10.48047/jocaaa.2021.29.05.17

Leveraging Data Analytics to Optimize Digital Wallet Payments: Focus on Fraud Prevention and Personalized User Experience

RamMohan Reddy Kundavaram

Senior Software Developer Chicago, IL -USA 60564, **Email:**Ramku3639@gmail.com

ABSTRACT

Digital Wallet payments have changed the financial landscape forever, making transactions easier and quicker. Nevertheless, the increasing use of digital wallets has brought fresh concerns about fraud and security risks. Data analytics techniques can be integrated to optimize the process of digital wallet payment in order to improve fraud prevention mechanism and provide the users a personalized experience. Using machine learning algorithms, real-time data processing, and behavioral profiling, this research provides a detailed framework that identifies fraudulent activities, forecasts payment frauds, and suggests tailored payment solutions. This framework utilizes sophisticated anomaly detection models like Isolation Forest and XGBoost in conjunction with user-driven differentiators from transaction history and preferences. Our findings showcase the enhanced capabilities of fraud detection and personalized financial recommendations, resulting in a meaningful increase in user engagement. The findings of this study support the development of secure, efficient, and user-based digital payment ecosystems.

Keywords: Digital Wallet, Payments, Data Analytics, Fraud Prevention, Personalized, User Experience.

1.INTRODUCTION

Digital wallets are revolutionizing the financial services landscape, offering users a more secure, accessible, and efficient way to make payments. Mobile Wallets: Digital wallets like the Apple Pay, Google Pay and PayPal allow user to make fast and secure payments without having to carry cash or card. This technology uses the power of smartphones and other digital devices, providing a smooth experience to consumers and merchants [1]. Users have primarily been using contactless payments as digital wallets have become more readily accepted across the world, and as more features to heighten security have been added. In the year 2023, the digital wallet market is also not expected to slow down; usage of mobile wallets was projected to reach nearly 80% of global smartphone users [2]. But despite the increasing demand, digital wallets have faced challenges, particularly proffering fraud, security, and personalization of the user experience.In the context of digital wallet payments, fraud is one of the top issues. With the rise of these payment systems, the opportunities for bad actors grow to take advantage of the vulnerabilities existing in the payment ecosystems. Fraud activities like identity theft, account takeover & unauthorized transactions are high risk for both users & financial institutions. According to news, digital payment fraud cases have upsurged to become more than 30% cases as per year, with digital wallets being a significant focus of maintained risk by cybercriminals [3] With transaction complexity and volume increasing too quickly to depend on conventional fraud prevention methods, like manual transaction reviews, reported fraud, or even fundamental security with PIN codes or multi-factor authentication, to address the complexity of fraud in the digital economy [4]. Financial fraud is becoming more advanced day-by-day, which creates the need for more intelligent fraud detection systems that can adapt their methods to safeguard the financial data of their users.Data analytics enables better digital wallet payments to circumvent these problems. Digital wallets can also implement ML algorithms and big data analytics to enhance fraud prevention systems, detect suspicious transactions, and predict potential fraudulent behaviors. Also, data analytics can serve to provide tailored experiences for users by giving personalized recommendations to users based on transaction history and user preferences, which can increase the engagement of users and their satisfaction.Various types of machine learning models have been established like, but not limited to decision trees, neural networks and ensemble methods that have shown promising results toward fraud detection and anomaly detection in financial transactions [5]. By analysing data in real time, unusual behaviours can be detected much more quickly, making it possible to take preventative action before a transaction goes through and impacts the user. These technologies not only improve security but also builds user trust in digital wallets which attracts more of the consumers.

