Multidisciplinary Reviews

REVIEW ARTICLE
Published Online: November 17, 2025
https://doi.org/10.31893/multirev.2026280

# Mobile payment fraud detection in UPIs through machine learning techniques: A systematic review

**Naga Bhavani Chakka**[a] | **Shaiku Shahida Saheb**[a]

[a]VIT-AP School of Business, VIT-AP University, Amaravathi, Andhra Pradesh, India.

**Abstract** The Unified Payment Interface (UPI) has transformed the digital payments landscape in India by providing a method for safe, instantaneous, and user-friendly financial transfer. With some arguably limited oversight, UPI was adopted quickly, but unfortunately, along with its growth, the landscape is littered with new forms of advanced fraud. Therefore, this study presents a systematic analysis of UPI fraud from 2016-2025, detailing common forms of fraud such as fake mobile apps, phishing, QR code attacks, pony payment requests, and fraud involving KYC regulation. Additionally, this paper explores advanced machine learning and deep learning models for fraud detection. Some of the models we explored include convolutional neural networks (CNNs), long short-term memory (LSTM) neural networks, and detection accuracies of up to 99.74%. Other effective models include support vector machines (SVMs), random forests, and XGBoost since they are able to classify flagged transactions as nonauthorized with high levels of precision. We see that augmented and integrated systems with biometric authentication and real-time monitoring and reporting become a layered defense against new threats to fraud. The study also highlighted the rise in autopay fraud to drive the need for continuous innovation in fraud detection, undermining those who have been manipulating UPIs and digital payments since 2019. There is a need to further incorporate supervised ML, deep learning, and gradient boosting with existing banks' processes for recovery and detection tools for malpositioning to further the financial safety of UPI users and develop a competent payment system for UPIs and their clients.

**Keywords:** digital payments, security, scams, autopay fraud, gradient boosting, LSTM

## 1. Introduction

Electronic payments have been fundamentally revolutionized by the rapid growth of technology (Ahmed & Sreeju, 2020), and digital platforms such as the Unified Payments Interface (UPI) have been essential in reshaping the financial environment (Mishra et al., 2023). A global surge in digital transactions has been spurred by the increasing utilization of mobile and contactless payments (Purohit & Purohit, 2024), which has been compounded by the COVID-19 outbreak (Kannan & Vasantha, 2021). The UPI, which was founded by the National Payments Corporation of India (NPCI) (Badak et al., 2023), promises unsurpassed efficiency and simplicity by facilitating real-time financial transfers via mobile devices. With 68% of payment transactions by volume, it has become the backbone of digital transactions in India. Although UPI has made payments simpler and encouraged financial inclusion (Rastogi et al., 2021), its broad usage has also highlighted severe security issues that need to be remedied immediately. The entire transaction value of the worldwide digital payments sector is predicted to reach US$16.62 trillion by 2028, indicating a compound annual growth rate (CAGR) of 9.52% from 2024--2028 (Bhujel, 2024).

The Unified Payments Interface (UPI) system in India has become a target for scammers and fraudsters (Edburg et al., 2024), leading to a major surge in fraudulent operations (Purohit & Purohit, 2024) . Government records reveal a surge in UPI fraud cases from 77,000 to over 95,000 in the financial year ending April 2023 (Ma et al., 2009), (Senturk et al., 2017). This spike in fraudulent activity is akin to phishing emails and texts that have troubled people in the past (Alabdan, 2020). Concerns have been expressed concerning the likelihood of fraud when people receive money via UPI (Shree et al., 2021), with criminals leveraging the system to fool unsuspecting victims (Kumar, 2025) Various types of UPI scams have been detected (Gupta et al., 2018), including receiving bogus payments or transfer requests and illegal access to UPI accounts by fraudsters (Niranjanamurthy & Chahar, 2013).

The government has made efforts to address these challenges by collecting data on UPI payment fraud (Chandra Agarwal et al., 2024) and establishing the Central Payments Fraud Information Registry (CPFIR). Additionally, social engineering programs connected to UPIs have grown increasingly widespread in India (Jain, 2023), resulting in considerable fraud concerns in quick payments (Tulsi & Patil, 2023). Given the increasing number of UPI fraud incidents (Gupta et al., 2023), people must remain attentive and take preventative steps to protect themselves from becoming victims of fraudulent operations (Atkins & Huang, 2013). Reporting any suspicious transactions to the bank quickly is vital since the bank may be able to reimburse losses according to standards established by the Reserve Bank of India (Logeshwaran, 2022), (Marquez-Chamorro et al., 2018). As the popularity of UPI transactions continues to expand

 Received: May 6, 2025 | Accepted: September 13, 2025

(Kumar & Unnisa, 2024), it is vital for consumers to be knowledgeable about possible fraud threats and implement best practices to preserve their financial information and assets (Hoffmann & Birnbrich, 2012). Strong authentication protocols, cutting-edge encryption technologies (Kumar et al., 2022), and real-time transaction monitoring are just a few of the solutions that academics and industry professionals have offered to solve these challenges (Verma et al., 2017). Unauthorized access has been effectively prevented by incorporating biometric authentication methods such as fingerprint and iris recognition (Arepalli et al., 2024). Proactive fraud identification and prevention are also made feasible by the expanding use of machine learning (ML) and deep learning (DL) algorithms to study user behavior and transaction patterns (Arepalli et al., 2024; Karthick et al., 2024). By ensuring data integrity and scalability, cryptographic advances such as weighted hyperbolic curve cryptography (WHCC) greatly increase transaction security (Toral-Cruz et al., 2017).

This article looks at the security issues in the UPI system and how modern technologies and layered security methods can strengthen it. Moreover, educating users and working with other countries is key to tackling new threats. AI models such as LSTM and CNN help keep transactions safe.

This study was inspired by the growing number of people using online payments and the increase in UPI scams that came with it. As more people rely on the internet, weaknesses in the system have led to more fraud. The goal is to find smart, effective ways to make digital payments safer.

## 2. Related Literature Review

### *2.1. Conceptual Literature Review*

#### *2.1.1. UPI history*

The UPI, designed by the NPCI and debuted in April 2016, is a real-time payment system (Gupta et al., 2024) that allows users to connect various bank accounts to a single mobile app for seamless financial transfers and merchant payments. Built on the Immediate Payment Service (IMPS) platform, it offers immediate payments 24/7. Its key benefit is interoperability (Obaid et al., 2019), enabling quick money transfers between multiple banks via a unique UPI ID linked to the user's bank account, ensuring safe and direct transactions (Mohapatra, 2017). The system leverages two-factor authentication, integrating MPIN and OTP for better security (Gupta & Xia, 2018). Additionally, UPI APIs allow app integration for direct bank payments (Bhatia-Kalluri & Caraway, 2025), with features including QR code scanning for rapid transactions (Chohan et al., 2022).

#### *2.1.2. UPI usage statistics*

The UPI has altered digital payments in India, becoming the most popular real-time payment system. The transaction volume exploded from 92 crores in FY 2017--18 to 13,116 crores in FY 2023--24, increasing at an annual rate of 129%. In only the first five months of FY 2024--25, the volume surpassed 7,062 crores. Similarly, transaction values climbed from ₹1 lakh crore to ₹200 lakh crore at a phenomenal 138% annual growth rate, with ₹101 lakh crore recorded between April and August 2024. The simplicity and broad acceptance of UPIs by banks and fintech firms have fueled their popularity among millions of consumers. (Source: www.npci.com Up to 2024 August 31). The statistics show a substantial increase in UPI fraud: 7.25 lakh cases equal to Rs 573 crore were recorded in FY 2022-23, increasing to 13.42 lakh cases totaling Rs 1,087 crore in FY 2023-24. By September 2024-25, 6.32 lakh fraud instances had already been reported, amounting to Rs 485 crore (Suman, 2024). Notably, 27 nations globally have implemented UPIs, including recent adopters such as Sri Lanka, France, and Singapore. Phone Pe holds the market lead with a 46% share, followed by Google Pay at 36% and Paytm at 13%. UPI Lite, particularly via Paytm, has gained traction, processing over 10 million transactions monthly. The State Bank of India leads with a share of 2.52 billion transactions in Q3 2023. Nevertheless, UPIs' growth is marred by challenges, with over 95,000 fraud incidents reported in the financial year 2023 (Vidani, 2024).

Figure 1 shows the UPI (Unified Payment Interface) payment system architecture. Essentially, it explains how multiple mobile applications, such as online banking (Kumar, 2025), *99# USSD services or third-party apps connect to banks via standard interfaces provided by payment service providers (PSPs) (Mallik et al., 2020). A central mapper containing account numbers and IFSC codes is part of the NPCI (National Payments Corporation of India) interface, which is the focal point of the system (Madwanna et al., 2021). By linking to a Central Repository that is linked to many payment systems (AEPS, UPI, IMPS, Rupay, E-com, and ECS), a single ecosystem is formed that permits seamless digital transactions across different banks and payment platforms (Ramesh et al., 2020). It is essentially a comprehensive framework that allows customers to securely and seamlessly make digital payments via any bank or payment app of their choice (Au & Kauffman, 2008).

