



## Fraudulent Transactions in Digital Payment System

*Dukka Gayatri*

*Student, Rajam, Vizianagaram, 535127, Andhra Pradesh, India.*

### ABSTRACT

India is going to become cashless. Indian government launched digital India Campaign to reduce dependency of Indian economy on cash and prevent from money laundering. To make cashless India and increasing trends in using digital payment system various Payment methods are emerging and developing. India is a developing country and maximum area is rural and most shocking is computer literacy is only 6.5-7.0% then different questions arises that implementation of digital payment system. This term paper is making focus on the problems of digital payment system (fault transactions) in India and effects of the system in people This paper presents an exploration of fault-tolerant digital transaction systems tailored to the specific needs of people. This paper is also going to apply multiple techniques in machine learning to the problem of fault transactions over limited area of people. We aim to demonstrate how the machine learning techniques can be used to rectify the most general problems which are became common to the current generation.

**Keywords:** Fraudulent transaction, digital transaction, logistic regression, regular updates, user support, public protection

### 1. Introduction

Mobile payment has gained significant popularity as a mainstream payment method, leading to a high volume of transactions on online trading platforms. Unfortunately, this popularity also attracts criminals who exploit the complex network environment to commit fraud. Such fraudulent activities not only harm consumers but also impede the healthy growth of the online economy. Consequently, effective transaction fraud detection becomes a vital tool in combating network transaction fraud. Traditional fraud detection approaches primarily rely on statistical and multi-dimensional analysis techniques. However, these verification based methods struggle to uncover the underlying patterns in transaction data, limiting their effectiveness. On the other hand, big data technology and machine learning algorithms offer efficient solutions for detecting transaction fraud. Machine learning, particularly when applied to large datasets, can capture important features that traditional statistical methods fail to describe. By utilizing suitable machine learning techniques, we can build models based on existing transaction data to detect network transaction fraud, thereby mitigating associated losses.

### 2. Literature Survey

**In paper [1].** It was developed to eradicate the hoaxers and attackers to develop fraudulent transactions and fool people for some amount of money. As the online payment platforms became high volume, fraudulent activities became common which harms not only consumers but also entire economy. In this system, an attempt is made to develop a machine learning model to identify fraudulent transactions in a transaction's dataset. Though different algorithms such as Decision Trees, Naive Bayes Classification, Least Squares Regression, Logistic Regression and SVM are used, the algorithm that demonstrates highest accuracy in results is used.

**In paper [2].** Mobile payment systems are becoming more popular due to the increase in the number of smartphones, which, in turn, attracts the interest of fraudsters. Extant research has therefore developed various fraud detection methods using supervised machine learning. However, sufficient labeled data are rarely available and their detection performance is negatively affected by the extreme class imbalance in financial fraud data. The purpose of this study is to propose an XGBoost-based fraud detection framework while considering the financial consequences of fraud detection systems. The framework was empirically validated on a large dataset of more than 6 million mobile transactions. To demonstrate the effectiveness of the proposed framework, we conducted a comparative evaluation of existing machine learning methods designed for modeling imbalanced data and outlier detection. The results suggest that in terms of standard classification measures, the proposed semi-supervised ensemble model integrating multiple unsupervised outlier detection algorithms and an XGBoost classifier achieves the best results, while the highest cost savings can be achieved by combining random under-sampling and XGBoost. Methods.

**In paper [3].** In this study, a method was developed that detects and prevents users who may harm the business in various ways, such as stealing, copying or leaking sensitive data produced and/ or stored in the mobile application, accessing personal data, exploiting system vulnerabilities, and using the system with a stolen card or account. The developed method was used in Kentkart, a smart public transportation developer and provider company. Kentkart, a company based in Turkey, provides mass transit systems in many countries. The usage data of the smart transportation mobile application of the company

used in USA/Kansas were employed. The purpose of the method was to identify fraudulent users (such as users who abuse application features and promotions, generate fake tickets, distribute or sell them, violate the personal rights of non-fraudulent users, make purchases with stolen credit/debit cards, etc.). In order to prevent fraud, users identified as fraudulent were automatically blacklisted per the company's management policy, thus preventing them from entering the system.