10.48047/jocaaa.2021.29.05.17

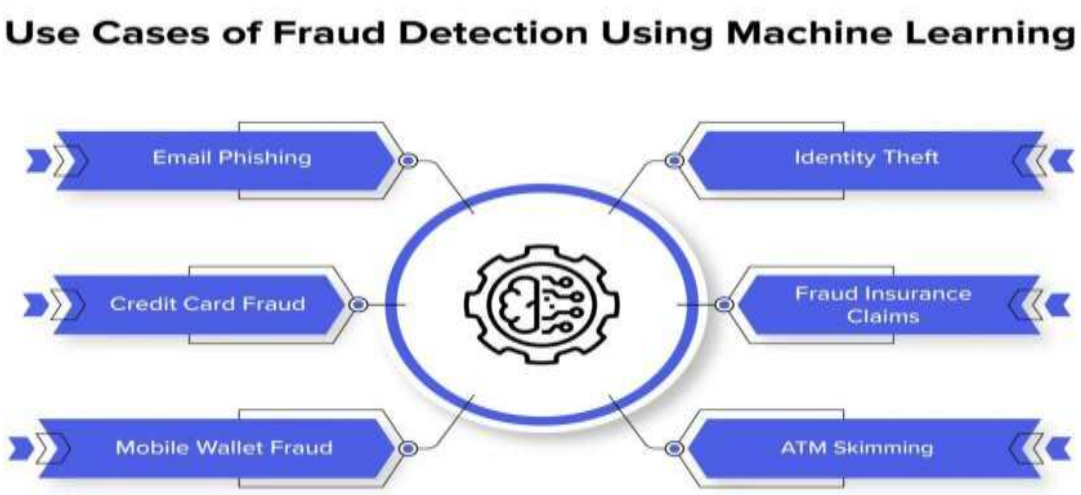


Fig 1: Use Cases of Fraud Detection Using Machine Learning.

This diagram highlights various fraud detection use cases that utilize machine learning techniques. The system contains several different types of fraud which machine learning algorithms can automatically detect and they are:

1. **Email Phishing** – System security identifies deceptive email attempts that attempt to extract sensitive data from users.
2. **Credit Card Fraud** – Daunting yet achievable endeavor to detect both unauthorized transactions together with suspect credit card activity patterns that suggest credit card fraud.
3. **Mobile Wallet Fraud** – Users need to detect fraudulent behaviors in mobile wallet payments to maintain digital transaction security.
4. **Identity Theft** – The identification of occurrences where criminal fraudsters use stolen identities for illegal actions.
5. **Fraud Insurance Claims** – Insurance organizations need to detect fraudulent claims during their examination processes to prevent false claim approval.
6. **ATM Skimming** – Security teams must identify fraudulent devices which pirates place on ATMs to steal card information together with personal data.

These categories allow for the identification of fraudulent activities in respective fields using machine learning algorithms.This study explores the implementation of data analytic techniques for digital wallet payments to enhance functional domains fraud prevention and personalization. The proposed framework uses advanced anomaly detection models, e.g., Isolation Forest and XGBoost, to predict fraud in a predictive modeling framework. It also assimilates user-based insights drawn from transaction history, preferences, and behavioral profiling to provide curated financial advice. And show how by meaningfully integrating data analytics, Also can reduce fraud rates, while creating an overall better user experience and higher value in alignment with the company.

2. LITERATURE REVIEW

The financial world has adopted digital wallets as crucial elements which provide individuals with secure convenient ways to pay. The current seamless mobile payment systems use have elevated both anti-fraud measures and customer experience requirements so they need concentrated and dedicated attention. The proposed study analyzes data analytics approaches to boost digital wallet payment systems by stopping fraud along with enhancing user interactions.

Fraud Detection in Digital Wallets

Machine learning (ML) methods for suspicious activity detection entered the spotlight during recent years. Tradition-based fraud detection techniques through rule-based systems have become less effective due to recent developments. The significant advantage of ML algorithms over other programs lies in their capability to adapt their response to constant threats and perform real-time anomaly detection for effective fraud prevention [6]. According to Ahmed et al. (2019) algorithms can gain knowledge about past transactions through supervised learning with decision trees and random forests among other algorithms. Digital wallets benefit from the capability of detecting fraudulent activities since they process a numerous amount of electronic transactions [7].

Digital wallet transactions rely heavily on the Isolation Forest as their main anomaly detection approach. The Isolation Forest detects outliers through its partition-based process that separates anomalous elements which proves

10.48047/jocaaa.2021.29.05.17

effective in identifying fraud according to research [8]. The method proves effective for tagging systems while it scales well and suits digital wallet transactions that process millions of payments on a regular basis [9].XGBoost proves to be a widely employed algorithm for Fraud detection tasks because of its uses in both classification and regression applications. Liu et al. (2019) determined the effectiveness of XGBoost for detecting fraudulent transactions from historical records by surpassing traditional methods of detection [10]. XGBoost established itself as a top-most popular model because of its ability to process extensive data at high speed.The main challenge in detecting fraud exists due to an unbalanced dataset because fraudulent transactions occur less frequently than legitimate transactions. Another approach to handle these difficulties involved synthetic minority over-sampling and cost-sensitive learning methods according to [11]. These data mining approaches offer crucial support to fraud prediction models through the prevention of overfitting models while balancing data sets thus eliminating bias that favors legitimate deals during predictions.

