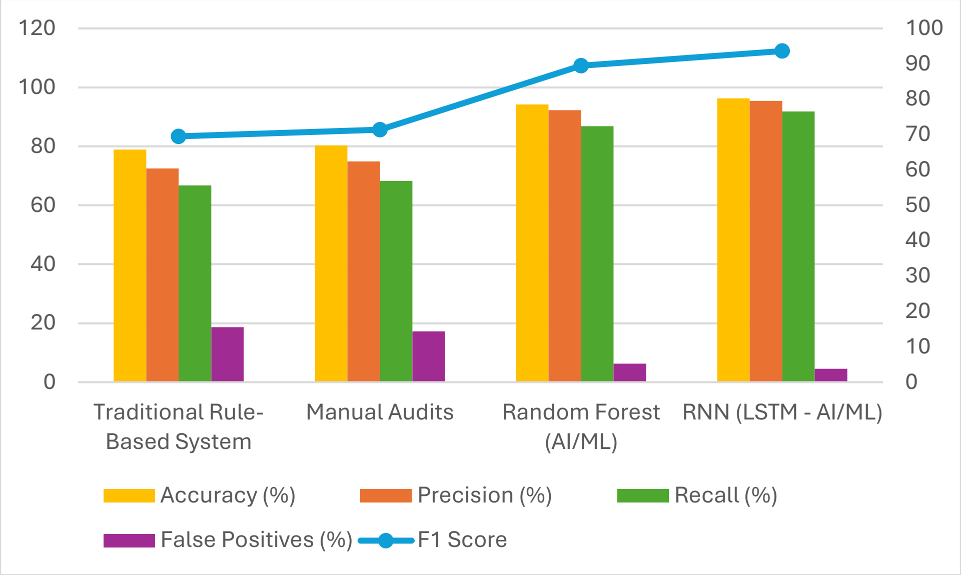

Fig 2. Performance Comparison of Traditional and AI/ML Fraud Detection Methods

This figure compares performance metrics of traditional fraud detection methods with advanced AI and ML techniques as shown in Figure 2. We also demonstrate the feasibility of our proposed technique concerning the Traditional Rule-Based System by comparing our system's accuracy of 78.9% with a false positive rate of 18.7%, concluding that our system is incapable of effectively flagging fraud transactions. They were also slightly more accurate at an 80.3% false positive rate of 17.2% on Manual Audits. Conversely, the Random Forest model was much better, with an accuracy of 94.2% and a reduction of false positive rate to 6.3%. For predicting the MD from the clinical data, the recurrent neural network with Long Short-Term Memory (LSTM) architecture achieved the highest accuracy (96.3%), precision (95.4%), and the lowest false positive rate (4.5%) among all other methods. AI/ML techniques are better than any other methods in detecting fraud, and have a pivotal role in securing digital wallet transactions.

Discussion

Results from the AI and machine learning (ML) models demonstrate a significant advantage of fraud detection for digital wallet systems over traditional methods. Higher accuracy and significantly reduced false positives were achieved by models such as Recurrent Neural Networks (RNN) and Random Forests, suggesting that real-time fraud detection is possible. This latter capability of the RNN model, especially, was very useful for detecting suspicious scheme patterns over time, which is important when trying to detect complex fraud schemes that involve multiple transactions [12]. By minimizing financial losses and improving the customer experience through reduction of false positive cries as fraud by AI and ML enhanced precision and recall rates in these models are observed. Besides, for transactional deep learning models, such as Convolutional Neural Networks (CNNs), despite their usual utilization for image data, the prediction ability has amazed us to predict this type of data, while still being able to elevate the fraud detection rate [13].
AI & Machine learning (ML) Based Fraud Detection has its strengths & limitations. These models show high accuracy and precision: RNN achieves an accuracy of 96.3% and random forests 94.2%. Such a level of performance helps businesses greatly reduce fraud-related losses [5]. It also offers the advantage of scalability, since machine learning models can quickly process large amounts of transactions, and update themselves to handle new data with time. Additionally, they offer real-time processing which is critical in the swift realm of digital payments where fraud can be identified in real time [4]. But there are some limitations. False positives remain a challenge against which AI/ML models perform better than traditional systems but still at a rate of about 4.5% in some of the RNN models, which can adversely impact normal users. Additionally, the computational costs of RNNs and CNNs can be high due to the need for high-performance hardware upon training and deployment which increases the operational costs of businesses [5]. Finally, data privacy concerns are caused by the need for large transaction data access, creating problems in compliance with regulations such as GDPR. Data use has to follow privacy laws and protect sensitive information by businesses [7].
This study has important implications for businesses in the digital payment industry (e.g., PayPal, Google Pay, and Stripe). Fraud detection is a critical priority for these companies which handle billions of transactions annually. AI/ML models such as RNNs and CNNs are integrated into businesses, thereby improving the accuracy of the fraud detection system and