**In paper [4]**, Now a days Digital transactions are rapidly increasing as it results in increasing online payment frauds too. In fact, according to the Reserve Bank of India, comparing March 2022 to March 2019, digital payments have risen in volume and value by 216% and 10%, respectively. People are starting to go all-in with digital transactions, but one can't deny the security issues that loom, and know-how when it comes to online payments. Few years ago, we could have barely seen the online payment, but today UPI payment QR code installed at doorstep. This invited the hoaxers and attackers to develop fraudulent transactions and fool people for some amount of money. Fortunately, the online transactions are monitored and hence could be analysed using the latest tools. In this system, an attempt is made to develop a machine learning model to identify fraudulent transactions in a transaction's dataset.

**In paper [5]**. This paper is divided into seven sections. Introducing electronic payments and its related study, which is already discussed above, is the Section 1. Section 2 will include an overview of the existing system and related work. The Section 3 is the description of the proposed conceptual design. Section 4 presents how the model would be implemented

---

### 3. Methodology

Here's a methodology flow for handling fraudulent transactions in digital payment systems:

#### 1. Transaction Initiation:

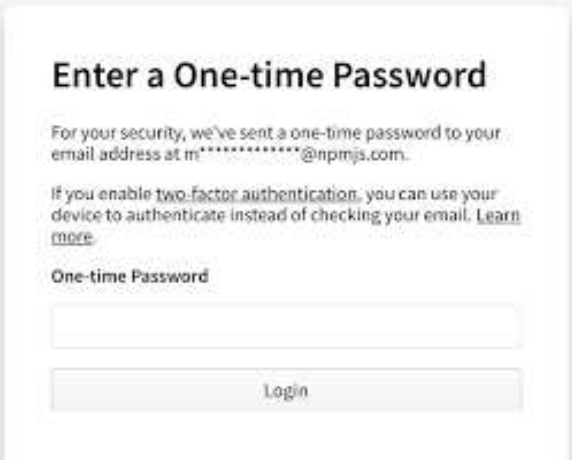
- Data Collection: Record transaction details (date, time, amount, payment method, device information, IP address, geolocation, etc.).
- Risk Assessment: Assign a risk score based on factors like transaction amount, geographic location, device history, behavioral patterns, and known fraud patterns.

#### 2. Fraud Screening:

- Rule-Based Filters: Apply predefined rules to flag suspicious activity (e.g., unusual transaction amounts, multiple attempts, blacklisted IP addresses).
- Machine Learning Models: Analyze transaction data to identify anomalies and predict fraud likelihood.
- Velocity Checks: Monitor transaction frequency to detect potential fraud attempts.

#### 3. Authentication and Verification:

- Multi-Factor Authentication (MFA): Require additional verification for high-risk transactions (e.g., one-time passwords, biometrics).
- Address Verification Service (AVS): Match billing and shipping addresses for card-based transactions.
- Card Verification Value (CVV): Verify the security code on the back of credit/debit cards.
- 3D Secure: Implement a two-factor authentication protocol for online payments.



The image shows a login interface with the following elements:

- Title:** Enter a One-time Password
- Text:** For your security, we've sent a one-time password to your email address at m\*\*\*\*\*@npmjs.com.
- Text:** If you enable two-factor authentication, you can use your device to authenticate instead of checking your email. [Learn more](#)
- Label:** One-time Password
- Input:** A text input field for entering the one-time password.
- Button:** A button labeled "Login".

#### 4. Review and Decision:

- **Manual Review:** Analyze high-risk transactions flagged by automated systems.
- **Decision:** Approve, decline, or hold the transaction based on risk assessment and review.



#### 5. Post-Transaction Monitoring:

- **Transaction Monitoring:** Track transaction patterns for anomalies and potential fraud after approval.
- **Chargeback Management:** Handle customer disputes and claims of unauthorized transactions.
- **Feedback Loop:** Incorporate feedback from chargebacks and fraud investigations to refine risk models and detection techniques.



