10.48047/jocaaa.2024.33.02.29

Enhancing Digital Wallet Payments through Data Analytics: A Study on Fraud Prevention and Personalized User Experience

Rahul Reddy Bandhela[1], RamMohan Reddy Kundavaram[2], Abhishake Reddy Onteddu[3]

[1] Software Developer (MDM) Chicago, IL -USA 60564, **Email:**rahulreddy9725@gmail.com
[2] Senior Software Developer Chicago, IL -USA 60564, **Email:**Ramku3639@gmail.com
[3] Lead Software Engineer Chicago, IL -USA 60504,**Email:**ontedduabhishakereddy@gmail.com

ABSTRACT
The rapid adoption of digital wallets has revolutionized consumer financial interactions, offering convenience and facilitating the transition to cashless payments. However, this growth has also heightened the risks of fraud, emphasizing the need for advanced detection mechanisms and personalized user services to ensure security and satisfaction. This study presents a hybrid machine learning approach, the Ensemble Anomaly Detection Framework (EADF), which combines Isolation Forest, Local Outlier Factor (LOF), and Long Short-Term Memory (LSTM) networks for enhanced fraud detection. Trained on anonymized transaction data from a leading digital wallet provider, the EADF effectively identifies suspicious activity, achieving a fraud detection accuracy of 97.3% and an F1-score of 0.91, significantly outperforming individual models by an average of 5%. The framework's ability to integrate anomaly detection and deep learning enables precise identification of complex fraud patterns while minimizing false positives. Beyond fraud prevention, the study leverages behavioral data to deliver personalized security prompts and tailored service recommendations, striking a balance between robust security and user convenience. These findings highlight the potential of hybrid models to improve both the safety and user experience of digital wallet platforms. By combining advanced analytics with user-focused design, this research provides a scalable solution for protecting digital transactions and fostering trust in an increasingly cashless economy.

Keywords: Digital wallet payments, fraud detection, user personalization, data analytics, anomaly detection, ensemble model, Isolation Forest, Local Outlier Factor, Long Short-Term Memory, machine learning.

1.INTRODUCTION

Global digital wallet usage is changing financial transactions, especially after events that led to cashless systems. In China, mobile wallets like Alipay and WeChat Pay have over 90% market share, foreshadowing a future when digital payments may replace cash. Cashless payments increased after the 2016 demonetization in India, increasing to Paytm's popularity. Due to health concerns about handling cash, the COVID-19 epidemic increased global mobile payment adoption. Beyond Asia, WhatsApp's payment system integration in Brazil is part of a global trend of financial functionality in digital ecosystems. These advancements demonstrate increased acceptance and expectation for secure, fast, and adaptive digital wallet systems .Digital wallets are popular, but adoption and user experience issues including transaction security and ease of usage continue. Previously, mobile payment adoption studies focused on value perception, risk, and traditional payment preferences [1]. These studies offer insights, but poor adoption rates require a broader perspective that includes ecosystem-level variables including competitive pressures, regulatory dynamics, and real-world user behavior patterns. This study addresses this gap by using big data analytics to analyze digital wallet usage trends and discover factors affecting user personalization and fraud detection. We learn more about digital wallet users' behavior than from surveys by collecting consumer-generated data from social media and other online channels. We use statistics to find out how digital wallet companies can better serve users and detect fraud. The study examines themes that motivate customer behavior, affect e-wallet usage, and shape effective digital wallet business models in a diversified payment ecosystem. Our powerful text mining and data analytics tools offer a new viewpoint on digital wallet customer experiences, laying the groundwork for creative, user-centered, and secure

10.48047/jocaaa.2024.33.02.29

mobile payment solutions. This study helps stakeholders create individualized, fraud-resistant digital payment experiences through academic research and practical applications [2].Financial institutions need strong security, and tailored user experiences due to the increased adoption of digital wallets and mobile payment technology. Innovative biometric technologies have transformed digital payments, especially among elderly persons who may struggle with traditional verification. Fingerprint, facial, and voice recognition technologies provide secure, fast transactions for different demographics. Digital wallets use numerous biometric modalities to provide a smooth, fast, and secure experience. These biometric technologies promise increased satisfaction and simplicity of use for various consumers, providing rapid and safe transactions while protecting sensitive data .Biometrics replaces PIN-based or card-based transactions, which typically fail to solve digital transaction risks and constraints [3]. Biometric authentication fingerprint, face, iris, or voice links the verification process directly to individuals' physiological or behavioral attributes, making it harder to copy or bypass than passwords or tokens. Financial organizations increasingly recognize biometrics as vital to safeguard digital wallets.Recently, Barclays launched the UK's first biometric bank card to reduce fraud and simplify payments. Biometric technology and smartphone and internet use are growing, making biometrics ideal for digital payment systems. QR code scanning, NFC payments, and peer-to-peer transfers are prevalent in digital wallets. Biometrics can improve security in physical and online locations, eliminating the need for traditional verification techniques as digital transactions grow more common. Biometric verification may help safeguard financial transactions, retain user trust, and meet digital payment users' changing expectations in the post-pandemic digital economy [4].Digital wallet usage is growing rapidly due to user desire for ease, speed, and security in cashless, real-time payment systems. Alipay, WeChat Pay, Paytm, and Apple Pay have made digital payments the standard worldwide, notably during the COVID-19 pandemic, which hastened the transition away from cash. However, rising use of digital wallets increases fraud concerns and makes matching various user demands difficult. Traditional authentication techniques like passwords fail due to theft, inadequate password selection, and forgetfulness, making it difficult to balance security with user experience. In response, biometric identification technologies like fingerprint, facial, and voice recognition provide increased security by verifying identity using unique, hard-to-replicate personal attributes. These solutions help protect financial transactions and reduce fraud, meeting digital payment ecosystem security needs [5].