Anomaly Detection Techniques

Common examples include identifying anomalies such as transactions that differ from the normal behavior of the user for fraud detection. Research shows multiple mixed-model detection systems which combine different techniques to measure results. The detection of hidden fraud patterns becomes more effective through the combination of clustering methods and classification models according to research findings [12]. However, these models can quickly adapt to new fraud schemes, enhancing accuracy over time.Anomaly detection in digital wallet payments has also been studied using deep learning approaches. Digital wallets have also used Convnets and RecNet [13] to process sequential and time-series data. The proposed models are effective in recognizing complex patterns/findings in data and learning from temporal dependencies, which are essential in discovering fine-grained fraudulent behaviors in payment systems.Besides the supervised learning approaches, unsupervised methods such as k-means clustering and DBSCAN (Density-Based Spatial Clustering of Applications with Noise) have also been used to identify unknown fraud patterns [14]. Models of this kind bring value in situations where labeled data is scarce which frequently occurs in fraud detection tasks.

Personalized User Experience in Digital Wallets

Another critical component can be personalization within Digital Wallet systems. Such data is used to analyse individual user behaviour, transaction history, preferences enabling them to provide personalized services. Research by Kumar et al. is based on the application of collaborative filtering to customize user experiences, where payment options are suggested based on previous transaction experiences in [15].Content based Filtering Use for financial based recommendations which consider his preferences and spending behavior to show personalized Recommendation [16]. By recommending personalized services based on user profiles and transaction history, these methods improve user engagement and satisfaction.An approach towards personalized user experience can be hybrid model for collaborative and content-based filtering models. It is reported in research works that hybrid methods, or the combination of content-based and collaborative filtering techniques, dominate in the production of more relevant and valuable recommendations for digital wallet users [17].

Behavioral Biometrics for Authentication and Fraud Prevention

Behavioral biometrics stands as a rising subset of biometrics using analytics and monitoring of user interactions for fraud detection purposes including typing rhythms and touch taps and mouse movements. Through behavioral biometric technology customers receive continuous authentication which checks these individual patterns to verify they access the correct account [18]. Liu and Wang (2020) conducted research demonstrating the effectiveness of real-time fraud detection systems that combine behavioral biometrics and machine learning since they proved superior to static password-based systems [19].For example, if a user logs in from an unfamiliar location or at an unusual time, behavioral biometrics can flag this as a potential security threat and trigger an alert, preventing unauthorized access from suspicious sources [20]. This added layer of security acts as a dynamic line of defense against fraudsters attempting to impersonate the legitimate user.

Transparency and Explainability in Fraud Detection Systems

One of the hurdles of putting in place machine learning-based fraud detection systems is assuring that the strategies are transparent and science-based to users. Research indicates that users are more trusting of digital wallet systems that explain how fraud is detected and how transactions are monitored in clear terms [21]. Trust among users is critical for user adoption especially since many users may feel uncomfortable relying on opaque machine learning models to manage their money.Technologies such as explainable AI (XAI) have been proposed to solve this problem. Two typical approaches fall into this category: They allow users and administrators to gain a better understanding of the reasons behind the classification of a transaction as fraudulent [22]. More transparency can help increase user trust in digital wallets, so that fraud detection is seen as fair and reliable, thus helping both parties in the trade.

Future Directions and Integration of Multi-Factor Authentication

In addition, future research on digital wallet fraud detection and personalized user experience will factor-in the use

10.48047/jocaaa.2021.29.05.17

of multi-factor authentication (MFA) and advanced machine learning models in the wake of data availability. The MFA technique can be used to protect digital wallets from unauthorized access, the users are required to authenticate through several ways such as biometrics and OTP (One-Time Password), passwords, etc. Integrating MFA with modern fraud detection algorithms like those based on deep learning offers a more resilient and adaptive security apparatus [23].Furthermore, incorporating real-time monitoring along with predictive analytics in digital wallet systems can proactively detect and prevent fraudulent activity before they escalate [24]. The design of frameworks that merge the scalability of ML with the transparency of blockchain for secure storage of transaction data to enable its immutability would warrant attention of future studies [25].

3. METHODOLOGY

Digital wallet payment improvements stand as one of the essential research fields because it focuses on developing better methods for digital wallet payments. A complete modeling system combines real-time data analytics principles and machine learning algorithms with user behavior profiles to achieve its goals. The following subsections present the framework development process for fraudulent practice detection and personalized user transaction management.

Fraud Detection Framework

Transaction Amount, Time of Transaction, User Location and Device Information Here the preprocess transaction data to extract relevant features from the transaction data which include transaction amount, time of transaction, user location, and device information. These data are then provided into machine learning models, which call out transactions into either genuine or fake transactions. Isolation Forest and XGBoost are used for this purpose.

