Scientific Research Publishing

Engineering, 2025, 17(1), 155-167
https://www.scirp.org/journal/eng
ISSN Online: 1947-394X
ISSN Print: 1947-3931

Mixed Integer Program for e-Wallet Security Based on Suspicious Transaction Detection

Pacôme Brou*, Kadokan Coulibaly, Siaho Diomande

Laboratoire des Sciences Technologiques de l'Information et de la Communication, Ecole Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC), Abidjan, Côte d'Ivoire
Email: *pacome.brou@esatic.edu.ci

How to cite this paper: Brou, P., Coulibaly, K. and Diomande, S. (2025) Mixed Integer Program for e-Wallet Security Based on Suspicious Transaction Detection. *Engineering*, **17**, 155-167.
https://doi.org/10.4236/eng.2025.171010

Received: December 1, 2024
Accepted: January 24, 2025
Published: January 27, 2025

Copyright © 2025 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Open Access

Abstract

With the rise of digital transactions, e-Wallets have become prime targets for fraudulent activity. Early detection of suspicious transactions is therefore crucial to protect users and maintain trust in these systems. This article proposes a mathematical model based on a Mixed Integer Program (MIP) to identify and block suspicious transactions. This mathematical approach is designed to analyze e-Wallet transactions in real time by combining integer and continuous decision variables, offering greater flexibility in modeling fraud detection constraints. It considers parameters such as transaction cost, geographical location, type of device used for the transaction, IP address and other potential fraud indicators. Assigning suspicion scores to each transaction enables the model to identify risks that become habitual behavior and mark them as suspicious. Tests carried out on 10,000 digital transactions show that using PMNE significantly improves the detection of fraudulent transactions by identifying the most critical anomalies in terms of accuracy, adaptability and operational efficiency. The model also offers greater accuracy, reducing the number of false positives and false negatives, enabling faster intervention to block truly suspicious transactions.

Keywords

e-Wallet, PMNE, Digital Transaction, Suspicion Score, Suspicious Transaction

1. Introduction

Electronic wallets (e-Wallets) have become a mainstay of modern financial transactions, due to their simplicity and accessibility. However, this massive adoption is accompanied by an exponential increase in the risk of fraud, particularly through unauthorized or suspicious transactions. According to recent reports, losses due to electronic fraud reach billions of dollars a year, underscoring the

urgent need for effective solutions to strengthen e-Wallet's security. Among existing approaches, suspicious transaction detection plays a key role in identifying anomalous behavior before it causes financial loss. However, heuristic models or those based solely on statistical techniques often lack precision in complex environments. In this context, Mixed Integer Programs (MIPs) have emerged as a robust and flexible alternative. These models make it possible to formulate detection problems in the form of mathematical optimization, integrating continuous and discrete variables to represent the diversity of transactional behaviors. In this paper, we propose a PMNI model for securing e-Wallets, specifically designed to detect and manage suspicious transactions. The model is based on a combination of constraints related to transaction amounts, geographical locations, device types and associated IP addresses. The results obtained demonstrate the effectiveness of PMNI in reducing false positives, while maintaining a high level of anomaly detection.

2. Literature Review

Securing electronic wallets has become a major challenge in the context of increasing digital fraud. The integration of techniques for detecting suspicious transactions relies on mathematical models, notably Mixed Integer Programs (MIPS). These models enable decision problems to be formulated by combining continuous and discrete variables, offering an optimal solution for identifying and managing fraudulent behavior. The popularity of e-wallets rests on their convenience, but their vulnerability to attack remains a major challenge. Thus, in 2019, Jha *et al.* proposed a review of fraud detection techniques in digital payments, including both statistical and algorithmic approaches; the article highlights the importance of hybrid models to improve performance [1]. According to Gupta *et al.* in [2], detection of suspicious behavior relies on intelligent algorithms to analyze transaction data in real time; electronic fraud includes abnormal transactions (unusually high amounts, unfamiliar locations, etc.). Nguyen *et al.* in 2020 show that the use of unsupervised methods such as clustering can identify suspicious transactions; they propose hybridization with combinatorial models to improve accuracy in detecting suspicious transactions [3]. As for Estevez *et al*, in 2018 they proposed an analysis of features important for detecting anomalies in digital transactions, with an emphasis on geographical and behavioral variables [4]. MIPs offer a rigorous representation of decision problems by integrating linear constraints and discrete variables; thus, Hansen and Jaumard in the 90s developed a mathematical program in financial contexts to model optimization decisions under uncertainties [5]; 3 decades later, Zhao and Hryniewicz advocated robust optimization approaches to secure transactions in high uncertainty environments [6]; Thus, Wang *et al.* in 2021 developed a PMNI to classify transactions as suspicious or not, based on dynamic thresholds linked to the user's habits, this model proved more efficient thanks to its integration with real-time data [7]. Also in 2021, Kim and Lee analyze transactional behaviors to identify anomalies, with a focus on geographic locations and amounts [8]. A year later, in 2022, Li and Liu, develop a