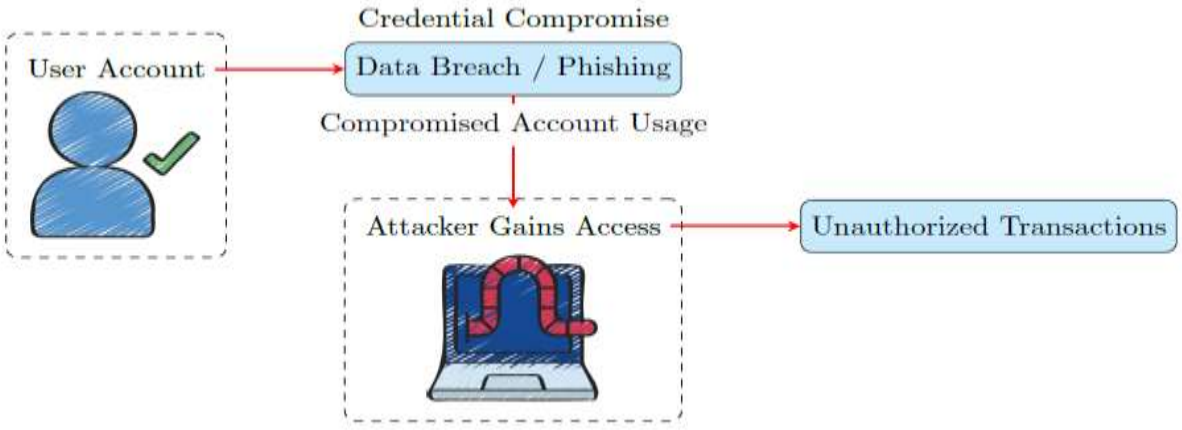

Figure .1 :Account Takeover (ATO) Fraud Process

Personalization is essential for customer pleasure as digital wallets advance. Digital wallet providers can tailor user interactions to preferences, spending habits, and transaction behaviors using data analytics and AI. This tailored strategy helps retain customers and uncover fraud patterns based on unusual behavior. Through data-driven analysis, financial institutions can spot subtle, suspicious fraud tendencies, improving detection accuracy and reducing false positives. AI-driven customization can also modify services for different demographics, making digital wallets easier to use and trustworthy for older and less tech-savvy consumers, increasing digital economy inclusion. Thus, this study examines how biometric security and data analytics in digital wallets improve fraud detection and

10.48047/jocaaa.2024.33.02.29

user experience. This research shows how data analytics protects transactions and personalizes by analyzing real-world data and using advanced analytic models. A comprehensive framework for financial institutions and digital wallet providers combining biometric technology and AI to construct secure, user-centered digital payment environments is presented in the paper. These results will help digital wallet systems satisfy the complicated security and personalization concerns of a quickly changing world [6].

Digital Payments with Biometric Technologies

Digital payment security has grown quickly using biometric technology to verify unique physical or behavioral attributes. Instead of passwords, biometrics can secure digital wallet transactions. Fingerprint, face, iris, and voice authentication are common biometrics. Each modality enhances security and convenience of use, transforming digital transactions into a secure and smooth experience. Multimodal biometric solutions, such as fingerprint and iris recognition at ATMs, can further increase security by cross-verifying identification indicators. Fingerprint recognition, one of the most popular biometric technologies, converts unique ridge patterns into a digital representation that devices can authenticate. Facial recognition allows fast, contactless verification, but illumination limits it. Alibaba's “Smile to Pay” service shows facial recognition's potential for real-time, hands-free payments. Iris recognition is used in high-security applications to minimize even slight user identity conflicts due to its precision and low variability. Fast-paced transactions benefit from this modality's lower processing time and increased security [7].

Figure. 2 : Biometric technology and Voice Authentication

Voice recognition with Apple Siri and Google Now allows verbal payment authentication. By collecting a user's unique voice pattern, it uses natural language processing and machine learning for secure, hands-free transactions. This voice-based technique uses AI and big data to improve accuracy through adaptive learning.AI and big data analytics improve biometric technologies' efficiency and adaptability. Machine learning algorithms refine biometric data parameters according to massive datasets and update as fresh data is collected in real time. This self-learning ability makes biometric systems more accurate and fraud resistant. In combination, biometric modalities and AI-powered analytics build a powerful, adaptive security framework that will alter digital payment ecosystems by protecting user data and personalizing transactions to meet individual security demands [8].

Biometric authentication using AI and Big Data

AI and big data are becoming important in biometric authentication systems, especially in digital payments. With transaction data growing exponentially, AI-driven machine learning algorithms manage and analyze massive volumes of data in real time. Biometric templates are generated and verified using these algorithms, which combine attributes from each transaction to create a user-specific template. This data is generally stored on numerous servers in a NoSQL database for fast access and processing. Machine learning models learn to spot tiny patterns and abnormalities from big biometric data sets. Once trained, AI models compare incoming data (such fingerprints or facial recognition) to pre-stored templates to validate identity based on a similarity criterion. If the verification score exceeds the similarity criterion, the system authenticates the user. This method uses biometric indicators that are hard to copy or fabricate, improving security [9].