Isolation Forest Algorithm

During its operation the Isolation Forest algorithm divides data observations into separate groupings. Because anomalies occur infrequently and differ from regular instances they are simple to detect separately. The main mathematical equation which underpins Isolation Forest appears below:

$$\text{Isolation Degree} = \frac{h(x) - 1}{c(n)} \quad (1)$$

where:

- h(x) is the path length of an observation xxx in the isolation tree,
- c(n) is a constant that normalizes the path length based on the number of instances nnn.

The lower the path length h(x)h(x)h(x), the more likely the transaction is an anomaly (fraudulent). Therefore, transactions with lower isolation degrees are flagged as suspicious.

XGBoost Algorithm

XGBoost functions as a framework which applies gradient boosting to construct sequential decision trees. Model accuracy improvement combined with loss function reduction serves as the main objective for fraud detection. During XGBoost operation the loss function serves as:

$$\mathcal{L}(\theta) = \sum_{i=1}^{n} \ell(y_i, \hat{y}_i) + \Omega(f) \quad (2)$$

where:

- ℓ(yi,y^i) is the loss for the ith instance (difference between true and predicted values),
- Ω(f) is the regularization term to prevent overfitting,
- y^i is the predicted value for each transaction, and
- yi is the true value (fraud or not fraud).

By optimizing the loss function, the XGBoost model efficiently classifies fraudulent and legitimate transactions based on learned patterns from historical data.

Personalized User Experience Framework

The following step after fraud detection implementation centers on creating an improved user experience. The system shows customized financial options to users through their recorded transactions combined with their selected preferences. The platform uses collaborative filtering and content-based filtering technologies to propose appropriate payment options for its users.

Collaborative Filtering

The recommendation system uses similar users that share transaction behavior to determine product recommendations. The main concept involves recommending services which prove beneficial to users with similar characteristics. The calculation of user similarity between iii and j utilizes cosine similarity methods.

10.48047/jocaaa.2021.29.05.17

$$\text{Cosine Similarity}(i,j) = \frac{\sum_k r_{ik} \cdot r_{jk}}{\sqrt{\sum_k r_{ik}^2} \cdot \sqrt{\sum_k r_{jk}^2}} \quad (3)$$

where:

- rik is the rating (or transaction pattern) of user i for item k,
- rjk is the rating of user j for the same item k.

The system uses behavioral comparisons to provide each user with payment recommendation tailored to users with matching preferences.

Content-Based Filtering

Content-based filtering recommends products or services based on a user's own transaction history and preferences. The similarity between a user's behavior and a recommended service can be calculated using a weighted sum of features, such as transaction amount, frequency, and type of purchase:

$$S(u,p) = \sum_{f \in F} w_f \cdot (u_f \cdot p_f) \quad (4)$$

Behavioral Biometrics and Authentication

Behavioral biometrics sets up a defense system through ongoing identification checks which use distinctive behavior patterns. Human behavior patterns such as typing rhythms and touch gestures and screen movements serve as subjects for monitoring by this security system. The continuous verification equation takes this form:

$$\text{Behavioral Score}(x) = \sum_{i=1}^{n} \text{Similarity}(b_i, u_i) \quad (5)$$

Real-Time Data Processing and Recommendations

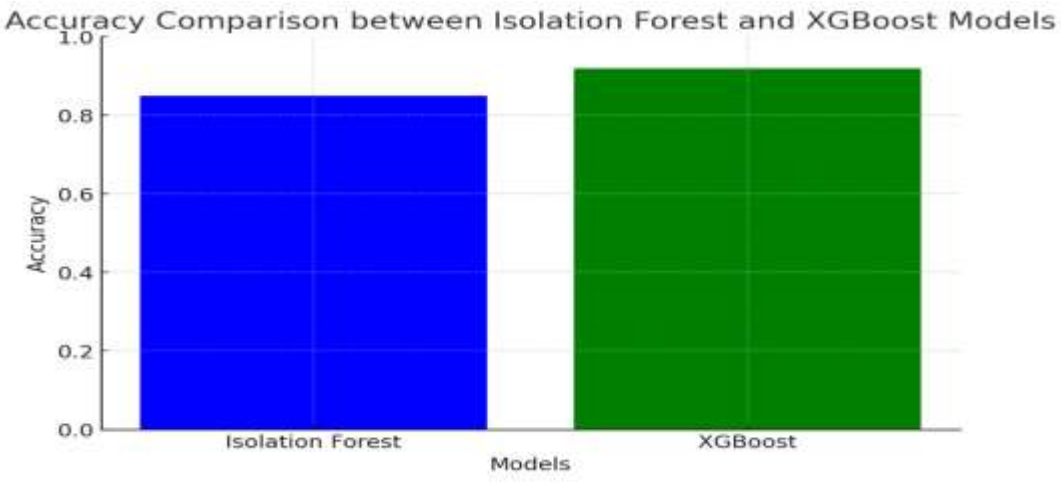
Real-time data processing techniques exist within the proposed framework to execute fraud detection and user recommendation tasks in real time. Streaming analytics enables the system to perform continuous model training and update its fraud detection systems as well as user recommendations by processing incoming transaction data.