Figure 2 shows the flow of transactions between different organizations engaging in digital payments, which represents the high-level architecture of the Unified Payments Interface (UPI) system. The consumer (payer) commences the process by employing a mobile application that their payment service provider (PSP) has made accessible (Kakade & Veshne, 2017). The VPA Management Service replies with the VPA creation confirmation after the user establishes a Virtual Payment Address (VPA) via this app (Yang & Lee, 2019). An option is for the customer to use the app to scan a QR code, which triggers the QR Code Generator/Scanner Service to process the information and supply the appropriate data to commence a payment (Eren, 2024).

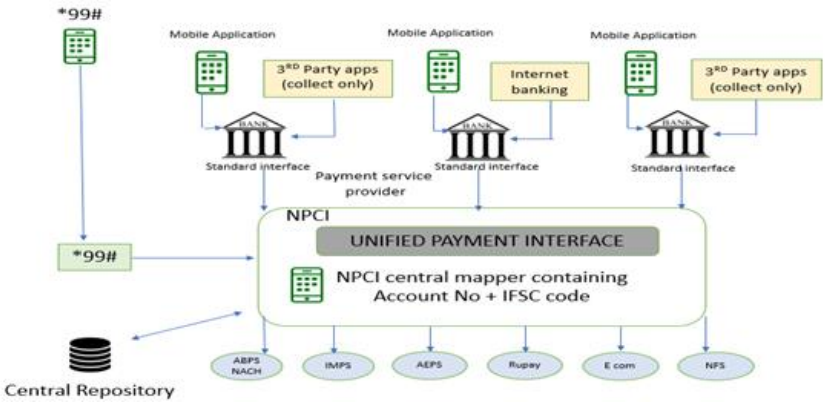


**Figure 1** UPI architecture. *Source:* Gochhwal (2017) and Scopus Database.

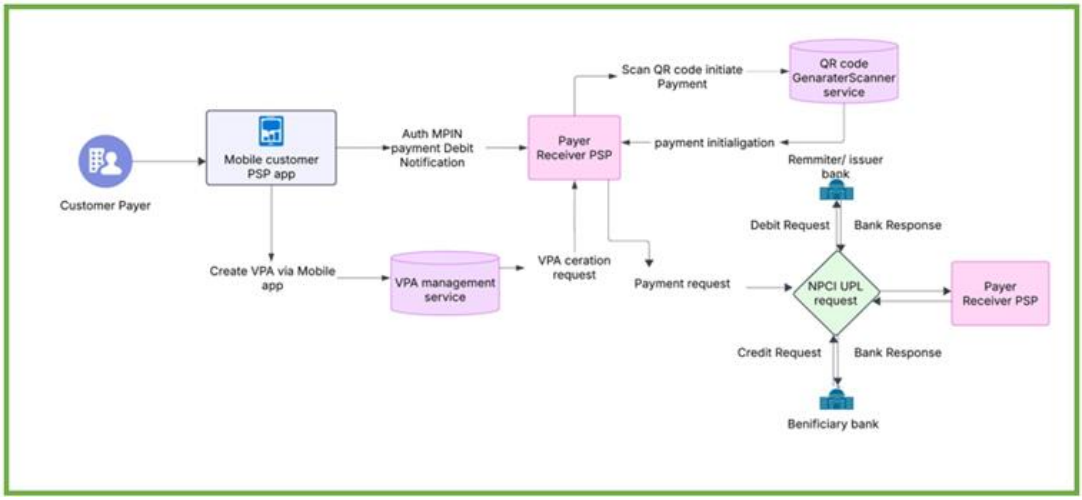


**Figure 2** UPI payment system workflow. *Source:* Mittal (2023) and Scopus Database.

The PSP initiates the payment by sending a request to the NPCI UPI network, which is responsible for conducting the transaction (Faccia, 2023). A debit request is transmitted by the UPI network to the payer's (remitter's) bank for verification (Ashok & Hallur, 2023). To validate the transaction, the network simultaneously queries the payee's bank for the client's details (Kousaridas et al., 2008). As the payee's bank reviews and confirms the payee's information, the payer's bank responds by allowing or refusing the debit request (Braithwaite, 2024).

The beneficiary bank receives a credit request from the NPCI UPI network to conclude the transaction after successful validation from both banks (Bera & Li, 2024). After that, a payment debit response is delivered to the payer's PSP, alerting the customer whether the transaction was successful or not. A smooth and secure movement of data and money between the customer, PSP, banks, and the UPI network is assured by this approach (Maharana, 2024).

## 3. Objectives and Methodology

The researcher designed the following objectives:

1. To describe the sophisticated deception techniques that are being used in mobile payments through UPI
2. To analyze various machine learning techniques for fraud detection in mobile payments via UPI

This systematic literature review covers documents from 2016 to 2025. Databases (IEEE Xplore, Scopus, SpringerLink) were queried via the terms “UPI fraud,” “machine learning,” and “digital payments.” Inclusion criteria included peer-reviewed articles, conference papers, and reports on ML-based UPI fraud detection in English from 2016–2025. The exclusion criteria included non-UPI studies, non-ML methods, and pre-2016 studies. From 250 records, 50 studies were selected after abstract and full-text screening for relevance and quality, as show in Figure 3.

Data extraction involves fraud types, ML models, datasets, and metrics (e.g., accuracy and precision) (Tranfield et al., 2003). Qualitative synthesis groups findings into fraud strategies and detection techniques. Limitations include potential bias from English-only sources and restricted access to proprietary datasets (Rodgers et al., 2009).

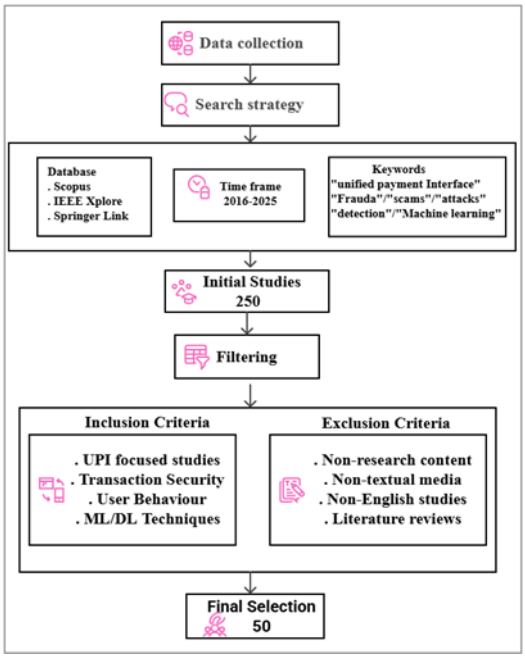


**Figure 3** Process of retrieving documents from databases for review.

### *3.1. Common types of fraud in UPI payments*

Fraud concerns associated with UPI transactions include lottery schemes, phishing, phony apps, AutoPay scams, tampering with QR codes, subscription fraud, and KYC scams. Fraudsters utilize urgency or impersonate reliable services to trick users into authorizing illegal transactions. Typical strategies include spoofing messages, manipulating QR codes, and making many payment requests. Rule-based fraud detection systems and supervised, unsupervised, and deep learning approaches are employed to detect suspicious patterns and improve financial security to counter these threats.

#### *3.1.1. UPI autopay fraud*

Scammers exploit UPIs' collect money and autopay request features by sending multiple payment requests to unsuspecting users (Edburg et al., 2024). If you accidentally approve of one of these requests, the fraudster gains access to your money (Akomea-Frimpong et al., 2019). The scam is deceptive because the request appears legitimate, and users often cannot differentiate between a real request and a fraudulent request (Tambe Ebot et al., 2024). Once approved, the money is transferred to the scammer's account (Fischer et al., 2013). Therefore, collect request fraud has occurred through.

Figure 4 refers to spamming activities by fraudsters in UPI. The message is a UPI AutoPay scam attempt that deceives users into activating automatic deductions by using phishing links and phony rewards. Users who click on the link can be redirected to a bogus website, which could result in illegal transactions. Users should confirm AutoPay requirements, stay away from dubious sites, and report fraud right away to stay safe.