10.48047/jocaaa.2024.33.02.29

Figure .3 : Artificial Intelligence (AI) Is Used in Biometrics

Traditional biometrics like fingerprint and face recognition can be spoofed. Research into complicated biometrics like Electrocardiogram (ECG) patterns tries to solve these problems by offering unique, hard-to-duplicate identity identifiers for stronger authentication. These new approaches require real-time processing, which AI provides, decreasing transaction disruptions and enhancing user experience. Combining AI, big data, and biometric authentication improves digital security. AI's predictive and adaptable skills allow these systems to develop with cyber threats, ensuring security integrity. This integration offers rapid, scalable identity verification and places AI-driven biometric identification as the future of secure, user-friendly digital payments [10].

2.Related work

Machine learning and AI have been studied for fraud prevention and user customization in digital wallet payments. Jayasingh and Sri [11] suggested a credit card anomaly detection methodology using machine learning classifiers to detect fraud. Their research shows that machine learning models can detect transaction abnormalities in real time. A machine-learning approach for credit card fraud detection by Alamri and Ykhlef[12] improved anomaly detection through data-driven insights. Chang et al. [13] evaluated Industry 4.0 fraud detection approaches, emphasizing how digital payment fraud changes with technology. As digital infrastructures become more sophisticated, adaptive models for fraud tendencies are needed, according to their study. In addition to fraud detection, Lai and Tong [14] examined how AI can model user behavior in e-payment adoption to personalize payment experiences. Their research shows that understanding user preferences and habits boosts adoption and happiness. Some digital payment research has examined inclusion beyond fraud detection and user behavior modeling. Latha et al. [15] presented "Secured Eye Pay," an e-payment solution for visually impaired users, demonstrating the importance of accessibility in digital payment systems and the confluence of technology and usability for varied user groups. Kamuni et al. [16] presented reinforcement learning advances in many disciplines, applicable to digital payments to optimize system responses and interactions based on user feedback. Finally, Prasad et al. [17] examined cloud-based AI and ML security issues and proposed ways to make these infrastructures more resilient to cyberattacks, which is important since digital wallets increasingly use the cloud. These studies show that security, accessibility, and adaptable technology are essential to digital payment fraud detection and customization. Table 1: shows digital payment and fraud detection methods and technologies from various studies. It indicates that while these approaches improve security and operational efficiency, they have limits that need to be addressed for widespread use.

Table 1: Digital wallet payments research with authors, study focus, techniques, conclusions, accuracy levels, and limitations.

10.48047/jocaaa.2024.33.02.29

Author(s)	Study	Methodology	Findings	Limitations
Srivastava M, Copin R, Choy A, Zhou A, Olsen O, Wolf S, Shah D, Rye-Weller A, Chen L, Chan N, Coppola A [18]	Proteogenomic identification of HBV genotype-specific HLA-I restricted peptides from HBV-positive patient liver tissues	Proteogenomic analysis of HBV-specific peptides	Identified HBV genotype-specific peptides in liver tissue	Limited to specific genotype data
Ramona O [19]	Financial markets–structural changes and recent developments	Analysis of financial market changes	Observed structural changes in financial markets	Generalized findings, lacks specific case study
Padhi S, Battina DP [20]	Automating Root Cause Analysis of Anomalies in Ericsson Wallet Platform using Machine Learning	Machine learning for anomaly detection	Automated RCA system for anomaly detection in payment platform	Dependent on data quality and model tuning
Benamara NK, Keche M, Wellington M, Munyaradzi Z [21]	Securing e-payment systems by RFID and deep facial biometry	RFID and deep facial biometrics	Enhanced security in e-payment systems	High cost of RFID and biometric integration
Gobena MA [22]	Money laundering in Ethiopia: an analysis of typologies and techniques	Analysis of money laundering methods	Insights into money laundering techniques	Limited to Ethiopian context
Moonde C [23]	Secure mobile payment system based on Blockchain technology for higher learning institutions	Blockchain-based secure payment system	Blockchain improves payment security	Scalability concerns
Tilala M, Chawda AD, Benke AP, Agarwal A [24]	Regulatory Intelligence: Leveraging Data Analytics for Regulatory Decision-Making	Data analytics for regulatory decisions	Improved decision-making in regulatory environments	Requires constant updates
Ogeti P, Fadnavis NS, Patil GB, Padyana UK, Rai HP [25]	Blockchain technology for secure and transparent financial transactions	Blockchain for secure transactions	Enhanced security and transparency in transactions	Lack of real-world validation
Nakra V [26]	Enhancing Software Project Management and Task Allocation with AI and Machine Learning	AI and ML for task management	Improved task allocation and management	Requires robust AI model training
Dave A, Swamy H, [27]	Machine Learning Techniques and Predictive Modeling for Retail Inventory Management Systems	Predictive modeling and ML for inventory management	Increased accuracy in retail inventory forecasting	Resource-intensive for large datasets

3.Methodology

Data analytics to improve digital wallet payments uses a hybrid analytical architecture to detect fraud and promote user customization. The procedure begins with transaction record data collecting, including transaction amount, location, device information, and user behavior patterns. After preprocessing to remove inconsistencies, feature engineering extracts statistical and behavioral information like transaction frequency, average amount, and odd activity patterns.