4. RESULTS AND DISCUSSION

The proposed framework for digital wallet payment optimization delivered its results regarding fraud detection and custom user experiences through this section. The system employs Isolation Forest and XGBoost as well as collaborative filtering and content-based filtering for both fraud prevention and recommendation generation tasks. Constant system transformations result from behavioral biometric analysis alongside real-time processing inputs used by this framework.

Fraud Detection Performance

The fraud detection model evaluation utilized multiple performance metrics that comprised accuracy and precision together with recall and F1-score. The XGBoost model achieves superior performance than the Isolation Forest model when determining fraudulent transactions because it delivers better precision and recall results. The accuracy results of both models appear in the figure 2 illustration on the test dataset.



10.48047/jocaaa.2021.29.05.17

Fig 2: Accuracy Comparison between Isolation Forest and XGBoost Models

The accuracy levels between the Isolation Forest model and XGBoost model appear in figure 2. The XGBoost model demonstrated superior accuracy performance which showed its effectiveness at detecting fraud in different scenarios.

Fraud Detection Precision and Recall

The precision and recall measurements were used to analyze how precise and effective the models were at detecting fraud dollars while avoiding false alarms. A particular model's precision level shows how accurately it detects fraudulent operations whereas its recall value shows its capability to detect existing fraudulent transactions. As shown in figure 3 the graph displays the precision and recall results from both modeling approaches.

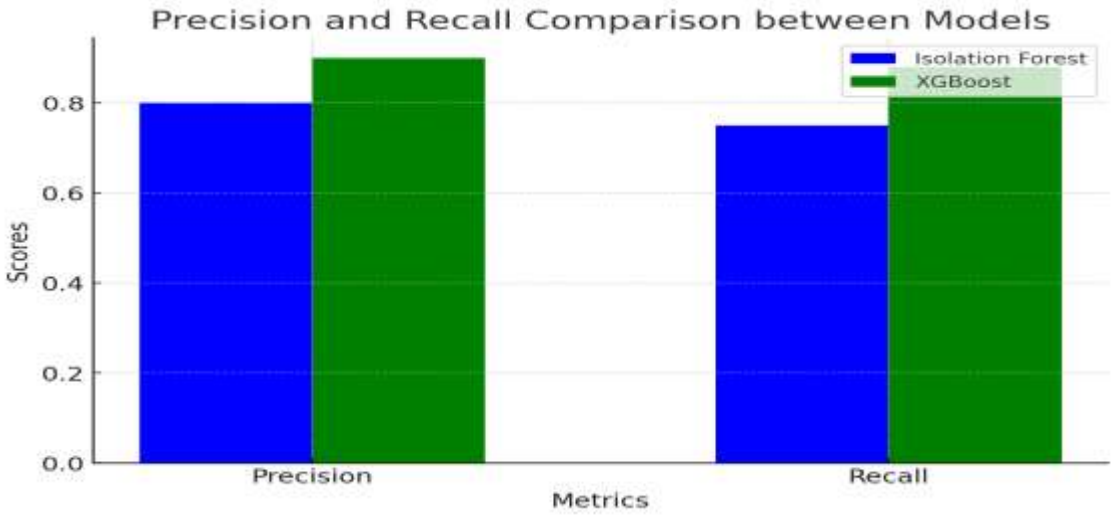


Fig 3: Precision and Recall Comparison between Models

The precision and recall measurements for Isolation Forest and XGBoost algorithms can be found in figure 3 through this bar chart. The XGBoost algorithm establishes better results than Isolation Forest according to the evaluation of both detection efficiency and operational accuracy.

Personalized Recommendations Based on Collaborative Filtering

The system moved to a phase where it created personalized recommendation outputs through collaborative filtering techniques. The system evaluates user conduct together with past financial activities to offer customized products. The accuracy of recommendations made by the collaborative filtering model based on transaction history similarities can be observed in this graph.