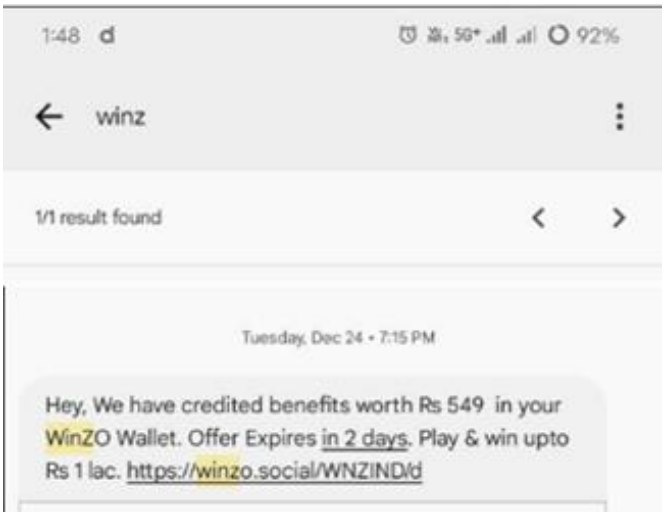


**Figure 4** Fraudsters spamming UPI IDs with multiple collect requests. *Source:* Das (2025).

*3.1.2. Fake UPI applications*

The use of fraudulent applications is one of the most common ways in which fraud is perpetrated (Ngai et al., 2011). There are many duplicate programs on the market, and the use of fraudulent applications is growing globally (Ekwonwune et al., 2022). This paper investigates UPI security issues in MPIN updates and fraud detection, recommending email notifications, additional authentication, and AI-driven behavioral analysis to improve fraud protection in UPI transactions (Krithiga Lakshmi et al., 2019). Research has shown that perceived safety, security, and risk influence technology adoption. Risk reduction entails exchanging information on a regular basis, analyzing features, implementing defensive measures, and changing trial designs to improve user trust and security (Edburg et al., 2024).

*3.1.3. Phishing fraud*

Phishing frauds are deceptive attempts to fool people into disclosing private information, such as bank account numbers, credit card numbers, usernames, or passwords (Gupta et al., 2017). Fraudsters imitate reputable organizations via telephone calls, text messages, or counterfeit websites (Ali et al., 2019). Phishing exploits urgency, tricking victims with fake prizes or threats to steal data for fraud. It targets human psychology, not technology (DeLiema et al., 2021; Charan & Thilak, 2023). Research has shown that phishing fraud in UPIs is escalating via counterfeit URLs and QR codes. Artificial intelligence, machine learning, and cryptography models improve fraud detection by examining user knowledge, scam methodologies, and security protocols. Phishing turns into AI-driven assaults. Prevention includes email filtering, SSL, MFA, and education. Awareness and reporting decrease financial, reputational, and psychological damage (Putra et al., 2024).

Figure 5 exhibits a sample of phishing fraud messages and a link in UPI payments. The message pop-up would look like this. A fraudster phones the victim, falsely alleging an inadvertent transfer and demanding reimbursement. The victim returns the money without confirming it, only to realize later that they were duped by a scammer who took advantage of their eagerness and confidence.

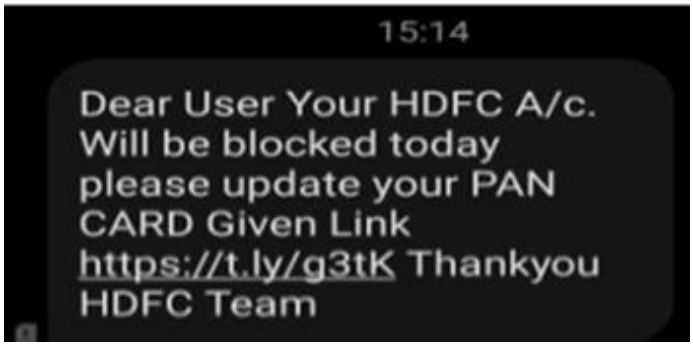


**Figure 5** Fraud phishing message disguised as a bank SMS. *Source:* Jain (2023).

*3.1.4. Tricky QR codes*

Fraudsters create fake QR codes that appear to have come from respectable companies, such well-known brands. These codes might be sent by text or email, or they could be displayed in public places (Pawar et al., 2022). Given their extensive usage in payments, QR codes are subject to social engineering and phishing. Research has identified security concerns, usability difficulties, and the need for multilayered protection and methodical recommendations to improve digital transaction security (Krombholz et al., 2014). News18 reported that when a customer paid with a QR code at her medical business in the morning, Omvati Gupta, one of the victims, prevented the scam. The client informed Gupta that the associated account had a different name (NEWS18, 2025).

Figure 6 shows an example of QR code manipulation in UPI payments. The picture demonstrates QR code tampering, in which minor adjustments cause payments to be redirected to fictitious accounts while still being scannable. Scammers take advantage of people's faith in QR-based UPI payments, which makes detection challenging. Verifying QR codes, utilizing secure payment mechanisms, and raising user and merchant knowledge to stop fraud are all necessary to defend against such assaults.

**Figure 6** QR code manipulation. *Source:* Wahyu Dharmawan & Ginardi (2017).

### *3.1.5. Lottery winning-related fraud*

Lottery scams include fraudsters masquerading as winners and deceiving victims with false reward claims. They want UPI IDs, PINs, or processing fees while offering commissions. Victims naively accept debit transactions or send money, only for fraudsters, to vanish or demand more money, claiming transfer difficulties. This research investigates the identification of fraud in lotteries and internet gambling, as well as money laundering and insider threats. A hybrid approach that incorporates statistical aggregation, fraud testing, and clustering improves detection accuracy while reducing false alarms, hence enhancing fraud protection efforts (Christou et al., 2011).

Figure 7 shows lottery pop-up fraud taken from Times of India newspaper article. The picture seems to be a fraud effort masquerading as a payout alert. Although it says the user has earned $17.9, they have to pay an absurdly high $24,780 charge before they can obtain their rewards. Financial fraud results from scammers using such techniques to fool people into submitting payment information. This method avoids disclosing sensitive information and always involves double-checking such statements.


**Figure 7** Lottery POP-UP fraud. *Source:* The Times of India (2020).

### *3.1.6. Subscription fraud*

Currently, the subscriptions of any platform are in the autopay option. With autopay, the owner will not have to worry about remembering to pay for the subscription (Kabari et al., 2015). Scammers falsely subscribe, deceiving users of unauthorized charges and profits (Alae Chouiekha, 2018). False URLs trick customers into unauthorized payments by mimicking autopay transactions (Koskelainen et al., 2023). Subscription fraud affects telecom profits and brands; ANN-based detection reveals fraudulent tendencies, enhancing fraud prevention in GSM mobile networks (Ekwonwune et al., 2022). This research uses data mining to identify fraudulent telecom subscriptions. A hybrid approach combines clustering (SOM, K-means) with classification (SVM, neural networks). Real data demonstrate good accuracy, with SVMs and boosted trees performing best (Farvaresh & Sepehri, 2011).

Figure 8 exhibits subscription fraud message and link in UPI payments. This image depicts a scam SMS that encourages users to click on a malicious link intended to steal personal or financial information by offering to provide free one-year Netflix membership because of the epidemic.

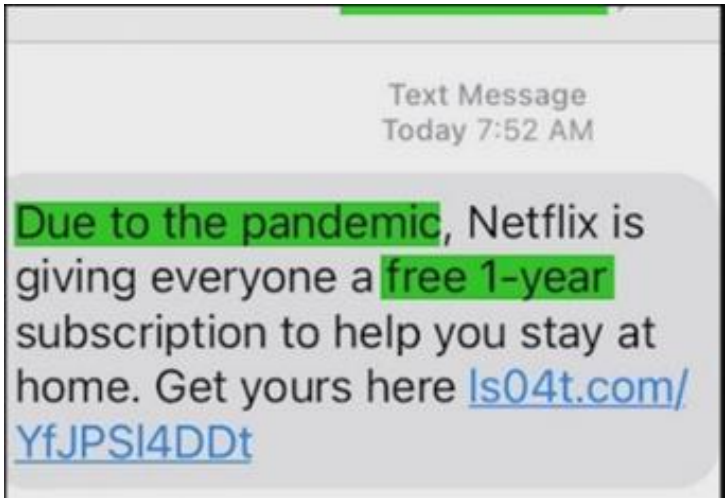


**Figure 8** Subscription fraud. *Source:* Mercedes (2020).

*3.1.7. KYC fraud*

KYC fraud is a type of online scam that involves scammers using the know-your customer (KYC) process to steal sensitive information from individuals and institutions (Kumar Pakina et al., 2023). Scammers serve as bank employees to steal personal data, enabling identity theft, fake accounts, and fraudulent transactions, causing financial losses (Shulzhenko & Romashkin, 2020). This study analyzes KYC fraud by smishing and vishing, using machine learning to detect fraud and enhance security against rising threats (Dharmavaram & Mishra, 2022). This study improves fraud detection and creates a risk assessment tool that uses machine learning and KYC data to identify fraudulent behavior, suspicious transactions, and default risks at bank branches for increased security (Chen, 2020).

Figure 9 shows KYC fraud in UPI. The fraudulent SMS in this picture purports to be from SBI and urges the user to click on an untrustworthy link for a KYC update to obtain private data. It also warns of account suspension.