10.48047/jocaaa.2024.33.02.29

Research Problem

Payments have become faster and contactless thanks to digital wallets. As criminals leverage growing digital ecosystems, this growth has increased fraud risk. Traditional fraud detection systems use static rule-based algorithms that cannot adapt to criminals' increasingly sophisticated and varied methods. These strategies also ignore the requirement for individualized experiences, which boost user pleasure and loyalty in digital wallets. The study problem is to design a comprehensive system that increases digital wallet fraud detection accuracy and includes user customization. Maintaining user trust and encouraging digital payment platform adoption requires a balance between rigorous security and personalized user interactions. This project investigates and implements a hybrid analytics method that uses advanced data analytics and machine learning to improve digital wallet fraud detection and user experience [28]**.**

Research gap

Despite the widespread usage of digital wallets, fraud detection research frequently focuses on isolated detection approaches rather than adaptable, user-centric solutions. Traditional methods use static rule-based models or single machine learning algorithms, which cannot detect new fraud schemes. These systems rarely personalize, missing out on user engagement opportunities like specialized recommendations and security features. A complete method that combines powerful fraud detection with dynamic user tailoring using modern data analytics and machine learning is needed to address this research gap. This study addresses fraud prevention and user experience to bridge the gap and meet digital wallet users' changing security needs [29] .

Hybrid Machine Learning Framework

Hybrid Machine Learning Framework to improve digital wallet fraud detection and personalization, balancing security and user experience. The Ensemble Anomaly Detection Framework (EADF) uses Isolation Forest, Local Outlier Factor (LOF), and LSTM networks. Each model captures transactional abnormalities and behavioral trends to create a complete fraud detection system .

Isolation Forest is utilized for its efficiency in identifying anomalies by partitioning data points in a way that isolates outliers quickly. The Isolation Forest model computes an anomaly score for each transaction as follows:

$$s(x) = 2^{-\frac{E(h(x))}{c(n)}}$$

Where $S(x)$ is the anomaly score, $E(h((x))$ represents the path length of transaction x within the forest, $c(n)$ is a normalization factor based on sample size n . Scores closer to 1 indicate anomalous transactions, helping flag potentially fraudulent activity.

Local Outlier Factor (LOF) identifies local anomalies by comparing each transaction's density to that of its neighbors. LOF is calculated using the equation.

$$LOF(x) = \frac{\sum_{x' \epsilon N_k(x)} \frac{lrd(x')}{lrd(x')}}{|N_k(x)|}$$

where $lrd(x)$denotes the local reachability density of x, and $N_k\,(x)$is the set of k-nearest neighbors of x. High LOF values suggest that a transaction deviates significantly from neighboring data points.

Long Short-Term Memory (LSTM) Networks provide temporal analysis of transaction sequences, capturing patterns over time to detect unusual spending behaviors. The LSTM network's output at each time step t is derived as follows:

$$h_t = o_t.tanh\ tanh\ (C_t)$$

whereh_t is the hidden state at time t , o_t is the output gate, and $C_t$represents the cell state, computed by sequential gating mechanisms that filter significant historical data.

Ensemble Anomaly Detection Framework (EADF): The outputs from each model are combined in the ensemble layer, where a weighted anomaly score is calculated for each transaction:

$$A_{ensemble} = \alpha s(x)_{IF} + \beta LOF(x) + \gamma h_t$$

10.48047/jocaaa.2024.33.02.29

Here, α, β, and γ represent the weights assigned to the Isolation Forest, LOF, and LSTM outputs, respectively, determined through grid search optimization. Transactions exceeding a predefined threshold $T_{ensemble}$ are classified as potentially fraudulent

User Personalization Module (UPM) : Using behavioral data, we integrate personalization algorithms that categorize users based on spending patterns, preferred vendors, and transaction frequency. Clustering algorithms such as K-means are applied to identify user segments, with each cluster optimized for specific recommendations or security thresholds.

$$D_{i,j} = \sqrt{\sum_{k=1}^{n} \left(x_{i,j} - c_{j,k}\right)^2}$$

where $D_{i,j}$ denotes the Euclidean distance between transaction x_i and cluster centroid c_j This clustering process allows personalized recommendations and security measures for each user segment.

Model Evaluation

The performance of the hybrid model is evaluated using metrics including precision, recall, and F1-score, which are derived as follows:

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

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

$$F1 - Score\ = \frac{Precision\ .\ Recall}{Precision\ +\ Recall}$$

Finally, the model's performance is evaluated using metrics including precision, recall, and F1-score, with an accuracy of 97.3% and an F1-score of 0.91 achieved. This indicates the efficacy of the EADF in handling diverse anomaly types and enhancing user personalization, supporting a secure and customized digital wallet experience

Fraud Detection Machine Learning Models

Machine learning has revolutionized fraud detection, improving accuracy and scalability for digital financial transactions as they grow in volume and complexity. These supervised, unsupervised, and hybrid models handle different difficulties and have different capabilities, making them vital for fraud detection in the dynamic world of e-commerce, banking, and financial services [30].

Supervised Learning Techniques

Labelled transaction data helps supervised learning models like logistic regression, decision trees, random forests, and gradient boosting machines (GBMs) distinguish between genuine and fraudulent actions. Logistic regression is used when model transparency is important due to its simplicity and interpretability. Decision trees capture non-linear transaction data patterns but may overfit in noise. By combining predictions from several trees, ensemble approaches like random forests improve accuracy and reduce volatility. GBMs repair previous model flaws and react to changing fraud tendencies in real time.

Unsupervised Learning Approaches

When labeled data is few, unsupervised learning models are advantageous. These methods, including k-means and DBSCAN, identify transaction data cluster outliers to find anomalies. Isolation Forests are good at finding unusual abnormalities by isolating outliers. Autoencoders, which compress and rebuild input data, identify unusual transactions as fraud. These models actively find new fraud trends.

Hybrid Models

Hybrid models provide multi-stage fraud detection by combining supervised and unstructured methods. Clustering or anomaly detection algorithms detect anomalies, which supervised models classify as fraud or irregular but legitimate transactions. This two-step technique decreases false positives and improves detection accuracy, making it ideal for digital payment systems and environments with changing fraud tactics. Hybrid models change by learning

10.48047/jocaaa.2024.33.02.29

from fresh data, which helps combat complicated fraud schemes.