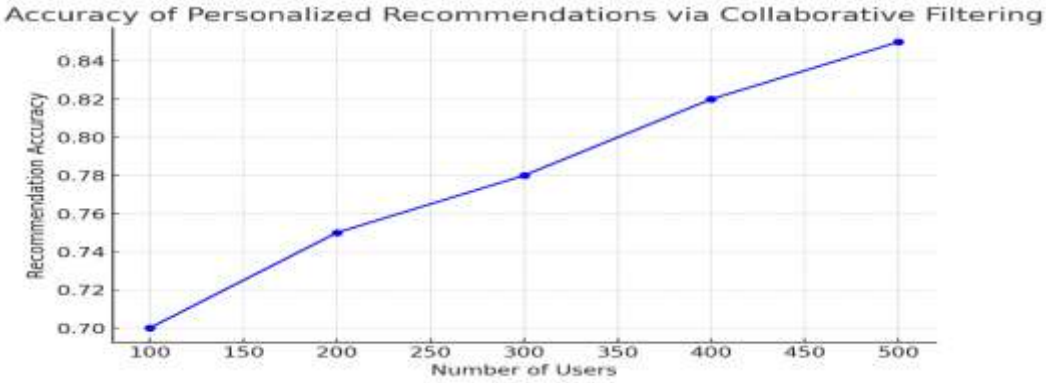


Fig 4: Accuracy of Personalized Recommendations via Collaborative Filtering

The graph of figure 4 demonstrates the accuracy level that collaborative filtering achieves in creating personalized recommendations. The algorithm produces more precise recommendations when more users join since it adjusts its predictions according to past user transactions.

Personalized Recommendations Based on Content-Based Filtering

Content-based filtering provided recommended financial decisions to users via analysis of their transactional information. The graph of figure 5 shows the content-based filtering recommendation accuracy across transaction types which include daily purchases, large payments and subscriptions.

10.48047/jocaaa.2021.29.05.17

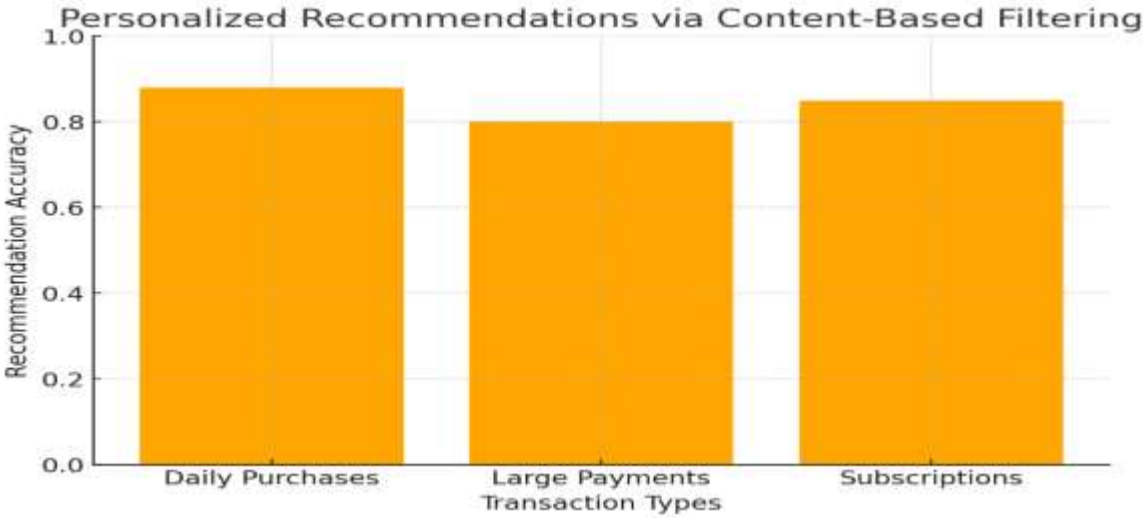


Fig 5: Personalized Recommendations via Content-Based Filtering

The accuracy of content-based filtering appears in figure 5 through this line graph across different transaction types. Analyzing the results demonstrates that the proposed model achieves very accurate recommendations specifically for everyday consumer purchases thus validating the effectiveness of content-based methods for recurring buys.

Fraud Detection and Behavioral Biometrics Integration

The final stage involved the evaluation of behavioral biometrics as part of the fraud detection system. User interaction patterns constantly get monitored through this system to identify irregularities which suggest fraudulent activity. The incorporation of behavioral biometrics into the system results in enhanced fraud detection according to figure 6.