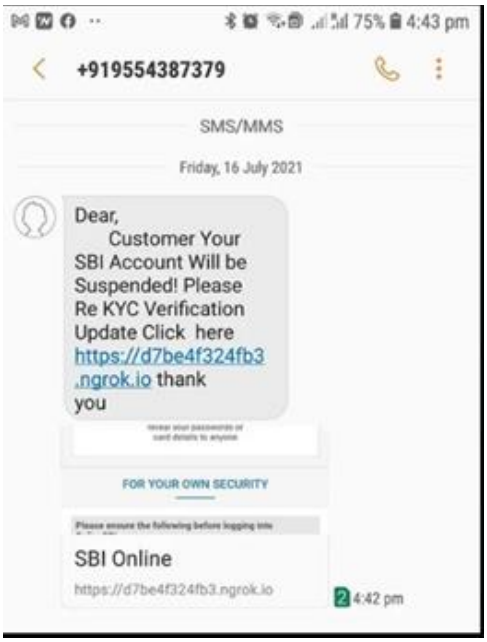


**Figure 9** KYC fraud. *Source:* Moneylife Digital Team (2021).

## 4. Machine Learning for Fraud Detection

Machine learning is becoming very important in spotting and stopping fraud in UPI transactions. It uses large amounts of data and smart algorithms to find unusual or suspicious activities (Md Rokibul Hasan et al., 2024). Techniques such as decision trees and random forests learn from past transactions to determine whether new transactions are safe or possibly fake (Ahmed et al., 2016). Other methods, such as clustering, look for strange patterns that might signal fraud (Palacio, 2019). Advanced models such as RNNs and LSTMs are excellent at understanding the order of transactions over time (Benchaji et al., 2021). When different models are combined, they become even better at catching fraud (Forough & Momtazi, 2021). Today's systems often use a mix of these smart tools and traditional rules to protect users in real time.

*4.1. Most frequently used fraud detection techniques*

Table 1 provides an overview of numerous studies on fraud detection, highlighting the strategies utilized, the datasets evaluated, and their performance. It highlights diverse methodologies, including machine learning models, convolutional neural networks, and social engineering detection methods, illustrating how these techniques help in recognizing and preventing fraudulent transactions in digital payment systems.

Table 1 provides an overview of numerous studies on fraud detection, highlighting the strategies utilized, the datasets evaluated, and their performance. It highlights diverse methodologies, including machine learning models, convolutional neural networks, and social engineering detection methods, illustrating how these techniques help in recognizing and preventing fraudulent transactions in digital payment systems.

**Table 1** Fraud detection techniques.

| Author/year | Title | Model | Dataset | Accuracy |
|---|---|---|---|---|
| (Almazroi & Ayub, 2023) | Online payment fraud detection | RXT-j model | IEEE-CIS Fraud detection dataset | 98% |
| (Akinje & Fuad, 2021) | Fraudulent detection model using machine learning techniques | Random forest | Fraud detection dataset | 100% |
| (Zhang et al., 2018) | Online transaction fraud detection | CNN | B2C online transaction dataset | 98% |
| (Charizanos et al., 2024) | fraud detection framework for credit card transactions | Fuzzy logistic regression | Credit card transaction dataset | 99.6% |
| (Hanae et al., 2023) | End-to-End Real-time Architecture for Fraud Detection in Online Digital Transactions | Isolation forest model | Online transaction dataset | 99% |
| (Jeyalakshmi et al., 2024) | Financial Fraud detection using Supervised and Unsupervised Learning | Logistic regression | credit card transaction dataset | 78.7% |
| (Bhowmik & Howlader, 2025) | Online payment fraud monitoring and detection | XGBoost | Sender Account Type, Beneficiary Account Number and Amount | 99.21% |
| (Patil et al., 2025) | An Automated Alert System for Financial Fraud Detection | Hybrid approach | ATM transactions and online transactions dataset | 97.5% |
| (Agrawal et al., 2023) | An Effective Approach to Classify Fraud SMS Using Hybrid Machine Learning Models | Hybrid model Multinomial Naive Bayes Random Forest Extra Tree Classifier | labeled as spam/ham messages dataset | 96.9% |
| (Pol et al., 2024) | Online Transaction Fraud Detection | Sparrow Search Algorithm (SSA), Time Convolutional Network (TCN | online credit card transaction dataset | 97.50% |
| (Raju et al., 2024) | Detection of fraudulent activities in UPI | LSTM | Online transactional data | 99.74% |

*Source:* Scopus and Web of Science Database.

## 5. Results

The results of the systematic literature review (SLR) provide a comprehensive analysis of existing research on UPI fraud detection, highlighting key findings, trends, and gaps. This review identifies machine learning (ML) and deep learning (DL) as the dominant approaches, with logistic regression, random forest, and neural networks frequently used for fraud classification. Cryptographic techniques, such as weighted hyperbolic curve cryptography (WHCC), are emerging as promising methods for enhancing security.

Table 2 presents a comprehensive analysis of existing research on UPI fraud detection, highlighting key findings, trends, and gaps. This review identifies machine learning (ML) and deep learning (DL) as the dominant approaches, with logistic regression, random forest, and neural networks frequently used for fraud classification.

**Table 2** Review of the most relevant articles (comprehensive synthesis of pivotal scholarly contributions).

| Title | Author/Year | DOI | Variables | Methodology | Findings | Future scope |
|---|---|---|---|---|---|---|
| Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions | (Rani et al., 2024) | 10.1109/ICDT61202.2024.10489682 | Valid transaction and fraud transaction. | XGBoost | Effective accuracy with 98.2% | include data, compliance, biometrics, and AI. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Fraud Fighters - How AI and ML are revolutionizing UPI Security | (Naik et al., 2024) | 10.1109/ICSTEM61137.2024.10560740 | Transaction Data, Fraud Indicators, Machine Learning Features. | AI&ML(CNN) | AI(CNN) is 97.68% accurate | fraud detection with machine learning, scalability, time, and location analysis. |
| Role of UPI Application Usage and Mitigation of Payment Transaction Frauds: An Empirical Study | (Edburg et al., 2024) | 10.1177/mjmrp.231222347 | perceived safety, perceived relative benefits, perceived risk, and perceived security, together with internal and external attacks. | Multiple regression analysis | $R^2$ value of 0.713 | Fraud prevention using smarter AI tools, studying rules and comparing fraud trends in different cultures. |
| A Robust UPI Fraud Identification Scheme over Digital Money Transactions using Learning Powered Classification Principles | (Ragavee et al., 2025) | 10.1109/ICEARS64219.2025.10941576 | UPI QR Scan code and UPI – id fraud identification. | M-DBN model | 98.4% Accuracy | With real time UPI data, handle uneven fraud cases better, and adapt to new scam methods over time. |
| Detection of Fraudulent Activities in Unified Payments Interface using Machine Learning - LSTM Networks | (Raju et al., 2024) | 10.1109/ICCPCT61902.2024.10672890 | amount, frequency, timestamp, merchant type, trends. | LSTM | 99.74% accuracy | combining reinforcement learning, extending datasets, and conducting continuous model updates to better fraud detection. |
| UPI fraud detection using machine learning | (Jagadeesan et al., 2024) | 10.1201/9781003559085-130 | dataset's completeness, relevance, and use for addressing the complexity of the study's objectives. | Random Forest | 94% Accuracy | New fraud strategies, and investigating novel machine learning techniques. |
| HMLM: An Intelligent Artificial Intelligence assisted Strategy to Identify UPI Frauds based on | (Bharath et al., 2025) | 10.1109/ICSES63760.2024.10910549 | Transaction amount, Time stamps, Device and location info, user behavior patterns. | HMLM | 98.61%Acccuracy | Real- time deployment, handling devices fraud types, adopting to evolving threats and integrating |