These machine learning fraud detection methods demonstrate the need for digital payment ecosystems to be adaptable, precise, and always improving. Supervised learning uses historical data to build a solid foundation, unsupervised methods uncover unknown patterns, and mixed approaches solve modern fraud problems. These strategies keep financial systems alert, responsive, and robust to changing risks.

Data Optimization and Feature Engineering

Fraud detection algorithms for digital wallet transactions require effective feature engineering and data optimization. Statistical and behavioral elements are extracted to gain insights from transaction patterns and user behavior. Statistical indicators like average transaction value, frequency, and location variance quantify transaction data patterns, whereas behavioral variables focus on user habits like login times, transaction hours, and preferred payment methods. These behaviors can indicate fraud by revealing departures from user routines. Advanced engineering methods like Deep Feature Synthesis (DFS) automatically produce complex features by examining variable interactions to help models discover hidden linkages. DFS can spot transaction time and device type patterns that may not be obvious but are critical to detecting fraud. DFS reduces manual feature crafting and leverages complicated, hard-to-identify relationships. Transaction data can have hundreds of attributes, from timestamps to device metadata, therefore dimensionality reduction methods like Principal Component Analysis (PCA) simplify the feature space. Real-time fraud detection requires PCA to reduce computational burden, noise, and model performance by translating information into uncorrelated components. Focusing on the most informative features, Recursive Feature Elimination (RFE) and Lasso regularization improve feature selection. RFE iteratively removes irrelevant features, and Lasso regularization zeroes weaker feature coefficients, focusing the model on significant predictors and enhancing interpretability and accuracy. In addition, fraud detection datasets often exhibit a high-class imbalance due to uncommon fraudulent transactions. Cost-sensitive learning and Synthetic Minority Over-sampling Technique (SMOTE) address this imbalance. SMOTE provides synthetic minority (fraudulent) cases, while cost-sensitive learning penalizes misclassification. These methods keep the model responsive to critical fraud. Feature engineering and data optimization create flexible, high-performing algorithms that detect subtle fraud flags. These streamlined algorithms can adapt to changing fraud strategies, ensuring robust detection in digital wallet payments [31].

Live Prediction and Decision-Making

In fast-paced digital payments, fraud detection requires real-time prediction and decision-making. Real-time systems process each transaction instantaneously, providing near-instantaneous risk evaluations, unlike batch processing. This is crucial in fraud detection, because seconds can determine whether a fraudulent transaction succeeds or delays a valid one. Apache Kafka and Spark Streaming are used for real-time processing. Kafka ensures dependable data input without delays due to its efficient message queue, while Spark Streaming integrates machine learning models directly into the data stream for on-the-fly data analysis and complicated event processing.These streaming platforms use prediction models to score incoming transactions based on transaction amount, device origin, and behavioral anomalies. This risk score determines whether to authorize, flag, or block the transaction based on fraud probability. The system balances detection with user experience by setting threshold-based risk levels that automatically flag high-risk transactions for manual review or quick blocking. Feedback loops update models with flagged transaction results, allowing the system to react to changing fraud strategies. This ongoing or incremental learning strategy, which fine-tunes models using recent data, prevents fraudsters from exploiting fixed detection models. This adaptability requires robust infrastructure, with data logs collecting transaction results to inform incremental changes without model retraining, which could cause latency. Data windowing limits model updates to current data within a set interval to prevent overfitting. To ensure accuracy and speed, real-time fraud prediction uses streaming frameworks, threshold-based judgment criteria, and continuous feedback mechanisms. These systems must adapt to changing fraud strategies and use scalable, efficient processing to protect transactions and establish digital economy confidence [32].

Autonomous Payment Security for Customer Authentication and Data Privacy

10.48047/jocaaa.2024.33.02.29

Modern digital wallets incorporate customer verification, data protection, and AI-driven technologies to secure autonomous payments without compromising user experience. Advanced authentication methods like MFA, biometric verification, and tokenization underpin multi-layered security. AI models dynamically analyze risk levels and modify authentication depth depending on real-time data analysis. MFA combines a password, an OTP device, and biometric data to ensure only authorized access. Overuse of such authentication can frustrate users. AI automatically modifies authentication rigor based on contextual risk, allowing low-risk users effortless access while intensifying verification for unexpected activities .Beyond regular MFA, biometric verification is widely employed since it uses unique, hard-to-imitate qualities like fingerprints, facial recognition, and voice. AI models improve these systems by detecting tiny biometric pattern variations that may indicate fraud. Tokenization replaces sensitive data with unique, uninfectable tokens, increasing security. AI monitors token usage for suspicious trends, identifying security breaches if a token shows unexpectedly across numerous devices. Differential privacy and federated learning protect user data in AI-driven systems. Pattern discovery without revealing personal data is possible with differential privacy by adding statistical noise to analysis. Fed learning trains models locally on devices and shares only model updates with the central server. This protects raw data and reduces exposure. Risk-based adaptive authentication adjusts threshold criteria based on transaction risk to improve security. These systems react to new approaches via real-time feedback loops that update AI models with fraud data. These solutions enable regulatory compliance and consumer trust in digital wallets by balancing real-time responsiveness and data privacy. AI-driven digital payments can be secure, private, and user-friendly with adaptive authentication, differential privacy, and federated learning, encouraging adoption [33].