combination of PMNE with machine learning models (neural networks) to dynamically adjust constraints and improve accuracy while reducing computation times [9]. Other complementary methods for detecting fraud in mobile financial transactions have been developed, including ensemble approaches (bagging, boosting) to reinforce PMNI models [10]; and a technique combining combinatorial models and supervised learning to improve fraud detection [11]. Finally, Sadighian and Karimi recommend an analysis of security policies and their role in reducing fraud [12]. This review demonstrates the various contributions of Mixed Integer Programs to securing digital transactions, combining optimization techniques, behavioral analysis and machine learning. Although these models offer a solution for detecting and preventing suspicious transactions, they are based on a single-criteria parameter.

In this context, this paper proposes a new mixed integer program combining both discrete and continuous variables under several constraints: transaction cost, geographical location, type of device used to perform the transaction and its IP address, with the aim of capturing the true complexity of transactional systems by reducing classification errors linked to false positives (normal transactions classified as suspicious) and false negatives (suspicious transactions classified as normal). Multiple constraints make it possible to exploit the relationships between variables to obtain a robust, optimized mathematical program that improves accuracy, reduces errors and adapts easily to different user behaviors and transactional environments. This approach significantly enhances the security of e-Wallets.

3. Materials and Method

3.1. Model Formulation

The mixed integer program developed is designed to detect suspicious transactions in an electronic wallet (e-Wallet). The Fitness function aims to maximize the detection of suspicious transactions while minimizing false positives. Variables and constraints are defined to capture transactional characteristics such as amount, geographical location, device type and IP address.

❖ Variables type definition:

The MIP is composed of two types of variables:

Continuous variables, binary integer variables

- Binary variable

$$x_i = \begin{cases} 1 & \text{if a transaction is classified as suspect} \\ 0 & \text{otherwise} \end{cases}$$

$y_{ij} \in \{0,1\}$: Binary variable representing an anomaly detected for characteristic j in the transaction i

if $j = 1$: characteristic relates to amount of the transaction

if $j = 2$: characteristic relates to geographical location

if $j = 3$: characteristic relates to type of Peripheral

if $j = 3$: feature relates to IP address

- Continuous variables

$S_i \geq 0$: Transaction suspicion score i

$C_i \in \mathbb{R}^+$: Transaction cost i

❖ Function-Objective

The MIP objective function is a linear combination of successful detections and penalties for errors, weighted by suspicion scores and adjusted by priority coefficients.

These components are:

Suspicion score (S_i): score attribué à chaque transaction i

$\left(w \cdot S_i \cdot x_i\right)$: This term values suspicious transactions correctly detected by the model

$\left(\omega \cdot \left(1-x_i\right) \cdot F_i\right)$: This term penalizes misclassified transactions

with:

w : Weight that adjusts the importance of suspicious transactions in the objective function

ω : weight adjusting penalty for false negatives

F_i : False negatives: Suspicious transactions not detected ($x_i = 0$)

S_i : Transaction suspicion score i

x_i : Binary variable indicating transaction suspicion i

$$\text{Maximize } Z = \sum_{i=1}^{n}\left(w \cdot S_i \cdot x_i - \omega \cdot \left(1-x_i\right) \cdot F_i\right)$$

Note:

The weights w and ω control the balance between maximizing the detection of suspicious transactions and minimizing classification errors.

If w is high, the model will focus on anomaly detection.

If ω is high, the model will minimize false negatives.

This allows the objective function: (Z) ensure efficient and optimized detection as part of e-wallet security.