| | | | | | | |
|---|---|---|---|---|---|---|
| Hybrid Markov Learning Methodology | | | | | | with national payment system. |
| User's Opinion Analysis toward Unified Payment Interface (UPI) Transactions Using Artificial Intelligence | (Sekar, 2024) | 10.1109/ICONSTEM60960.2024.10568859 | App performance, Customer support, Payment success rate. | AI&NLP method | 97.21% Accuracy | Enhancing sentiment models, incorporating regional languages and expanding datasets for deeper UPI user behavior insights. |
| Enhancing Transaction Security through Iris Recognition | (Arepalli et al., 2024) | 10.1109/ICOECA62351.2024.00124 | crypts, furrows, and ridges. | G6_iris_recognizer | To address this, a system that adds iris authentication by replacing the existing PIN system. | Acceptability, privacy, and integration. |
| UPI Based Financial Fraud Detection Using Deep Learning Approach | (Gupta et al., 2024) | 10.1109/ACROSET62108.2024.10743663 | Data, category, Ref no, withdrawal, deposit, balance, binary classification label. | Deep learning based RNN method | 87.5%Accuracy | Build smarter, faster fraud detection systems that learn user behavior, protect privacy, and explain decisions. |
| UPI fraud detection in mobile payment using a Boost based frame work. | (Kumar et al., 2025) | https://doi.org/10.1063/5.0263094 | User behavior, transaction patterns, and user profile information. | XGBoost | XGBoost-LSTM hybrid effectively detects fraud while solving the imbalanced dataset challenge in financial transactions. | Real-time monitoring integration and regulatory compliance features would enhance adaptability against evolving fraud patterns. |
| UPIp: An Envisioned Policy-Based UPI Architecture for Secure Transactions | (Varshney, 2024) | 10.1109/MASS62177.2024.00105 | User based, Environmental conditions. | Attribute-Based Access Control (ABAC) | The study presents UPI a new system that makes UPI payments safer by letting users set rules to block fraud. | Develop a UPI prototype in real senarios, explore advanced ABAC biometrics, exception policies, and assess user adoption. |
| Evaluating Machine Learning Algorithms for Effective UPI Fraud Detection: A | (Sindhu, 2024) | 10.17148/IARJSET.2024.11670 | transaction amount, transaction duration, user behavior metrics, device | The methodology provided in the project for UPI fraud detection comprises applying several ML algorithms, including Random | ML with Random Forest and SVM provides UPI fraud prevention detection. | Prospects for the future improve digital payments, user security, and fraud detection. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Comparative Analysis | | | information, and previous transaction data. | Forest and Support Vector Machine (SVM) | | |
| Fraud detection in UPI transactions using ml | (Kavitha et al., 2024) | 10.36713/epra16459 | transaction patterns, user behavior, and different attributes retrieved from transaction data. | The technology employs HMM, clustering, and neural networks to identify fraud, assuring adaptability, efficiency, and effective anomaly identification | K-means, Markov models, and neural networks improve the detection of UPI fraud. | Refining algorithms, real-time monitoring, and reinforcement learning for fraud detection. |
| Detection of UPI Fake Payments using ML | (Murganandham & Subburaj, 2024) | 10.15680/IJMRSET.2024.0708032 | transactional data, user activity, and transaction patterns. | The process comprises gathering data, analyzing reports, and deploying machine learning models to enhance online payment security. | With real-time monitoring, SVM and RFC are successful at detecting UPI fraud. | Future research should strengthen systems, compliance, analysis, analytics, and algorithms. |
| Detection of Phishing Link and QR Code of UPI Transaction using Machine Learning | (Charan & Thilak, 2023) | 10.1109/ICIMIA60377.2023.10426613 | Phishing URLs, counterfeit QR codes, and transaction metadata help detect fraud. | Behavioral analysis, real-time detection, training, validation, supervised learning, feature extraction, and model selection. | Machine learning for phishing detection, real-time monitoring, and security is the main emphasis of the study. | Improve phishing detection through teamwork, real-time monitoring, machine learning, and user education. |
| Enhanced UPI Fraud Detection Using CNN: A Comparative Analysis with Machine Learning Models | (Bhargavi & Ram, 2025) | https://doi.org/10.54660/.IJMRGE.2025.6.2.452-455 | payer, payee, date, category, Reference No., Type of Transaction, Amount, Location. | CNN model to effectively detect fraudulent transactions and send alert message to the user. | Our results justify that the proposed model delivers superior performance compared to the existing models. | We improve fraud detection by adding features for dynamic patterns. |

*Source:* Scopus and Web of Science Database.

## 6. Discussion

India has used Unified Payments Interface (UPI) systems more quickly as a result of recent developments in financial technology. However, security issues, especially those pertaining to fraud, have also increased as a result of the rise in digital transactions. In an effort to combat these risks, an increasing amount of research has focused on biometric advancements, machine learning, and artificial intelligence. Seventeen important papers that address these issues are summarized in this study.

To address class imbalance and dimensionality reduction, a foundational study by Rani et al. (2024) created a machine learning-based UPI fraud detection system that uses XGBoost, SMOTE, and principal component analysis (PCA). The model demonstrates the possibility of combining biometric authentication with regulatory compliance for scalability, achieving an astonishing 98.2% accuracy. Building on this ML foundation, convolutional neural networks (CNNs) have also been shown to improve real-time fraud detection in UPI systems (Naik et al., 2024). With a 97% accuracy rate, their model reduced false positives and recommended the use of location-based analytics to enhance the system. By shifting the focus from algorithmic optimization to user-centric insights, Edburg et al. (2024) offered an empirical investigation of how users perceive the safety,

risk, and fraud protection of UPIs. The results highlighted the importance of incentives and awareness efforts, and they suggested blockchain and SWOT analysis as tactical instruments for improving security. In alignment with user-focused fraud mitigation, Ramakrishnan et al. (2024) added a recurrent neural network (RNN)-based predictive model integrated with the customer account security system (CASS) to support this user-focused approach. This model offered improved fraud prediction and encouraged deeper learning refinements and stronger regulatory integration.

To benchmark the performance of traditional classifiers, Sindhu (2024) used random forest and support vector machine (SVM) models to compare the performance of classification techniques. Using transactional, behavioral, and device-related data, the research confirmed the accuracy of machine learning (ML) in fraud detection and argued for algorithmic improvements to adapt to changing digital payment ecosystems. Using clustering approaches and Hidden Markov Models (HMMs) in conjunction with neural networks, J. Kavitha et al. (2024) extended this analytical rigor to detect abnormalities. Their methodology facilitated adaptive learning and stimulated the investigation of reinforcement learning for potential future uses. When Jagadeesan et al. used conventional machine learning approaches on real-world datasets, such as SVM, random forest, and logistic regression, they demonstrated the random forest model's higher accuracy and lower false-positive rates. They emphasized how important algorithmic optimization and blockchain integration are. Stacking long short-term memory (LSTM) networks, generative adversarial networks (GANs), and SMOTE were combined in Raju et al.'s (2024) hybrid deep learning architecture. They emphasized the importance of time series modeling and promoted reinforcement learning and dynamic dataset updates, with their model's impressive 99.74% accuracy.

Murganandham et al. (2024) focused on real-time monitoring and regulatory improvement while detecting UPI fraud via SVM and random forest. Arepalli et al. (2024) investigated iris-based biometric authentication and argued that its use in UPI systems would increase privacy. Karthick et al. (2024) supported dataset growth and real-time capabilities by analyzing temporal and geographical transaction data via an ANN, deep learning, and random forest. Using supervised machine learning, Charan and Thilak (2023) approached phishing and QR code fraud, emphasizing behavioral analytics and user education. Global compliance was demanded by Vadlamudi and Sam (2022), who concentrated on data privacy via tokenization, AI-driven risk assessments, and GPS-linked protection. Through the formal analysis of UPI systems, Malladi (2021) proposed improvements to OTP and blockchain. Design issues such as OTP interception and rogue applications were noted by Madwanna et al. (2021), who called for AI integration and user awareness. Bhargavi and Ram (2025) advanced detection by putting out a CNN-based model that outperforms conventional methods in recognizing dynamic fraud tendencies.

## 7. Conclusion

Digital payments, particularly via UPIs, have become a fundamental part of everyday life in India, but this convenience has also created serious security issues. The study demonstrates that machine learning algorithms, notably the XG boost and LSTM networks, have been extraordinarily effective in identifying fraudulent transactions, with accuracy rates reaching 99.74%. However, technology alone is not enough to address fraud. The most successful solution combines powerful algorithms with user education, real-time monitoring, and solid security features such as biometric verification. The growth in phishing attempts and bogus payment schemes during the COVID-19 pandemic underlined the need for stronger security mechanisms. The emphasis should be on creating more complex fraud detection tools that can adapt to new types of fraud while simultaneously making these systems more cost-effective and user-friendly. This report underlines that securing UPI transactions requires a complete approach that includes technology innovation, robust privacy.

## 8. Future Research Directions

Future research should focus on applying machine learning techniques to increase recovery rates from UPI payment fraud. A supervised learning algorithm can analyze transaction attributes, investigation timing and the institutional framework to predict recovery outcomes across fraud typologies. Deep learning architectures combined with real-time anomaly detection systems offer promising avenues for deploying early warning systems that significantly improve recovery rates. The integration of a gradient boosting classifier with traditional banking protocols may establish more effective recovery pathways, ultimately strengthening the financial security infrastructure.

## Acknowledgment

We would like to share our sincere honor with our esteemed supervisor regarding those works and insights that contributed to this study. I would also like to acknowledge the valuable resources provided by the academic and research community.

## Ethical Considerations

All data used in this study were obtained from publicly available sources or anonymized datasets, ensuring that no personal or sensitive information was disclosed, in adherence to ethical research standards.

## Conflict of Interest

The authors declare no conflicts of interest.

## Funding

The study did not receive any funding.