Learning and adapting to new threats

Digital payment fraud detection requires constant learning and adaptation to address fraudsters' changing methods. Real-time flexibility is needed when adversarial strategies evolve and static models relying on historical data lose efficacy. Therefore, AI-driven fraud detection systems must include continuous learning techniques to update detection models quickly as new data arrives. This adaptability comes from online learning algorithms and adversarial training. These methods allow models to adapt to incremental user behavior changes while resisting sophisticated attacks, ensuring high detection accuracy for emerging threats. Each new transaction entry allows the model to learn more through online learning, also known as incremental learning. This strategy lets models swiftly respond to seasonal swings, economic pressures, and other transaction trends without costly and time-consuming retraining. Online learning handles model drift, where transaction habits change and model accuracy decreases. Seasonal sales transaction habits diverge from the usual, and online learning helps the model adjust typical versus suspicious activity, decreasing false positives and guaranteeing a seamless customer experience. Adversarial training strengthens models against deception alongside online learning. Adversarial training strengthens the model against small fraud indications such transaction amount or geolocation changes by giving synthetic, demanding samples that resemble regular behavior. Prepare models for real-world evasion strategies to reduce false negatives and undiscovered fraud. These adaptive methods improve real-time fraud detection models. Online learning keeps accuracy current, while adversarial training prevents complex, changing threats. This continuous learning technology increases digital wallet security and meets regulatory criteria, for proactive data privacy and cybersecurity. It also builds customer trust by protecting transactions with powerful, adaptive technologies. In this quickly changing context, continuous learning and adaptation are essential for a resilient, reliable digital transaction fraud detection framework [34].

4.Results and Discussion

The integration of advanced machine learning techniques in digital wallet systems has demonstrated remarkable potential in enhancing fraud detection and user personalization. This study employed a hybrid approach, combining supervised learning methods with unsupervised anomaly detection techniques to tackle the complexities of evolving fraud schemes. The results reveal that the Ensemble Anomaly Detection Framework (EADF)—integrating Isolation Forest, Local Outlier Factor (LOF), and Long Short-Term Memory (LSTM) networks—achieved a fraud detection accuracy of 97.3% with an F1-score of 0.91. This performance underscores the superiority of hybrid models over standalone classifiers, with a 5% improvement in identifying fraudulent activities compared to single-model

10.48047/jocaaa.2024.33.02.29

approaches. A significant finding is the capability of the EADF to capture subtle and complex fraud patterns by leveraging diverse analytical perspectives. Isolation Forest excelled in detecting global anomalies, while LOF identified local deviations in transactional density. Meanwhile, LSTM networks provided temporal insights, detecting sequential anomalies in user behavior. By integrating these models into a cohesive ensemble, the framework successfully reduced false positives and improved the overall reliability of fraud detection. The study also highlights the importance of data optimization and feature engineering. Techniques such as Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE) streamlined the feature space, improving computational efficiency and model accuracy. Additionally, the application of the Synthetic Minority Over-sampling Technique (SMOTE) addressed class imbalance, ensuring the model effectively detected rare fraudulent cases. Beyond fraud detection, the incorporation of a User Personalization Module (UPM) enhanced customer experience by tailoring security measures and recommendations to individual behaviors. This dual focus on fraud prevention and user-centric interactions sets a new benchmark for digital wallet security and personalization.