Constraints

Transaction amount constraint (for $j = 1 \Rightarrow y_{i1}$)

A transaction is considered suspicious if its cost C_i deviates significantly from the historical average of transactions for a given user.

$$y_{i1} = \begin{cases} 1 & \text{if } \left|C_i - \mu C\right| > \kappa_1 \cdot \sigma C \\ 0 & \text{otherwise} \end{cases}$$

With

μC : Average transaction cost per user

σC : Standard deviation of transaction values

κ_1 : Adjustable threshold factor.

Constraints on geographical location (for $j = 2 \Rightarrow y_{i2}$)

$$y_{i2} = \begin{cases} 1 & \text{if } D\left(\left(L_i, l_i\right), \left(\mu_L, \mu_l\right)\right) > \xi \\ 0 & \text{otherwise} \end{cases}$$

with:

L_i, l_i : Transaction latitude and longitude i

μ_L, μ_l : Average latitude and longitude of usual transactions

$D(.)$: Geographical distance.

ξ : Distance threshold $D(.)$

Device type constraints (for $j = 3 \Rightarrow y_{i3}$)

$$y_{i3} = \begin{cases} 1 & \text{si } p_i \notin P_{\text{approved}} \\ 0 & \text{otherwise} \end{cases}$$

with:

p_i : Peripheral

P_{approved} : All devices authorized for the user.

IP address constraints (for $j = 4 \Rightarrow y_{i4}$)

A transaction is considered suspicious if the A_i IP address does not correspond to an IP range authorized for the user

$$y_{i4} = \begin{cases} 1 & \text{si } A_i \notin A_{\text{authorized}} \\ 0 & \text{otherwise} \end{cases}$$

A_i : IP address used for the transaction

$A_{\text{authorized}}$: All authorized IP ranges.

Suspicion score

The suspicion score for a transaction i is a weighted combination of the anomalies detected.

$$S_i = \beta_j \cdot y_{ij}; \text{ where } j = \{1,2,3,4\}$$

For a transaction i , the suspicion score is:

$$S_i = \beta_1 \cdot y_{i1} + \beta_2 \cdot y_{i2} + \beta_3 \cdot y_{i3} + \beta_4 \cdot y_{i4}$$

β_j : Weight assigned to each j characteristic

Suspicious transaction classification constraint

Let θ : the predefined suspicion score threshold

$$x_i = \begin{cases} 1 & \text{if } S_i \geq \theta \text{ then the transaction is classified as suspicious} \\ 0 & \text{si non} \end{cases}$$

Non-negativity constraints

$$x_i \in \{0,1\}$$

$$y_{ij} \in \{0,1\}$$

$$C_i \in \mathbb{R}^+$$

$$S_i \in \mathbb{R}^+$$

$$\theta \in \mathbb{R}^+$$

The Mixed Integer Program is:

$$\max Z = \sum_{i=1}^{n} \left(w \cdot S_i \cdot x_i - \phi \cdot (1 - x_i) \cdot F_i \right) \quad (1)$$

s.c

$$S_i = \beta_j \cdot y_{ij};\ \text{with}\ j = \{1,2,3,4\} \tag{2}$$

$$x_i = \begin{cases} 1 & \text{if } S_i \geq \theta \text{ the transaction is classified as suspicious} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

$$x_i \in \{0,1\} \tag{4}$$

$$y_{ij} \in \{0,1\} \tag{5}$$

$$C_i \in \mathbb{R}^+ \tag{6}$$

$$S_i \in \mathbb{R}^+ \tag{7}$$

$$\theta \in \mathbb{R}^+ \tag{8}$$

with

$$y_{i1} = \begin{cases} 1 & \text{if } \left|C_i - \mu C\right| > \kappa_1 \cdot \sigma C \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

$$y_{i2} = \begin{cases} 1 & \text{if } D\left(\left(L_i, l_i\right), \left(\mu_L, \mu_l\right)\right) > \xi \\ 0 & \text{otherwise} \end{cases} \tag{10}$$

$$y_{i3} = \begin{cases} 1 & \text{if } p_i \notin P_{\text{otherwise}} \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

$$y_{i4} = \begin{cases} 1 & \text{if } A_i \notin A_{\text{authorized}} \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

This mathematical program enables accurate classification of suspicious transactions, optimizing resources and reducing false positives, while maintaining high detection capacity.