## References

Agrawal, N., Bajpai, A., Dubey, K., & Patro, B. D. K. (2023). An effective approach to classify fraud SMS using hybrid machine learning models. In *Proceedings of the IEEE 8th International Conference for Convergence in Technology (I2CT)* (pp. 1–6). https://doi.org/10.1109/I2CT57861.2023.10126300

Ahmed, M., Mahmood, A. N., & Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. *Future Generation Computer Systems, 55*, 278–288. https://doi.org/10.1016/j.future.2015.01.001

Ahmed, S. C. B., & Sreeju, V. V. (2020). The digital banking in India: Recent trends, opportunities and challenges. *Global Journal for Research Analysis, 9*(1), 5–8. https://doi.org/10.36106/gjra

Akinje, A. O., & Fuad, A. (2021). Fraudulent detection model using machine learning techniques for unstructured supplementary service data. *International Journal of Innovative Computing, 11*(2), 51–60. https://doi.org/10.11113/ijic.v11n2.299

Akomea-Frimpong, I., Andoh, C., Akomea-Frimpong, A., & Dwomoh-Okudzeto, Y. (2019). Control of fraud on mobile money services in Ghana: An exploratory study. *Journal of Money Laundering Control, 22*(2), 300–317. https://doi.org/10.1108/JMLC-03-2018-0023

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet, 12*(10), 1–39. https://doi.org/10.3390/fi12100168

Alae Chouiekha, E. H. I. E. H. (2018). ConvNets for fraud detection analysis. *Procedia Computer Science, 127*, 133–138. https://doi.org/10.1016/j.procs.2018.01.107

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems, 100*, 408–427. https://doi.org/10.1016/j.future.2019.03.041

Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *IEEE Access, 11*, 137188–137203. https://doi.org/10.1109/ACCESS.2023.3339226

Arepalli, G. S., Bhavana, P., Krishna, Y. V. S., & Surendrababu, C. (2024). Enhancing transaction security through iris recognition. In *Proceedings of the 2024 International Conference on Expert Clouds and Applications (ICOECA)* (pp. 684–688). https://doi.org/10.1109/ICOECA62351.2024.00124

Ashok, P., & Hallur, G. (2023). Seamless mobility: Innovating the digital service landscape in telecom industry. In *Proceedings of the International Conference on Cognitive Computing and Cyber Physical Systems, 991* (pp. 177–188). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-2550-2_14

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(3), 23–32. https://doi.org/10.4236/jss.2013.13004

Au, Y. A., & Kauffman, R. J. (2008). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. *Electronic Commerce Research and Applications, 7*(2), 141–164. https://doi.org/10.1016/j.elerap.2006.12.004

Badak, S., Kolte, V., Agrawal, M., & Gupta, S. (2023). Mobile computing, communications & revolution of digital payment in India. *Journal of Mobile Computing, Communications & Mobile Networks, 10*(3), 29–37. https://doi.org/10.37591/JoMCCMN

Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. *Journal of Big Data, 8*(1), 1–21. https://doi.org/10.1186/s40537-021-00541-8

Bera, S., & Li, B. (2024). UPI: The future of payment system in India. *Journal of Philanthropy and Marketing, 4*(1), 201–210.

Bharath, S., Prasad, G. L. V., Sujatha, V., Hemajothi, S., Mani, D. S., & Merlin, N. R. G. (2025). HMLM: An intelligent artificial intelligence assisted strategy to identify UPI frauds based on hybrid Markov learning methodology. In *Proceedings of the International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 1*(1) (pp. 1–6). https://doi.org/10.1109/ICSES63760.2024.10910549

Bhargavi, S. M., & Ram, B. K. (2025). Enhanced UPI fraud detection using CNN: A comparative analysis with machine learning models. *International Journal of Multidisciplinary Research and Growth Evaluation, 6*(2), 452–455. https://doi.org/10.54660/IJMRGE.2025.6.2.452-455

Bhatia-Kalluri, A., & Caraway, B. R. (2025). Transformation of the digital payment ecosystem in India: A case study of Paytm. *Social Inclusion, 11*(3), 320–331. https://doi.org/10.17645/si.v11i3.6687

Bhowmik, S., & Howlader, J. (2025). Online payment fraud monitoring and detection: Performance analysis of tree-based ensemble machine learning models. In *Proceedings of the 2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS)* (pp. 102–107). IEEE. https://doi.org/10.1109/COMSNETS63942.2025.10885622

Bhujel, S. (2024). Factors driving the adoption of fintech services: An empirical analysis of customers of commercial banks in Kathmandu. *Apex Journal of Business and Management, 3*(2), 67–85. https://doi.org/10.61274/apxc.2024.v03i02.007

Braithwaite, J. (2024). 'Authorized push payment' bank fraud: What does an effective regulatory response look like? *Journal of Financial Regulation, 10*(2), 174–193. https://doi.org/10.1093/jfr/fjae006

Chandra Agarwal, S., Shukla, V., & Awasthi, A. (2024). Digital payment dynamics: Unveiling the impacts on sustainable development, environmental protection, and social inclusion. *International Journal of Trend in Scientific Research and Development, 8*(1), 519–525. https://www.ijtsrd.com/papers/ijtsrd63442.pdf

Charan, G. R., & Thilak, K. D. (2023). Detection of phishing link and QR code of UPI transaction using machine learning. In *Proceedings of the 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 658–663). IEEE Xplore. https://doi.org/10.1109/ICIMIA60377.2023.10426613

Charizanos, G., Demirhan, H., & İçen, D. (2024). An online fuzzy fraud detection framework for credit card transactions. *Expert Systems with Applications, 252*(2), 1–15. https://doi.org/10.1016/j.eswa.2024.124127

Chen, T.-H. (2020). Do you know your customer? Bank risk assessment based on machine learning. *Applied Soft Computing, 86*, 105779. https://doi.org/10.1016/j.asoc.2019.105779

Chohan, F., Aras, M., Indra, R., Wicaksono, A., & Winardi, F. (2022). Building customer loyalty in digital transaction using QR code: Quick Response Code Indonesian Standard (QRIS). *Journal of Distribution Science, 20*(1), 1–11. https://doi.org/10.15722/jds.20.01.202201.1

Christou, I. T., Bakopoulos, M., Dimitriou, T., Amolochitis, E., Tsekeridou, S., & Dimitriadis, C. (2011). Detecting fraud in online games of chance and lotteries. *Expert Systems with Applications, 38*(10), 13158–13169. https://doi.org/10.1016/j.eswa.2011.04.124

Das, N. (2025). New UPI fraud trend: Fraudsters spamming UPI IDs with multiple collect requests; one careless approval means money gone from bank a/c. *Economic Times*. https://economictimes.indiatimes.com/wealth/save/new-upi-scam-alert-upi-autopay-set-up-request-could-swindle-money-out-of-your-account-if-you-are-not-careful. Accessed October 1, 2025.

DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adults. *Innovation in Aging, 5*(4), 1–11. https://doi.org/10.1093/geroni/igab043

Dharmavaram, V. G., & Mishra, O. (2022). KYC fraud: A new means to conduct financial fraud–how to tackle it? In S. Verma, V. Vyas, & K. Kaushik (Eds.), *Cybersecurity issues, challenges, and solutions in the business world* (pp. 81–94). IGI Global.

Dr. Murganandham, Dr. T. Subburaj, M. (2024). Detection of UPI fake payments using ML. *International Journal of Multidisciplinary Research in Science, Engineering and Technology, 7*(8), 13952–13955. https://doi.org/10.15680/IJMRSET.2024.0708032

Edburg, B. F., Umadevi, K., Vidya, M., & Kumar, P. M. R. (2024). Role of UPI application usage and mitigation of payment transaction frauds: An empirical study. *MDIM Journal of Management Review and Practice, 2*(1), 7–22. https://doi.org/10.1177/mjmrp.231222347

Ekwonwune, E. N., Chukwuebuka, U. C., Duroha, A. E., & Duru, A. N. (2022). Analysis of global system for mobile communication (GSM) subscription fraud detection system. *International Journal of Communications, Network and System Sciences, 15*(10), 167–180. https://doi.org/10.4236/ijcns.2022.1510012

Eren, B. A. (2024). QR code m-payment from a customer experience perspective. *Journal of Financial Services Marketing, 29*(1), 106–121. https://doi.org/10.1057/s41264-022-00186-5

Faccia, A. (2023). National payment switches and the power of cognitive computing against fintech fraud. *Big Data and Cognitive Computing, 7*(76), 1–28. https://doi.org/10.3390/bdcc7020076

Farvaresh, H., & Sepehri, M. M. (2011). A data mining framework for detecting subscription fraud in telecommunication. *Engineering Applications of Artificial Intelligence, 24*(1), 182–194. https://doi.org/10.1016/j.engappai.2010.05.009

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology, 43*(10), 2060–2072. https://doi.org/10.1111/jasp.12158

Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing, 99*, 106883. https://doi.org/10.1016/j.asoc.2020.106883

Gochhwal, R. (2017). Unified payment interface—An advancement in payment systems. *American Journal of Industrial and Business Management, 7*(10), 1174–1191. https://doi.org/10.4236/ajibm.2017.710084

Gupta, A., & Xia, C. (2018). A paradigm shift in banking: Unfolding Asia's FinTech adventures. In W. A. Barnett & B. S. Sergi (Eds.), *Banking and finance issues in emerging markets* (pp. 215–254). Emerald Publishing Limited.

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems, 67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing and Applications, 28*(12), 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

Gupta, R., Gupta, S., & Ajekwe, C. C. M. (2023). Electronic banking frauds: The case of India. In A. Rafay (Ed.), *Theory and practice of illegitimate finance* (pp. 166–183). IGI Global.