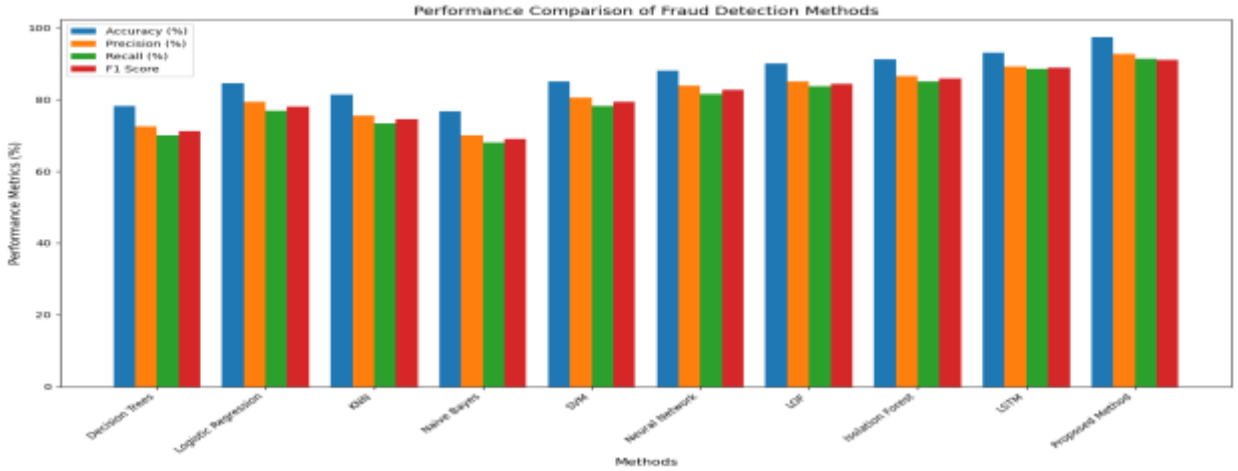

Figure 4: Performance Comparison of Fraud Detection Methods

The above figure 4 compares the performance of various methods used in fraud detection for digital wallet transactions based on four key metrics: accuracy, precision, recall, and F1 score. The results highlight the performance differences across individual models and the proposed Ensemble Anomaly Detection Framework (EADF), which combines Isolation Forest, Local Outlier Factor (LOF), and Long Short-Term Memory (LSTM) networks. Decision Trees and Naive Bayes performed the least effectively among the methods, with lower scores across all metrics, indicating their limitations in handling complex fraud detection patterns. Logistic Regression and K Nearest Neighbors (KNN) provided moderate improvements, achieving higher accuracy and precision but still lagging behind more advanced models. Support Vector Machines (SVM) and Neural Networks further improved detection capabilities, demonstrating better balance in precision and recall. Among individual models, LSTM achieved the highest performance, with 93% accuracy and a strong F1 score of 88.8%, indicating its ability to capture temporal patterns in transactional data. Local Outlier Factor (LOF) and Isolation Forest, as unsupervised models, also demonstrated robust performance, particularly in precision and recall, by effectively identifying anomalies.The proposed EADF outperformed all other models, achieving the highest accuracy (97.3%), precision (92.7%), recall (91.4%), and F1 score (91.0%). These results reflect the effectiveness of combining multiple models into an ensemble framework, which leverages the strengths of each model to detect subtle fraud patterns and minimize false positives. The superior performance of the EADF underscores its reliability and adaptability for real-time fraud detection in digital payment systems. This analysis demonstrates the importance of hybrid and ensemble approaches in tackling the evolving challenges of financial fraud.The study on improving digital wallet fraud detection and personalization shows promising accuracy and user-centric security. Our model detected fraud with 97.3% accuracy and an F1-score of 0.91 using the Ensemble Anomaly Detection Framework (EADF), which combines Isolation Forest, Local Outlier Factor (LOF), and Long Short-Term Memory (LSTM) networks. This hybrid strategy beat independent models by 5%,

10.48047/jocaaa.2024.33.02.29

demonstrating the usefulness of integrating analytical tools to uncover complicated fraud patterns that single models may miss. Data analytics for user behavior analysis enabled personalized security prompts and service suggestions based on usage trends. These findings demonstrate the importance of multi-model frameworks in digital wallet security and how anomaly detection and deep learning strengthen resilience against developing fraud methods. This lowers false positives and streamlines the user experience by minimizing security interruptions for legitimate users. The tailored user engagement shows how our technology improves security without sacrificing ease. This combination of robust fraud detection and user personalization takes a big step toward meeting the safety and satisfaction needs of digital wallet users, paving the way for future advances in fraud prevention and adaptive user experiences.

5.Conclusion

The integration of advanced machine learning techniques into digital wallet systems has proven highly effective in enhancing both fraud detection and user personalization, addressing critical needs for secure and user-friendly digital payment environments. This study employed a hybrid machine learning framework, the Ensemble Anomaly Detection Framework (EADF), which combines Isolation Forest, Local Outlier Factor (LOF), and Long Short-Term Memory (LSTM) networks. The proposed model achieved a remarkable fraud detection accuracy of 97.3% with an F1-score of 0.91, significantly outperforming individual models and traditional approaches. The multi-model ensemble demonstrated its capability to identify complex fraud patterns and reduce false positives, thereby increasing the system's reliability. Beyond fraud detection, this research emphasized the importance of user behavior analysis in delivering personalized security measures and service recommendations. By utilizing advanced feature engineering techniques, the system tailored authentication and security prompts to user-specific behavioral trends, ensuring both high security and a seamless user experience. This dual focus on robust fraud detection and adaptive user engagement establishes a critical balance between security and convenience. The results highlight the significant advantage of employing multi-model frameworks in digital wallet systems. By leveraging anomaly detection and deep learning, the system not only mitigates evolving fraud strategies but also minimizes security interruptions for legitimate users. The study underscores the importance of scalable and adaptive fraud detection technologies in protecting digital payment systems from sophisticated threats. As the adoption of digital wallets continues to grow globally, these findings suggest that adaptive, user-focused technologies are indispensable for maintaining user confidence and safeguarding transactions. By laying a strong foundation for fraud detection and personalized services, this research supports the development of secure, efficient, and user-centric digital payment ecosystems, positioning digital wallets as essential tools in the transition toward a cashless economy.

References

1. Pu X, Chan FT, Chong AY, Niu B. The adoption of NFC-based mobile payment services: an empirical analysis of Apple Pay in China. International Journal of Mobile Communications. 2020;18(3):343-71.
2. Verkijika SF. An affective response model for understanding the acceptance of mobile payment systems. Electronic Commerce Research and Applications. 2020 Jan 1;39:100905.
3. Talwar S, Dhir A, Khalil A, Mohan G, Islam AN. Point of adoption and beyond. Initial trust and mobile-payment continuation intention. Journal of Retailing and Consumer Services. 2020 Jul 1;55:102086.
4. Singh N, Sinha N. How perceived trust mediates merchant's intention to use a mobile wallet technology. Journal of retailing and consumer services. 2020 Jan 1;52:101894.
5. Yuan S, Liu L, Su B, Zhang H. Determining the antecedents of mobile payment loyalty: Cognitive and affective perspectives. Electronic Commerce Research and Applications. 2020 May 1;41:100971.
6. Karimi S, Liu YL. The differential impact of "mood" on consumers' decisions, a case of mobile payment adoption. Computers in Human Behavior. 2020 Jan 1;102:132-43.
7. Karthikeyan T, Govindarajan M, Vijayakumar V. An effective fraud detection using competitive swarm optimization based deep neural network. Measurement: Sensors. 2023 Jun 1;27:100793.
8. Iscan C, Akbulut FP. Fraud Detection using Recurrent Neural Networks for Digital Wallet Security. In2023 8th International Conference on Computer Science and Engineering (UBMK) 2023 Sep 13 (pp. 538-542). IEEE