(1) is the fitness function whose main objective is to optimize anomaly detection by assigning a suspicion score S_i to each transaction i, while minimizing false positives and false negatives in the classification of transactions as suspicious ($x_i = 1$) or normal ($x_i = 0$). is the suspicion score assigned to each transaction i obtained by a weighted combination of the various anomalies detected (amount, location, device, IP). (3) and (4) are binary variables respectively indicating whether a transaction is classified as suspicious or not. (5) Binary variable representing an anomaly detected for characteristic j in transaction i. (6): continuous variable representing the cost of a transaction; (7): continuous variable representing the value of the suspicion score assigned to each transaction i; continuous variable defining the threshold value of the predefined suspicion score used to define the type of transaction i. (9), (10), (11) et (12): are binary variables indicating anomalies detected for amount, location, device and IP address respectively.

The mathematical program developed combines two main objectives:

Efficient anomaly detection: By maximizing suspicion scores for suspicious transactions. Reduce classification errors: By minimizing false positives and false negatives through penalties integrated into the objective function.

This combination of objectives is rarely seen in literature, where models often

focus solely on detection. The aim is to provide a balanced solution, suitable for financial systems where minimizing disruption to legitimate users is essential.

Study of the complexity of the Mixed Integer Program

The mathematical model proposed in section 3.1 is based on a Mixed Integer Program (MIP) to detect suspicious transactions in an e-Wallet system. This type of program combines continuous variables (transaction amounts) and discrete variables (binary indicators of suspicion) in an objective function optimized under several constraints. To study its complexity is to analyze the computational difficulty of finding an optimal solution.

MIP belongs to the NP-hard complexity class. This is due to the presence of continuous and discrete variables in the model, whereas in general cases, integer linear optimization problems require an exhaustive search in the space of discrete solutions. In addition, multiple non-trivial constraints such as transaction cost, location, type of device used for the transaction and IP addressing increase the dimensionality of the problem and make the solution space more complex.

In addition, certain key variables influence complexity: considering n: Total number of transactions (variables to be optimized), m: Number of constraints in the model, k: Number of discrete (binary) variables. The exhaustive search for possible solutions for k discrete variables in a MIP has an exponential complexity in k, *i.e.* $O\left(2^k\right)$.

Solving sub-problems for continuous variables with linear relaxation is feasible in polynomial time with simplex algorithms or the interior point algorithm. Thus, its total complexity is combined is $O\left(2^k \cdot P\left(n,m\right)\right)$ where $P\left(n,m\right)$ represents the solving complexity of a relaxed linear program. An exact resolution is feasible for moderate-sized data sets, but quickly becomes impractical on a large scale without recourse to heuristics or relaxation.

3.2. Experimentation

❖ Simulation and development environment

- Language: Python 3.13.1
- Library: Pulp, pandas, Numpy et matplotlib

Simulation data are presented in Table 1.

Datasets: the dataset is a CSV file of 10,000 records with the following information: Transaction_ID, Value, Latitude, Longitude, Device_Type, adress_IP and suspicion score thresholds for the first 20 lines of the dataset are shown in Table 2.

3.3. Result: Analysis and Discussion

The results of the various experiments are presented below.

The histogram of transaction amounts in Figure 1 reveals a significant concentration around a mean of 513.99 monetary units, with a standard deviation of $\sigma = 118.45$ indicating that most transactions fall within a reasonable range around this average. The shape of the histogram seems close to a slightly asymmetric

Table 1. Simulation data.

Labelle		Value
Transaction costs	Average normal costs	500
	Standard deviation of normal costs	100
	Suspicion threshold	800
Geographical location	Average latitude	40.7128
	Average longitude	−740,060
	Distance threshold	0.15
Device type (P)	P = {mobile, Desktop} authorized	
IP Adress (A)	Permitted ranges	192.168.xxx.xxx
Suspicion Scores	$S_i = \beta_1 \cdot y_{i1} + \beta_2 \cdot y_{i2} + \beta_3 \cdot y_{i3} + \beta_4 \cdot y_{i4}$	
	β_1	0.4
	β_2	0.3
	β_3	0.2
	β_4	0.1
Suspicion threshold	If $S_i \geq \theta$ then the transaction is suspicious	
	θ	0.5

Table 2. Data sets for the first twenty transaction records.

