Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

CYBERSECURITY THREATS IN ONLINE PAYMENT SYSTEMS

Name- Lavlesh Bagwe & Ankit Chaudhary
College Name – CDOE, University of Mumbai
Email- (lavleshbagwe11163@gmail.com) / (ankitcha810@gmail.com)

Abstract

The rapid expansion of online payment systems such as UPI, mobile wallets, debit/credit cards, and net banking has transformed digital financial transactions worldwide. However, the growing dependence on electronic payments has also increased exposure to cybersecurity threats. This research paper examines major cyber threats including phishing, malware, SIM swap fraud, QR code fraud, and social engineering attacks affecting digital payment platforms. It further analyzes key vulnerabilities such as weak authentication mechanisms, insecure mobile devices, poor network security, and lack of user awareness that contribute to successful cyberattacks. The study also explores preventive security measures including encryption, two-factor authentication, biometric verification, and AI-based fraud detection systems. The findings highlight the importance of continuous technological advancement and user awareness in ensuring secure and reliable online financial transactions.

1. Introduction

Online payment systems have transformed the way financial transactions are conducted by enabling users to transfer money electronically through digital platforms. These systems allow individuals and businesses to perform transactions using mobile phones, computers, or other digital devices without the need for physical cash. Common examples of online payment systems include Unified Payments Interface (UPI), mobile wallets, debit and credit cards, and internet banking. Due to their speed, convenience, and accessibility, online payments have become an integral part of modern financial systems.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

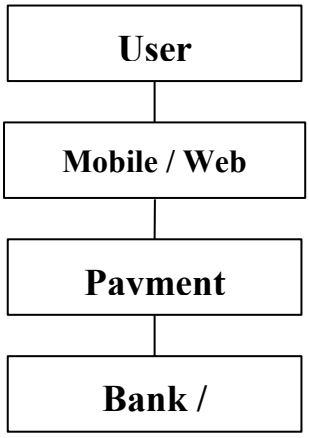


Figure 1: Basic Architecture of an Online Payment System

In recent years, there has been a rapid growth in digital payments, particularly in countries like India, where initiatives promoting cashless transactions have gained momentum. Platforms such as UPI, mobile wallets, and net banking have witnessed a significant increase in adoption due to the widespread use of smartphones and affordable internet services. The ease of making instant payments anytime and anywhere has encouraged users to rely heavily on digital payment methods for daily transactions such as bill payments, online shopping, and fund transfers.

With the expansion of digital payment platforms, cybersecurity has become a crucial aspect of online financial transactions. **Cybersecurity** refers to the protection of digital systems, networks, and data from unauthorized access, cyber attacks, and security breaches. In online payment systems, effective cybersecurity mechanisms are required to protect sensitive information such as user credentials, bank details, and transaction records. Ensuring data confidentiality, integrity, and availability is essential to maintain user trust and the reliability of digital payment services.

However, the increasing use of online payment systems has also raised serious concerns related to cybersecurity. Since these transactions involve sensitive financial and personal information, they have become attractive targets for cybercriminals. Any security breach in online payment systems can result in financial losses, identity theft, and loss of user confidence. The dependency on mobile-based payment applications has further increased the exposure to cyber threats, as users often perform transactions over public networks or insecure devices.

Moreover, lack of awareness among users regarding safe digital practices, such as identifying phishing messages or using secure networks, contributes significantly to the success of cyber attacks. As a result, online payment systems face continuous challenges in protecting users from evolving cyber threats.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

The purpose of this research paper is to study the various cybersecurity threats associated with online payment systems, analyze the vulnerabilities that lead to such threats, and understand the importance of effective security mechanisms in protecting digital financial transactions.

2. Objectives of the Study

The main objective of this research paper is to examine the cybersecurity threats associated with online payment systems and to understand the factors that contribute to security risks in digital financial transactions. As the usage of online and mobile-based payment platforms continues to grow, it becomes essential to analyze the security challenges and protective measures related to such systems.

The specific objectives of the study are as follows:

- To study the various cybersecurity threats affecting online payment systems such as UPI, mobile wallets, debit/credit cards, and net banking.
- To analyze the vulnerabilities present in digital payment transactions that may be exploited by cybercriminals.
- To examine common cyber attacks, including phishing, malware, SIM swap fraud, and QR code fraud, which impact online payment users.
- To understand the role of weak authentication mechanisms, insecure networks, and user negligence in enabling cyber attacks.
- To study the existing security mechanisms and technologies used to prevent online payment fraud, such as OTP-based verification, encryption, and two-factor authentication.
- To evaluate the importance of user awareness and safe digital practices in reducing cybersecurity risks in online payment systems.
- To highlight the need for continuous improvement in cybersecurity measures to ensure secure and reliable online financial transactions.

3. Overview of Online Payment System

Online payment systems represent a digital framework that enables the electronic exchange of money between users, merchants, and financial institutions. These systems are designed to support fast, convenient, and secure transactions by integrating software applications, communication networks, and banking services. Unlike traditional payment methods, online payment systems reduce manual intervention and allow automated processing of financial transactions.

From an operational perspective, online payment systems rely on secure communication channels and authentication mechanisms to validate transactions. Each transaction involves verification of user identity, authorization of payment, and confirmation of transaction status. The efficiency of

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

these systems depends on factors such as transaction speed, system availability, and security controls implemented by service providers.

a. Types of Online Payment Systems

Online payment systems can be broadly classified into the following categories:

1. Unified Payments Interface (UPI):

UPI is a real-time payment system that allows instant bank-to-bank transactions using mobile devices. It enables users to transfer funds using a Virtual Payment Address (VPA) without sharing sensitive bank details. Due to its simplicity and speed, UPI has gained widespread adoption in India.