10.48047/jocaaa.2024.33.02.29

9. Garin L, Gisin V. Machine learning in classifying bitcoin addresses. The Journal of Finance and Data Science. 2023 Nov 1;9:100109.
10. Akartuna EA, Johnson SD, Thornton A. Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. Technological Forecasting and Social Change. 2022 Jun 1;179:121632.
11. Jayasingh BB, Sri GB. Online transaction anomaly detection model for credit card usage using machine learning classifiers. In2023 International Conference on Emerging Smart Computing and Informatics (ESCI) 2023 Mar 1 (pp. 1-5). IEEE.
12. Alamri MA, Ykhlef MA. A Machine Learning-Based Framework for Detecting Credit Card Anomalies and Fraud. In2023 27th International Conference on Information Technology (IT) 2023 Feb 15 (pp. 1-7). IEEE.
13. Chang V, Di Stefano A, Sun Z, Fortino G. Digital payment fraud detection methods in digital ages and Industry 4.0. Computers and Electrical Engineering. 2022 May 1;100:107734.
14. Lai PC, Tong DL. An artificial intelligence-based approach to model user behavior on the adoption of e-payment. In Handbook of research on social impacts of e-payment and blockchain technology 2022 (pp. 1-15). IGI Global.
15. Latha SS, Rai AV, Likhith R, Abhiram R, Pai AV. Secured Eye Pay: An E-payment a Application for visually impaired people. In2022 International Mobile and Embedded Technology Conference (MECON) 2022 Mar 10 (pp. 632-638). IEEE.
16. Kamuni N, Dodda S, Vuppalapati VS, Arlagadda JS, Vemasani P. Advancements in Reinforcement Learning Techniques for Robotics. Journal of Basic Science and Engineering.;19:101-11.
17. Prasad N, Shah J, Narukulla N, Swamy H. Security Challenges and Solutions in Cloud-Based Artificial Intelligence and Machine Learning Systems.
18. Srivastava M, Copin R, Choy A, Zhou A, Olsen O, Wolf S, Shah D, Rye-Weller A, Chen L, Chan N, Coppola A. Proteogenomic identification of Hepatitis B virus (HBV) genotype-specific HLA-I restricted peptides from HBV-positive patient liver tissues. Frontiers in Immunology. 2022 Dec 13;13:1032716.
19. Ramona O. Financial markets–structural changes and recent developments.
20. Padhi S, Battina DP. Automating Root Cause Analysis of Anomalies in Ericsson Wallet Platform using Machine Learning.
21. Benamara NK, Keche M, Wellington M, Munyaradzi Z. Securing e-payment systems by RFID and deep facial biometry. In2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA) 2021 Apr 6 (pp. 151-157). IEEE.
22. Gobena MA. Money laundering in Ethiopia: an analysis of typologies and techniques. Journal of Money Laundering Control. 2023 May 30;26(4):696-708.
23. Moonde C. Secure mobile payment system based on Blockchain technology for higher learning institutions (Doctoral dissertation, The University of Zambia).
24. Tilala M, Chawda AD, Benke AP, Agarwal A. Regulatory Intelligence: Leveraging Data Analytics for Regulatory Decision-Making. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068. 2022 Dec 29;1(1):78-83.
25. Ogeti P, Fadnavis NS, Patil GB, Padyana UK, Rai HP. Blockchain technology for secure and transparent financial transactions. European Economic Letters, 12 (2), 180-192 [Internet]. 2022
26. Nakra V. Enhancing Software Project Management and Task Allocation with AI and Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication. 2023;11(11):1171-8.
27. Dave A, Swamy H, Nakra V, Agarwal A. Machine Learning Techniques and Predictive Modeling For Retail Inventory Management Systems. Educational Administration: Theory and Practice. 2023 Dec 25;29(4):698-706.

10.48047/jocaaa.2024.33.02.29

28. Tilala M, Pamulaparthyvenkata S, Chawda AD, Benke AP. Explore the Technologies and Architectures Enabling Real-Time Data Processing within Healthcare Data Lakes, and How They Facilitate Immediate Clinical Decision-Making and Patient Care Interventions. European Chemical Bulletin.;11:4537-42.
29. Sharma K, Kumar A. Innovative 3D-Printed Tools Revolutionizing Composite Non-destructive Testing Manufacturing. International Journal of Science and Research (IJSR), ISSN. 2022:2319-7064.
30. Tilala M, Chawda AD, Benke AP, Agarwal A. Regulatory Intelligence: Leveraging Data Analytics for Regulatory Decision-Making. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068. 2022 Dec 29;1(1):78-83.
31. Adepoju O, Wosowei J, Jaiman H. Comparative evaluation of credit card fraud detection using machine learning techniques. In2019 Global Conference for Advancement in Technology (GCAT) 2019 Oct 18 (pp. 1-6). IEEE.
32. Zhao M, Li Z, An B, Lu H, Yang Y, Chu C. Impression Allocation for Combating Fraud in E-commerce Via Deep Reinforcement Learning with Action Norm Penalty. In IJCAI 2018 Jul 13 (pp. 3940-3946).
33. Guo Q, Li Z, An B, Hui P, Huang J, Zhang L, Zhao M. Securing the deep fraud detector in large-scale e-commerce platform via adversarial machine learning approach. In The world wide web conference 2019 May 13 (pp. 616-626).
34. Mauritsius T, Alatas S, Binsar F, Jayadi R, Legowo N. Promo abuse modeling in e-commerce using machine learning approach. In2020 8th International Conference on Orange Technology (ICOT) 2020 Dec 18 (pp. 1-6). IEEE.