Transaction ID	Costs	Latitude	Longitude	Device Type	IP Adress	S_i
1	801.2969732	41.58753247	−72.86768319	unknown	203.0.113.0	0.6
2	801.2969732	41.93416157	−73.42255664	unknown	203.0.113.1	0.51
3	558.2832761	40.72284343	−74.01220233	desktop	192.168.0.231	0.2
4	467.3191242	40.65286289	−74.10250859	mobile	192.168.1.93	0.3
5	597.8201395	40.58191348	−74.02470116	unknown	192.168.0.145	0.57
6	453.1552046	40.6786535	−74.14553311	desktop	192.168.1.12	0.19
7	390.1733403	40.77647638	−74.00997866	mobile	192.168.0.160	0.26
8	438.3373814	40.81715879	−73.95068322	mobile	192.168.0.72	0.31
9	491.4919424	40.71810215	−74.07987681	mobile	192.168.1.35	0.2
10	451.3347954	40.92154411	−73.88329695	mobile	192.168.1.109	0.0149
11	656.1670221	40.88291484	−73.90632408	mobile	192.168.0.188	0.19
12	590.5311413	40.67007905	−73.97584051	desktop	192.168.1.21	0.3
13	355.6560898	40.76929776	−74.03274496	desktop	192.168.1.223	0.2
14	366.7920232	40.57240756	−73.89867227	mobile	192.168.0.16	0.18
15	564.0750157	40.82213589	−74.04541478	mobile	192.168.1.236	0.2

Continued

7	351.5469784	40.5878288	−73.8353967	mobile	192.168.1.100	0.31
17	519.2390329	40.61876406	−74.14057302	mobile	192.168.1.146	0.23
18	380.3300734	40.64415176	−73.90763125	unknown	192.168.0.102	0.3
19	563.1424988	40.91199458	−73.98919467	desktop	192.168.0.127	0.2
20	480.9881736	40.52645363	−74.02778645	desktop	192.168.0.5	0.2

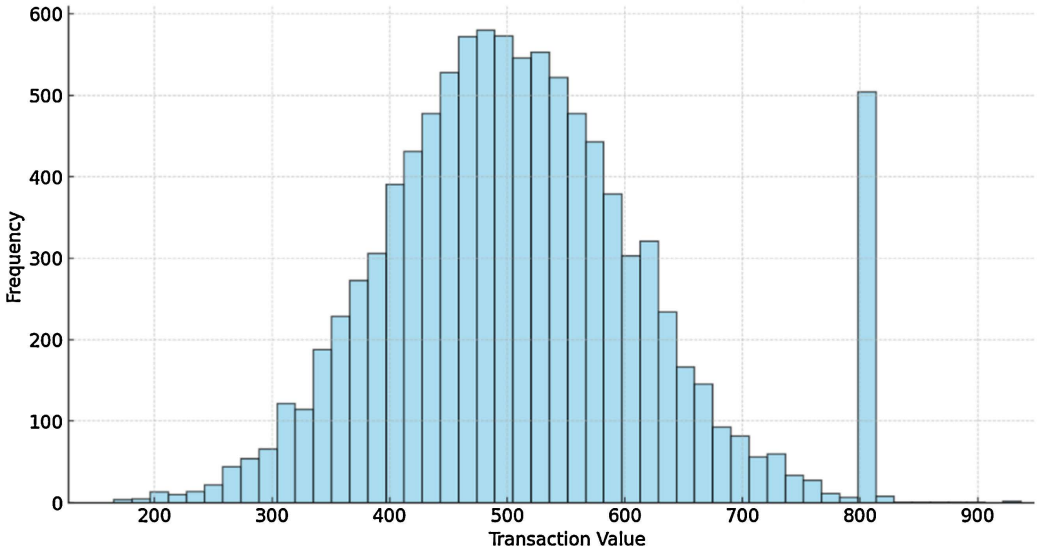

Figure 1. Transaction cost distribution.