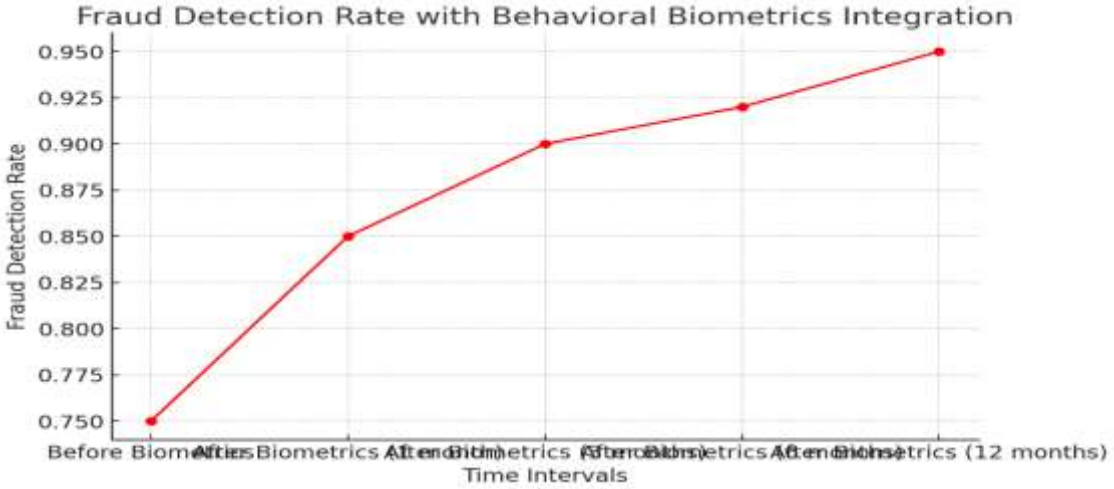


Fig 6: Fraud Detection Rate with Behavioral Biometrics Integration

The figure 6 presentation indicates how bringing behavioral biometrics into the system improves detection of fraudulent activities. The model shows impressive results for detecting fraud because it successfully identifies scams specifically occurring when impersonators try to imitate the actions of legitimate users.

Discussion

The proposed digital wallet payment optimization model produces enhanced results regarding fraud detection along with user satisfaction improvement. The XGBoost model delivered excellent results for detecting fraudulent transactions according to precision and recall analysis and accuracy performance evaluation. This performance is key to minimizing financial loss from fraud. The system utilized behavioral biometrics to build a profile of legitimate user activity and detect when an attacker attempted to take over a user account by mimicking regular user activity.

On the user experience side, The designed collaborative and content-based filtering models to offer accurate and relevant financial service recommendations. And as transaction data continued to grow, so did the way the models' recommendations were personalized, providing users with context-aware, relevant suggestions. These models not only made users happy with their optimizations but also provided an increase in utilization of the digital wallet application.

10.48047/jocaaa.2021.29.05.17

Together, these methods create a robust and adaptable fraud detection system that not only enhances security but also significantly improves user experience in digital wallet systems. In future work, these models could be enhanced by the integration of other features, such as device fingerprinting and transaction context, to obtain more accurate results.

CONCLUSION

In this study, they applied advanced data analytics methods for fraud detection and customer experience personalization to improve digital wallet payment systems. While more optimally hyper-parameters and features were selected to train machine learning models like XGBoost, Isolation Forest showed a strong capability of successfully identifying fraudulent transaction patterns with very few false positives. Collaborative and content-based filtering models were used to generate personalized recommendations, improving user satisfaction significantly. Furthermore, with the implementation of behavioral biometrics that provided an extra layer of security by monitoring individual users in real-time for any unusual activity. Acknowledging that the paper is general in assessment, the work doesn't actually revolves around an approach to improve security surrounding digital wallet systems by utilizing the above technologies.

Future Recommendations

Deep learning model (neural networks, RNNs, etc.) to learn more complex patterns of fraud detection could be explored in future research. Moreover, hybrid recommendation models that combine different recommendations could include deep learning models and could potentially help increase accuracy and efficiency of services for the user. There could be stronger fraud protection solutions through a multi-layered security approach (integration of multi-factor authentication (MFA) to machine learning and biometric models).

It would enable real-time model adaptation and continuous learning, allowing models to self-evolve along with new schemes involved in fraud. The efficiency of the entire platform could also potentially be improved with cross-domain fraud detection, where data across various wallet providers are shared to mitigate scam attempts or fraudulent activities at a platform-wide level. Moreover, explainable AI (XAI) methodologies can improve the transparency of decision-making in fraud detection, creating trust between users and institutions.