Gupta, V., Sharma, S., Nimkar, S., & Pathak, S. (2024). UPI based financial fraud detection using deep learning approach. In *Proceedings of the 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET)* (pp. 1–6). https://doi.org/10.1109/ACROSET62108.2024.10743663

Hanae, A., Abdellah, B., Saida, E., & Youssef, G. (2023). End-to-end real-time architecture for fraud detection in online digital transactions. *International Journal of Advanced Computer Science and Applications, 14*(6), 749–757. https://doi.org/10.14569/IJACSA.2023.0140680

Hoffmann, A. O. I., & Birnbrich, C. (2012). The impact of fraud prevention on bank-customer relationships. *International Journal of Bank Marketing, 30*(5), 390–407. https://doi.org/10.1108/02652321211247435

J. Kavitha, G. Indira, A. Anil Kumar, A. Shrinita, & D. Bappan. (2024). Fraud detection in UPI transactions using ML. *EPRA International Journal of Research & Development (IJRD), 9*(4), 142–146. https://doi.org/10.36713/epra16459

Jagadeesan, S., Arjun, K. S., Dhanika, G., Karthikeyan, G., & Deepika, K. (2024). UPI fraud detection using machine learning. In V. Sharmila, S. Kannadhasan, A. R. Kannan, P. Sivakumar, & V. Vennila (Eds.), *Challenges in information, communication and computing technology* (pp. 755–760). CRC Press.

Jain, S. (2023). Understanding social engineering and its impact on merchant-based UPI frauds. *International Research Journal of Engineering and Technology, 10*(3), 476–481.

Jeyalakshmi, R., Rajput, N., & Gracy, S. H. R. (2024). Financial fraud detection using supervised and unsupervised learning. In *Proceedings of the 4th International Conference on Power, Energy, Control and Transmission Systems: Harnessing Power and Energy for an Affordable Electrification of India (ICPECTS 2024)* (pp. 1–9). https://doi.org/10.1109/ICPECTS62210.2024.10780301

Kabari, L. G., Nuka Nanwin, D., & Uduak Nquoh, E. (2015). Telecommunications subscription fraud detection using artificial neural networks. *Transactions on Machine Learning and Artificial Intelligence, 3*(6), 1–16. https://doi.org/10.14738/tmlai.36.1695

Kakade, R. B., & Veshne, N. A. (2017). Unified payment interface (UPI)—A way towards cashless economy. *International Research Journal of Engineering and Technology, 4*(11), 762–766.

Kannan, R. R., & Vasantha, S. (2021). COVID-19 outbreaks on the growth of self-servicing technology using digital payments. *Webology, 18*(2), 22–40. https://doi.org/10.14704/web/v18i2/web18305

Karthick, N., Leema Roselin, G., Tamilarasan, M., Kalaiselvi, K., Sudha, S., & Jayanthi, J. (2024). Unified payment interface imposture and scam detection using deep learning and ANN. In *Proceedings of the 2024 3rd International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN 2024)* (pp. 5–10). https://doi.org/10.1109/ICSTSN61422.2024.10671346

Koskelainen, T., Kalmi, P., Scornavacca, E., & Vartiainen, T. (2023). Financial literacy in the digital age—A research agenda. *Journal of Consumer Affairs, 57*(1), 507–528. https://doi.org/10.1111/joca.12510

Kousaridas, A., Parissis, G., & Apostolopoulos, T. (2008). An open financial services architecture based on the use of intelligent mobile devices. *Electronic Commerce Research and Applications, 7*(2), 232–246. https://doi.org/10.1016/j.elerap.2007.04.003

Krithiga Lakshmi, K., Gupta, H., & Ranjan, J. (2019). UPI based mobile banking applications: Security analysis and enhancements. In *Proceedings of the 2019 Amity International Conference on Artificial Intelligence (AICAI 2019)* (pp. 903–908). https://doi.org/10.1109/AICAI.2019.8701396

Krombholz, K., Fr, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2014). QR code security: A survey of attacks and challenges for usable security. In *Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 79–90). Cham: Springer International. https://doi.org/10.1007/978-3-319-07620-1_8

Kumar Pakina, A., Kumar Kejriwal Meta, D., Dattatray Pujari, T., Kejriwal, D., & Goel, A. (2023). AI-generated synthetic identities in FinTech: Detecting deep fakes KYC fraud using behavioral biometrics. *IOSR Journal of Computer Engineering, 25*(3), 26–37. https://doi.org/10.9790/0661-2503032637

Kumar, A., Choudhary, R. K., Mishra, S. K., Kar, S. K., & Bansal, R. (2022). The growth trajectory of UPI-based mobile payments in India: Enablers and inhibitors. *Indian Journal of Finance and Banking, 11*(1), 45–59. https://doi.org/10.46281/ijfb.v11i1.1855

Kumar, K. (2025). Examining user awareness and addressing security challenges in the UPI framework: A comprehensive analysis framework. *International Journal of Scientific Research in Engineering and Management, 9*(5), 1–9. https://doi.org/10.55041/IJSREM47631

Kumar, P., Selvaraj, S., Balamurugan, S., & Ravi, S. A. (2025). UPI fraud detection in mobile payment using a boost-based framework. In *AIP Conference Proceedings* (p. 020073). AIP Publishing LLC. https://doi.org/10.1063/5.0263094

Kumar, S. V., & Unnisa, N. (2024). A study on UPI transactions in India. *International Journal of Advances in Business and Management Research, 1*(3), 8–22. https://doi.org/10.62674/ijabmr.2024.v1i03.002

Logeshwaran, J. (2022). The control and communication management for ultra dense cloud system using fast Fourier algorithm. *Ictact Journal on Data Science and Machine Learning, 3*(2), 281–284.

Ma, L., Ofoghi, B., Watters, P., & Brown, S. (2009). Detecting phishing emails using hybrid features. In *Proceedings of the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing* (pp. 493–497). IEEE. https://doi.org/10.1109/UIC-ATC.2009.103

Madwanna, Y., Khadse, M., & Chandavarkar, B. R. (2021). Security issues of unified payments interface and challenges: Case study. In *Proceedings of the 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)* (pp. 150–154). IEEE. https://doi.org/10.1109/ICSCCC51823.2021.9478078

Maharana, K. C. (2024). Technology in finance and service delivery. *SSRN Electronic Journal, 2*, 1–134. https://doi.org/10.2139/ssrn.4936118

Malladi, S. (2021). Towards formal modeling and analysis of UPI protocols. In *Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks* (pp. 239–243). IEEE. https://doi.org/10.1109/ICICV50876.2021.9388452

Mallik, A., Tran, C., & Twagirumukiza, A. (2020). USSD digital wallet. In *Proceedings of the 2020 Intermountain Engineering, Technology and Computing (IETC)* (pp. 1–5). IEEE. https://doi.org/10.1109/IETC47856.2020.9249106

Marquez-Chamorro, A. E., Resinas, M., & Ruiz-Cortes, A. (2018). Predictive monitoring of business processes: A survey. *IEEE Transactions on Services Computing, 11*(6), 962–977. https://doi.org/10.1109/TSC.2017.2772256

Md Rokibul Hasan, Md Sumon Gazi, & Nisha Gurung. (2024). Explainable AI in credit card fraud detection: Interpretable models and transparent decision-making for enhanced trust and compliance in the USA. *Journal of Computer Science and Technology Studies, 6*(2), 1–12. https://doi.org/10.32996/jcsts.2024.6.2.1

Mercedes, C. (2020). VERIFY: Sorry, but that free Netflix text is a scam. *KHOU*. https://www.khou.com/article/news/verify/free-netflix-text-verify/285-d03b10b6-1163-49b9-a183-7f59573f23a6. Accessed October 1, 2025.

Mishra, A., Vangaveti, A., & Majoo, S. M. K. (2023). Fintechs reshaping the financial ecology: The growing trends and regulatory framework. *IMIB Journal of Innovation and Management, 2*(1), 34–44. https://doi.org/10.1177/ijim.231200315

Mittal, A. (2023). UPI payment workflow. https://medium.com/@ayush_mittal/upi-payments-workflow-d0dcc65890f2

Mohapatra, S. (2017). Unified payment interface (UPI): A cashless Indian e-transaction process. *International Journal of Applied Science and Engineering, 5*(1), 29–42. https://doi.org/10.5958/2322-0465.2017.00004.1

Naik, S. K. L., Kiran, A., Kumar, V. P., Mannam, S., Kalyani, Y., & Silparaj, M. (2024). Fraud fighters: How AI and ML are revolutionizing UPI security. In *Proceedings of the 2024 International Conference on Science, Technology, Engineering and Management (ICSTEM)* (pp. 1–7). https://doi.org/10.1109/ICSTEM61137.2024.10560740

NEWS18. (2025). New scam alert! Fraudsters swap UPI QR codes. https://www.news18.com/india/new-scam-alert-fraudsters-swap-qr-codes-outside-madhya-pradesh-shops-to-get-payments-into-their-accounts-9186477.html

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Niranjanamurthy, M., & Chahar, D. (2013). The study of e-commerce security issues and solutions. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(7), 2885–2895.