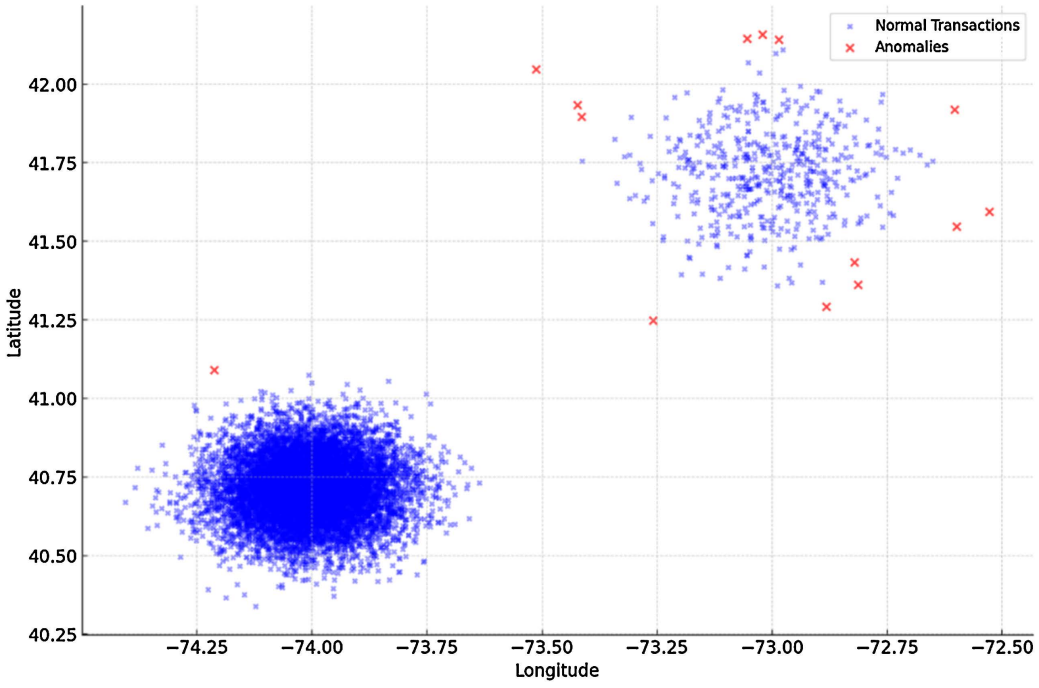

Figure 2. Geographical distribution of normal and suspicious transactions.

normal distribution. The concentration around the means suggests stable and predictable transaction behavior for most users. On the other hand, analysis of the extreme minimum and maximum values: [165.28, 936.79] could signal activity in unexpected regions. Indeed, the presence of high amounts (close to the maximum) may signal atypical transactions or merit specific attention in a security context. This could indicate risks, such as unusual transfers or malicious activities like ceiling attacks. However, concentration around the mean suggests stable and predictable transactional behavior for most users.

The visualization of geographical distribution in Figure 2 shows two distinct categories: Normal transactions are distributed (blue color) over a well-defined set of geographical areas, probably corresponding to regions of regular activity for users, these geographical clusters could correspond to urban areas or densely populated regions. Suspicious transactions (red color) are located outside the normal clusters, indicating transactions initiated from unusual geographical locations in relation to the user's historical behavior, or locations manipulated to mask the true origin of the transaction (use of proxies or VPNs). In addition, the concentration of transaction anomalies in a single region may indicate a coordinated fraud attempt.

Normal transactions follow a logical, dense distribution, aligned with expected activity zones, while suspicious transactions appear more scattered or concentrated in isolated areas:

- Isolated suspicious clusters: Several anomalies in the same isolated region may indicate coordinated fraud.
- Isolated single points: Isolated single points: An isolated anomaly may reflect a one-off incident requiring investigation.

Figure 3's analysis of device types shows a dominance of transactions carried out via mobile devices among normal transactions, followed by desktop and a significant percentage of unidentified devices (Unknown). This reflects modern usage patterns where smartphones dominate digital payments. A notable proportion remain classified as "unknown" and are associated with transactions classified as suspicious in the majority; however, some may result from misconfiguration of legitimate devices due to missing metadata. Anomalies show no use of mobile devices, suggesting that attacks are targeting fewer common devices or exploiting less monitored environments from proxies or VPNs to mask their identity? The non-involvement of mobile devices in the anomalies suggests that mobile transaction security systems are more robust, or that attackers are avoiding these devices.

Figure 4 shows a uniform distribution of anomalies across multiple IP addresses, where each address appears only once in the suspect data. This raises interesting questions about the nature and scope of suspicious transactions:

- Isolated attempts: The fact that the same IP only appears once could indicate one-off fraud attempts or non-recurring users.
- Address diversity: The use of a variety of IP addresses may reflect the use of masking tools such as VPNs, proxies, or bots configured to generate connections from different IP addresses.