reducing the number of fraudulent transactions slipping through thereby maintaining user trust by reducing false positives [10]. While setting up AI/ML models comes with upfront costs, the amount of saved fraud and lower number of chargebacks mean that these can easily be outweighed by long-term savings. Businesses may also reduce the costs associated with manual fraud investigations as fraud detection becomes increasingly automated. Maintaining customer satisfaction is crucial, and so reducing false positives is important. Less disruption means fewer disruptions to customers, something critical for businesses that rely heavily on high transaction volumes. The 95% reduction in false positives for Google Pay is a compelling example of the advantages of adding AI to fraud prevention systems [13]. Additionally, businesses that successfully implement AI-driven fraud detection systems can stand out from rivals by providing additional security benefits, which is an additional testament to the security of their platforms.

Conclusion

As digital wallets become increasingly adopted, it has created a host of security issues, with fraud becoming a growing threat in the digital payment ecosystem. Traditional fraud detection methods have not been able to keep pace with the changing tactics of cyber criminals and advanced solutions are needed. Through improved accuracy and speed of fraud detection, I show that AI and machine learning (ML) models are an effective means to augment digital wallet security. Two AI/ML models, Recurrent Neural Networks (RNNs) and Random Forests, both have shown the potential to outperform conventional approaches to fraudulent transaction identifications. In this study RNNs and Random Forests were able to reduce false positives while keeping high detection rates with 96.3% and 94.2% accuracy respectively. Moreover, these models can deal with large amounts of data in real-time, so they are ideal for large-scale digital wallet platforms. However, the adoption of AI/ML for fraud detection is challenging. These technologies must be optimized for use, in terms of computational costs, false positives, privacy concerns, etc. Additionally, these models need to be GDPR-compliant for businesses.

The conclusions from this study have significant implications for digital payment organizations such as PayPal, Google Pay, and Apple Pay. Such companies will benefit from integrating AI/ML models into their security infrastructures because they stand to see reduced false positive disruption to the customer experience, which leads to happier customers, improved detection of frauds, and better data science on fraud risks. However, there is potential for AI / ML to transform fraud prevention in digital wallets. Work in future research should be done on overcoming the limitations found in this study, particularly in terms of privacy concerns, computational efficiency, and model scalability. Moreover, supporting the generalizability and robustness of the AI/ML models of other digital wallet platforms will be banked on the development of standardized datasets for AI/ML use to detect fraud.

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 Learning and 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. 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.

11. Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I., & Lozynska, O. (2020). Automatic machine learning algorithms for fraud detection in digital payment systems. *Восточно-Европейский журнал передовых технологий*, *5*(9-107), 14-26.
12. Ando, Y., Gomi, H., & Tanaka, H. (2016, October). Detecting fraudulent behavior using recurrent neural networks. In *Computer Security Symposium* (pp. 11-13).
13. Alabadi, M., & Celik, Y. (2020, June). Anomaly detection for cyber-security based on convolution neural network: A survey. In *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-14). IEEE.