#### 6. Reporting and Analytics:

- **Generate reports:** Track fraud trends, identify weaknesses, and measure the effectiveness of fraud prevention measures.
- **Share insights:** Collaborate with law enforcement and other institutions to combat fraud.

#### Additional Considerations:

- **Biometric Authentication:** Utilize fingerprint, facial, or voice recognition for enhanced security.
- **Tokenization:** Replace sensitive payment card data with unique tokens to reduce exposure.
- **Encryption:** Protect data in transit and at rest to prevent unauthorized access.
- **User Education:** Promote awareness of common scams and best practices for online payment security.
- **Regular Updates:** Keep systems and security measures up-to-date to address evolving threats.

#### 4. Results and Discussion

Method	AUC	F1	ACC	Precision	Recall	Execution Time
K-NN	0.9313	0.1588	0.9881	0.0873	0.8744	4581.4
SVM	0.6543	0.4655	0.9991	0.9474	0.0386	12082.9
RF	0.8961	0.8394	0.9996	0.9146	0.7756	1196.2
XGBoost	0.9350	0.8410	0.9998	0.8794	0.8059	207.0
RUS+K-NN	0.8996	0.0405	0.9475	0.0207	0.8516	145.3
RUS+SVM	0.8344	0.0321	0.9431	0.0164	0.7255	1041.5
RUS+RF	0.9933	0.2305	0.9914	0.1303	0.9947	12.6
RUS+XGBoost	0.9955	0.2812	0.9934	0.1637	0.9976	2.4

We have proposed an XGBoost-based fraud detection framework while considering the financial impact of fraud detection. The findings from this study make several noteworthy contributions to the current literature. First, the XGBoost model was combined with under-sampling to effectively address the problem of extreme class imbalance and avoid overfitting. Second, to fully exploit the large amount of underlying data, unsupervised outlier detection methods were integrated into the XGBoost-based model. The comparison of the XGBoost-based fraud detection performance with various state-of-the-art machine learning methods confirmed that we have found a cutting-edge solution for fraud detection in mobile payment systems. Our findings also suggest a role for the proposed model in promoting cost savings of fraud detection systems. Taken together, our results strongly argue against a major role of single machine learning methods and unsupervised outlier detection methods in fraud detection of mobile payment transactions, implying that ensemble XGBoost-based methods are preferable.

#### 5. Conclusion

In conclusion, the application of machine learning algorithms in detecting and preventing fraudulent transactions in digital payment systems represents a significant leap forward in enhancing security and safeguarding financial transactions. Through the analysis of vast amounts of data, these algorithms can identify patterns, anomalies, and potential risks in real-time, allowing for swift and proactive response to mitigate the impact of fraudulent activities. By leveraging advanced techniques such as anomaly detection, supervised learning, and ensemble methods, machine learning models can adapt and evolve to stay ahead of evolving fraud tactics. The continuous learning nature of these algorithms enables them to refine their accuracy over time, ensuring a robust defence against emerging threats. As the digital landscape continues to evolve, the role of machine learning in fraud detection becomes increasingly indispensable. However, it is crucial to recognize that no system is entirely foolproof, and a holistic approach combining advanced technology with rigorous cybersecurity measures, user education, and regulatory frameworks is essential to create a resilient defence against fraudulent transactions in digital payment systems.

#### REFERENCES

- [1] Ms. Kishori Dhanaji Kadam, Ms. Mrunal Rajesh Omana, Ms. Sakshi Sunil Neje, Ms. Shraddha Suresh Nandai. 2023. "Online Transactions Fraud Detection using Machine Learning"
- [2] Ahmed, M., Mahmood, A. N., & Islam, M. R. (2020). "A survey of anomaly detection techniques in financial domain"
- [3] Abdallah, A., Maarof, M. A. & Zainal, A. (2021). "Fraud detection by machine learning algorithms: A case from a mobile payment system".
- [4] E. Kim et al., "Champion-challenger analysis for fraud detection (2020)". Expert Systems with Applications.
- [5] Varun Kumar K S, Vijaya Kumar V G, Vijay Shankar A, Pratibha (2023) "Fraud Detection using Machine Learning Algorithms"