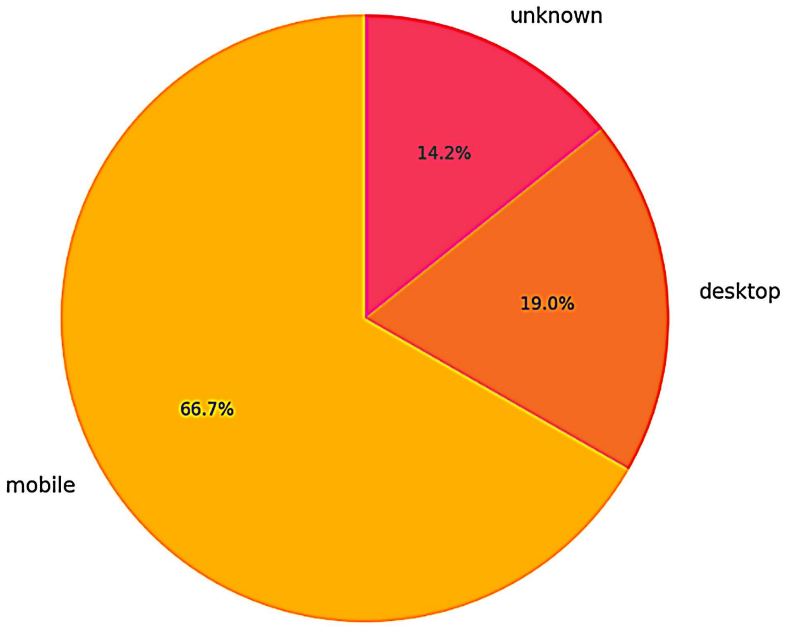

Figure 3. Distribution of device types.

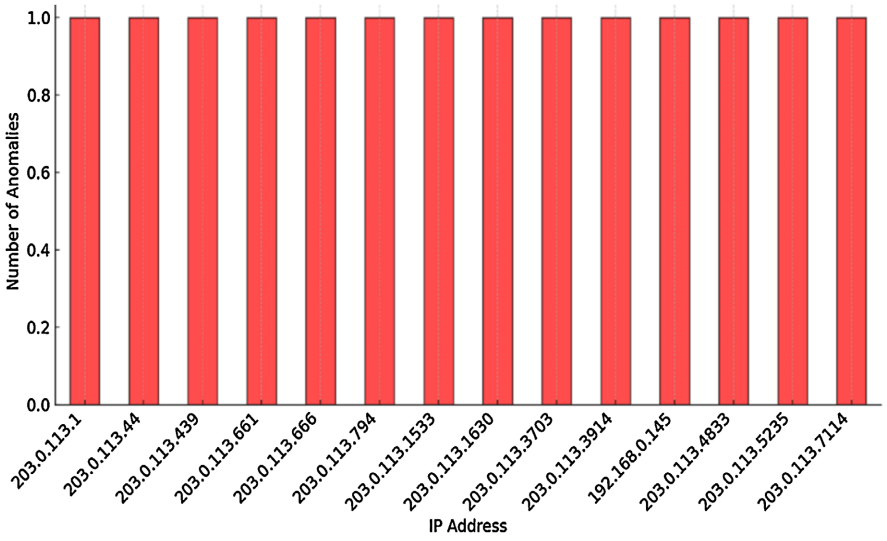

Figure 4. Distribution of suspect IP addresses associated with detected anomalies.

The typology of suspect IP addresses appears to belong to local ranges (192.168.0.145), while others belong to public ranges (203.0.113.x). This may indicate either a false positive for the IP address (192.168.0.145) or an attempt to mask the origin of the type of device used to carry out the transaction via shared public IP addresses, hence the lack of knowledge of the devices used.