Obaid, M., Bayram, Z., & Saleh, M. (2019). Instant secure mobile payment scheme. *IEEE Access, 7*, 55669–55678. https://doi.org/10.1109/ACCESS.2019.2913430

Palacio, S. M. (2019). Abnormal pattern prediction: Detecting fraudulent insurance property claims with semi-supervised machine-learning. *Data Science Journal, 18*(1), 1–15. https://doi.org/10.5334/dsj-2019-035

Patil, M., Aishwarya, G., Sharma, A., & Patil, S. (2025). An automated alert system for financial fraud detection with learning based models. In *Proceedings of the 8th IEEE International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS 2024, 1)* (pp. 1–6). IEEE. https://doi.org/10.1109/CSITSS64042.2024.10816781

Pawar, A., Fatnani, C., Sonavane, R., Waghmare, R., & Saoji, S. (2022). Secure QR code scanner to detect malicious URL using machine learning. In *Proceedings of the 2nd Asian Conference on Innovation in Technology (ASIANCON 2022)* (pp. 2–9). https://doi.org/10.1109/ASIANCON55314.2022.9908759

Pol, N., Rede, G. D., Agarwal, S., Sanjeera, S., Aravind, A. R., & Kumar, G. (2024). Online transaction fraud detection: Exploring the hybrid SSA-TCN-BiGRU approach. In *Proceedings of the 2nd World Conference on Communication and Computing (WCONF)* (pp. 1–6). IEEE. https://doi.org/10.1109/WCONF61366.2024.10692254

Purohit, S., & Purohit, S. (2024). From cash to code: Digital payment adoption and its ripple effects on economic landscape in Indian petro-retail. In M. D. Guillamón (Ed.), *Contemporary research in business, management and economics* (Vol. 2, pp. 27–46). B.P. International.

Putra, F. P. E., Ubaidi, U., Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of phishing attack trends, impacts and prevention methods: Literature study. *Brilliance: Research of Artificial Intelligence, 4*(1), 413–421. https://doi.org/10.47709/brilliance.v4i1.4357

Ragavee, U., Prithive Raj, M., Mithra, J. N., Balaji, S. S., Narayanan, L. A., & Mahimai Dass, Y. J. (2025). A robust UPI fraud identification scheme over digital money transactions using learning powered classification principles. In *Proceedings of the 2025 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 1551–1558). https://doi.org/10.1109/ICEARS64219.2025.10941576

Raju, M. N., Chandrasena Reddy, Y., Babu, P. N., Pavan Ravipati, V. S., & Chaitanya, V. (2024). Detection of fraudulent activities in unified payments interface using machine learning - LSTM networks. In *Proceedings of the 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)* (pp. 769–774). https://doi.org/10.1109/ICCPCT61902.2024.10672890

Ramakrishnan, R., Vanisri, S., & Yuvalakshmi, D. (2024). Unified payment interface seamless transaction using RNN model. *International Journal of Progressive Research in Engineering Management and Science, 4*(5), 1279–1283. https://doi.org/10.58257/IJPREMS34325

Ramesh, G., Jangid, A., Sivamalai, L., & Rebelly, A. B. (2020). NPCI: Chartering a payment freeway. *SSRN Electronic Journal, 4*(2), 1–55. https://doi.org/10.2139/ssrn.3760921

Rani, R., Alam, A., & Javed, A. (2024). Secure UPI: Machine learning-driven fraud detection system for UPI transactions. In *Proceedings of the 2nd International Conference on Disruptive Technologies (ICDT 2024)* (pp. 924–928). https://doi.org/10.1109/ICDT61202.2024.10489682

Rastogi, S., Panse, C., Sharma, A., & Bhimavarapu, V. M. (2021). Unified payment interface (UPI): A digital innovation and its impact on financial inclusion and economic development. *Universal Journal of Accounting and Finance, 9*(3), 518–530. https://doi.org/10.13189/ujaf.2021.090326

Rodgers, M., Sowden, A., Petticrew, M., Arai, L., Roberts, H., Britten, N., & Popay, J. (2009). Testing methodological guidance on the conduct of narrative synthesis in systematic reviews. *Evaluation, 15*(1), 49–73. https://doi.org/10.1177/1356389008097871

Sekar, S. (2024). Users opinion analysis towards unified payment interface (UPI) transactions using artificial intelligence. In *Proceedings of the 9th International Conference on Science, Technology, Engineering and Mathematics: The Role of Emerging Technologies in Digital Transformation (ICONSTEM, 2(3))* (pp. 1–6). https://doi.org/10.1109/ICONSTEM60960.2024.10568859

Senturk, S., Yerli, E., & Sogukpinar, I. (2017). Email phishing detection and prevention by using data mining techniques. In *Proceedings of the 2017 International Conference on Computer Science and Engineering (UBMK)* (pp. 707–712). https://doi.org/10.1109/UBMK.2017.8093510

Shree, S., Pratap, B., Saroy, R., & Dhal, S. (2021). Digital payments and consumer experience in India: A survey based empirical study. *Journal of Banking and Financial Technology, 5*(4), 1–20. https://doi.org/10.1007/s42786-020-00024-z

Shulzhenko, N., & Romashkin, S. (2020). Internet fraud and transnational organized crime. *Juridical Tribune, 10*(1), 162–172.

Sindhu, K. S. (2024). Evaluating machine learning algorithems for effective UPI fraud detection: A comparative analysis. *International Advanced Research Journal in Science, Engineering and Technology, 11*(6), 512–515. https://doi.org/10.17148/IARJSET.2024.11670

Suman, D. A. K. (2024). Fraud in UPI transactions. Government of India Ministry of Finance Department of Financial Services. https://sansad.in/getFile/loksabhaquestions/annex/183/AU211_sk53e3.pdf?source=pqals

Tambe Ebot, A. C., Siponen, M., & Topalli, V. (2024). Towards a cybercontextual transmission model for online scamming. *European Journal of Information Systems, 33*(4), 571–596. https://doi.org/10.1080/0960085X.2023.2210772

Team, M. D. (2021). SBI warns customers about phishing links offering freebies. *Moneylife.* https://www.moneylife.in/article/sbi-warns-customers-about-phishing-links-offering-freebies/64560.html

The Times of India. (2020). Internet lottery scam: 7 pictures that show how it works. https://timesofindia.indiatimes.com/gadgets-news/internet-lottery-scam-7-pictures-that-show-how-it-works/articleshow/74839758.cms

Toral-Cruz, H., Mihovska, A. D., Gaj, P., He, D., Ramírez-Pacheco, J. C., Voznak, M., & Lokshina, I. (2017). Advances and challenges in convergent communication networks. *Wireless Personal Communications, 96*(4), 4919–4927. https://doi.org/10.1007/s11277-017-4964-y

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Tulsi, A. V., & Patil, P. D. D. (2023). Prevention service for fraudulent and non fraudulent payments using online payment. *International Journal of Engineering and Management Research, 13*(6), 119–140. https://doi.org/10.31033/ijemr.13.6.15

Vadlamudi, S., & Sam, J. (2022). Unified payments interface – Preserving the data privacy of consumers. In *Proceedings of the 2022 International Conference on Cyber Resilience (ICCR)* (pp. 1–6). IEEE. https://doi.org/10.1109/iccr56254.2022.10024689

Varshney, G. (2024). UPI ρ: An envisioned policy-based UPI architecture for secure transactions. In *Proceedings of the 2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS, 3(4))* (pp. 658–663). IEEE. https://doi.org/10.1109/MASS62177.2024.00105

Verma, S., Kawamoto, Y., Fadlullah, Z. M., Nishiyama, H., & Kato, N. (2017). A survey on network methodologies for real-time analytics of massive IoT data and open research issues. *IEEE Communications Surveys & Tutorials, 19*(3), 1457–1477. https://doi.org/10.1109/COMST.2017.2694469

Vidani, J. (2024). A study on the rise and recent development in unified payments interface. *Journal of Advanced Research in Business Law and Technology Management, 7*(1), 21–30. https://doi.org/10.2139/ssrn.4849785

Wahyu Dharmawan, I. N. P., & Ginardi, R. V. H. (2017). Fraud avoidance using QR codes on transaction process on Finding – Tutor application in Android system. *Jurnal Teknik ITS, 6*(2). https://doi.org/10.12962/j23373539.v6i2.23144

Yang, H., & Lee, H. (2019). Understanding user behavior of virtual personal assistant devices. *Information Systems and E-Business Management, 17*(1), 65–87. https://doi.org/10.1007/s10257-018-0375-1

Zhang, Z., Zhou, X., Zhang, X., Wang, L., & Wang, P. (2018). A model based on convolutional neural network for online transaction fraud detection. *Security and Communication Networks, 2018*, 1–9. https://doi.org/10.1155/2018/5680264