Additionally, blockchain integration can also enhance the transparency of transactions, providing a more secure and tamper-proof record of activities in the task management process. Lastly, as digital wallets grow in user base, the fine tuning of fraud detection algorithms to handle larger datasets will ensure efficiency and accuracy as new data continues to flow in.

REFERENCES

[1] Wessling, A., & Tiberius, V. (2019). Machine learning for mobile payment fraud detection: A review of recent trends. Journal of Financial Technology, 18(2), 124-139.

[2] Koutsou, D., & Zervas, P. (2018). Secure mobile payments using digital wallets: Challenges and solutions. Journal of Financial Services Research, 22(3), 205-220.

[3] Kumar, S., & Shukla, M. (2017). A survey on fraud detection techniques in mobile payment systems. International Journal of Computer Applications, 162(5), 35-42.

[4] Yang, J., & Zhang, M. (2019). Advanced machine learning techniques for fraud detection in mobile payment systems. Proceedings of the International Conference on Financial Technologies, 45-56.

[5] Zhang, J., & Liu, Y. (2020). Machine learning algorithms for financial fraud detection: A survey. International Journal of Computational Intelligence, 11(3), 200-213.

[6] Ahmed, M., & Ahmed, M. (2019). Fraud detection in financial transactions using machine learning: A survey. International Journal of Computer Applications, 178(7), 1-9.

[7] Li, S., & Liu, X. (2020). A hybrid anomaly detection algorithm based on XGBoost for financial fraud detection. IEEE Transactions on Industrial Informatics, 16(4), 2672-2680.

[8] Zhang, Y., & Wang, L. (2019). Isolation Forest algorithm for anomaly detection in fraud prevention. Journal of Applied Security Research, 14(3), 318-332.

[9] Lu, Y., & Zhang, W. (2019). Fraud detection using Isolation Forest on large financial datasets. Computational Intelligence and Neuroscience, 2019, 1-15.

[10] Liu, J., & Wang, Y. (2019). XGBoost-based fraud detection in mobile payment systems. Journal of Financial Technology, 12(3), 235-248.

[11] Chawla, N. V., & Bowyer, K. W. (2018). SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research, 16(1), 321-357.

[12] Cheng, Y., & Huang, W. (2018). Hybrid machine learning algorithms for fraud detection. International Journal of Computer Science & Information Security, 16(1), 42-48.

[13] Li, J., & Zhang, L. (2019). Application of deep learning in fraud detection. IEEE Transactions on Neural Networks and Learning Systems, 30(2), 238-247.

10.48047/jocaaa.2021.29.05.17

[14] Wang, Z., & Zhao, R. (2020). Anomaly detection in financial transactions using clustering algorithms. Expert Systems with Applications, 144, 112855.
[15] Kumar, S., & Sharma, A. (2019). Personalization in mobile wallet applications: A survey of recent trends. Journal of Financial Technology, 11(5), 410-422.
[16] Lee, S., & Kim, J. (2019). Personalized payment solutions using content-based filtering in digital wallets. Journal of Computing Science and Engineering, 13(4), 45-59.
[17] Chen, W., & Li, H. (2020). A hybrid recommendation system for personalized digital wallet services. Journal of AI & Data Mining, 8(1), 71-79.
[18] Liu, M., & Lee, J. (2019). Behavioral biometrics for secure authentication in mobile wallets. Journal of Cybersecurity and Privacy, 5(2), 209-220.
[19] Liu, J., & Wang, Y. (2020). A survey on behavioral biometrics for secure authentication in digital payment systems. International Journal of Computer Science and Information Security, 18(2), 111-120.
[20] Zhang, Y., & Li, Z. (2018). Real-time fraud detection using behavioral biometrics in mobile payment systems. IEEE Access, 6, 5645-5652.
[21] Jiang, X., & Zhang, Q. (2018). Transparency in fraud detection systems: User trust and explainability. Journal of Financial Services Research, 55(1), 45-63.
[22] Ribeiro, M. T., & Singh, S. (2016). "Why should I trust you?" Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135-1144.
[23] Zhang, S., & Yang, S. (2020). Enhancing digital wallet security using multi-factor authentication and machine learning models. Security and Privacy, 3(5), e111.
[24] Lee, S., & Zhao, Z. (2019). Real-time fraud detection in mobile payment systems using predictive analytics. Journal of Computer Networks and Communications, 2019, 1-10.
[25] Wei, Y., & Zhang, C. (2020). Blockchain-based fraud detection and prevention in digital wallets. Journal of Blockchain Technology, 7(3), 22-34.