A false positive refers to a transaction or activity that is wrongly considered suspicious or malicious, even though it is legitimate. When it comes to IP addresses, several factors can contribute to these errors, affecting both the user experience and the effectiveness of security systems among other things: if users connecting via VPNs or shared proxies may have IP addresses associated

with fraudulent behavior in which case no legitimate transaction may be falsely reported if the IP address is listed as suspicious or if ISPs frequently reassign dynamic IP addresses, which can link suspicious past activities to innocent current users, this can lead to new transactions being classified as suspicious. The consequence of false positives is a degraded user experience: transactions are blocked or delayed, leading to a loss of confidence in the service. One solution to combat false positives will be to use reliable IP address databases and update them regularly to avoid errors due to obsolete information, or implement systems capable of detecting anomalies dynamically, considering changes in IP usage.

The Mixed Integer Program (MIP) accurately identifies suspicious transactions by integrating multiple criteria. It offers better prioritization of resources by reducing unnecessary expenditure on false positives. In addition, the mathematical program can be adjusted to meet the specific needs of an e-Wallet system. However, in terms of computational complexity, MIP can be resource-intensive for large-scale systems, and the robustness of the model will depend on the quality and completeness of the data used, since attackers are constantly modifying their strategies, which will entail regular revision of MIP. By exploiting its modeling and optimization capabilities, it is possible to create an efficient and sustainable mathematical security program, while maintaining smooth and frictionless user experience.

4. Conclusion

In this article, we propose an approach based on a Mixed Integer Program to enhance e-Wallets security by detecting suspicious transactions. This model is based on a rigorous mathematical formulation incorporating constraints linked to transaction amounts, geographical location, device type and IP address. The use of Mixed Integer Programs offers flexibility to model complex environments while guaranteeing an optimal solution. The results obtained in our simulations have shown that the proposed model significantly reduces the false positive rate while maintaining a high capacity to detect suspicious transactions. Compared with other heuristic or statistical approaches, the Mixed Integer Program proved particularly effective in environments with variable user behavior and heterogeneous data. This work represents an important contribution to the security of digital financial systems, responding to the growing need to protect users from digital fraud. Although the results are promising, several avenues of improvement can be envisaged to enrich the proposed model and increase its effectiveness in broader contexts. In this case, the integration of machine learning algorithms could enable the refinement of constraint thresholds in real time, and better adaptation to changes in transactional behavior.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Jha, S., Pathak, R. and Verma, K. (2019) Fraud Detection in Digital Payment Systems: A Review. *Computers & Security*, **89**, Article ID: 101675.

[2] Gupta, K., Singh, V. and Mishra, P. (2020) Secure Payment Systems: Challenges and Opportunities in e-Wallet Technology. *Journal of Financial Technology*, **45**, 15-23.

[3] Nguyen, H.T., Dang, M.L. and Tran, P.Q. (2020) Unsupervised Learning for Anomaly Detection in Payment Systems. *Expert Systems with Applications*, **161**, Article ID: 113731.

[4] Estevez, P.A., Tesmer, M. and Perez, C.A. (2018) Feature Selection for Anomaly Detection in e-Wallet Transactions. *Pattern Recognition*, **79**, 237-249.

[5] Hansen, P. and Jaumard, B. (1990) Algorithms for the Constrained Assignment Problem. *Journal of Optimization Theory and Applications*, **64**, 445-467.

[6] Zhao, Y. and Hryniewicz, O. (2019) Robust Optimization for Secure Payment Systems. *Cybersecurity Journal*, **10**, 145-163.

[7] Wang, X., Zhao, Y. and Chen, L. (2021) Mixed-Integer Programming Models for Fraud Detection in Digital Wallets. *Applied Mathematics and Computation*, **398**, Article ID: 125655.

[8] Kim, H.J. and Lee, J.S. (2021) Transaction Behavior Analysis for e-Wallet Security. *Cybersecurity Journal*, **10**, 145-163.

[9] Li, Z. and Liu, T. (2022) Artificial Intelligence-Enhanced Optimization Models for Fraud Detection. *IEEE Transactions on Neural Networks and Learning Systems*, **33**, 4567-4580.

[10] Ho, T.K. and Basu, M. (2019) Ensemble Learning for Fraud Detection. *Machine Learning Applications*, **3**, 85-102.

[11] Meidan, Y. and Klein, R. (2020) Hybrid Models for Anomaly Detection in e-Wallet Transactions. *Artificial Intelligence in Finance*, **12**, 287-305.

[12] Sadighian, P. and Karimi, M. (2021) Security Policies and Anomaly Detection for Digital Wallets. *International Journal of Information Security*, **20**, 49-68.