2. Mobile Wallets:

Mobile wallets are digital applications that store users' payment information and allow them to make transactions electronically. Examples include wallets used for bill payments, online shopping, and peer-to-peer transfers. Wallets offer convenience but require strong security measures to protect stored data.

3. Debit and Credit Cards:

Debit and credit cards are commonly used for online payments on e-commerce platforms. These cards require card details such as card number, expiry date, and CVV for transaction processing. Additional security mechanisms like OTP-based authentication are often used to reduce fraud.

4. Net Banking:

Net banking allows users to perform online transactions directly through their bank's website or application. It provides services such as fund transfers, bill payments, and account management. Although considered secure, net banking systems are also vulnerable to phishing and malware attacks.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

Payment Method	Transaction Speed	Convenience	Security Risk Level
UPI	Very High	Very High	Medium
Mobile Wallets	High	High	Medium
Debit Cards	Medium	Medium	Medium to High
Credit Cards	Medium	Medium	Medium to High
Net Banking	Medium	Low to Medium	Low to Medium

Table 1: Comparison of Common Online Payment Methods

b. Key Components of Online Payment Systems

Online payment systems consist of several interconnected components that work together to complete a transaction securely:

- **User Interface:** Allows users to initiate and manage transactions.
- **Authentication Module:** Verifies the identity of the user.
- **Transaction Processing System:** Handles payment authorization and validation.
- **Settlement System:** Ensures transfer of funds between banks or institutions.

Each component plays an important role in maintaining transaction efficiency and security.

4. Literature Review

Several studies have examined the impact of digital transformation on financial services, particularly focusing on the rapid growth of online payment systems. Researchers highlight that digital payment platforms such as UPI, mobile wallets, and internet banking have significantly improved transaction efficiency and financial inclusion ***(Sharma, 2021)***. However, the literature also emphasizes that increased digital adoption has expanded the attack surface for cybercriminal activities ***(Kumar & Singh, 2022)***.

Existing research widely discusses the **security challenges** associated with online payment systems. Studies indicate that cyber threats such as phishing, malware attacks, SIM swap fraud, and unauthorized access are among the most frequently reported incidents in digital transactions

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

(Patel, 2020). These threats often exploit both technological loopholes and human vulnerabilities, making cybersecurity a multi-dimensional problem ***(Rao, 2021).***

Several authors have focused on the **role of users in cybersecurity incidents**, noting that lack of awareness, poor password management, and unsafe browsing practices significantly contribute to successful cyber attacks ***(Mehta & Joshi, 2019)***. Research findings suggest that even advanced security systems may fail if users are unaware of basic cyber hygiene practices ***(Verma, 2022)***.

From a technical perspective, prior studies analyze vulnerabilities in payment system architectures, including weak authentication mechanisms, insecure APIs, and inadequate encryption standards ***(Chaudhary et al., 2021)***. While security measures such as OTP-based verification and two-factor authentication are commonly implemented, researchers argue that these mechanisms alone are insufficient against sophisticated and evolving cyber threats ***(Gupta, 2023).***

Recent literature also explores **advanced security solutions**, including artificial intelligence and machine learning-based fraud detection systems. These technologies are shown to enhance real-time monitoring and anomaly detection in online transactions ***(Iyer & Nair, 2022)***. However, multiple studies indicate that such solutions require continuous training, quality data, and regulatory support to remain effective ***(Das, 2023)***.

Despite extensive research, certain gaps remain in the existing literature. Many studies focus on individual payment methods or specific cyber attacks, rather than providing a comprehensive overview across multiple platforms ***(Banerjee, 2021).*** Additionally, limited research addresses the combined impact of technical vulnerabilities and user behavior, particularly in developing economies with diverse levels of digital literacy ***(Malhotra, 2022)***.

5. Cybersecurity Threats in Online Payment systems

The rapid expansion of online payment systems has introduced multiple cybersecurity threats that target both users and financial infrastructures. Cybercriminals exploit technological weaknesses, human errors, and insecure communication channels to gain unauthorized access to sensitive financial information. These threats not only cause monetary losses but also damage user trust and system reliability. Understanding the nature of these cyber threats is essential for designing effective security controls and ensuring safe digital transactions.

Online payment threats can broadly be categorized based on **attack methods**, **target entities**, and **intent**, such as data theft, financial fraud, or identity compromise.

The most common **cybersecurity threats** affecting digital payment platforms are discussed below:-

A. Phishing Attacks

Phishing attacks involve deceiving users into revealing sensitive information such as login credentials, OTPs, or card details through fake emails, messages, or websites. In online payments,

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

attackers often impersonate banks, payment apps, or customer support services to trick users into sharing confidential data.

B. Malware and Spyware

Malware refers to malicious software designed to infiltrate devices and steal sensitive data. Spyware can silently monitor user activities such as keystrokes and transaction details. Infected mobile devices used for digital payments are particularly vulnerable, leading to unauthorized transactions without the user's knowledge.

C. SIM Swap Fraud

SIM swap fraud occurs when attackers fraudulently obtain control of a victim's mobile number by issuing a duplicate SIM card. Once successful, attackers can intercept OTPs and authentication messages, enabling them to perform unauthorized online payment transactions.

D. Man-in-the-Middle (MITM) Attacks

In MITM attacks, cybercriminals secretly intercept communication between users and payment systems. This commonly occurs over unsecured public Wi-Fi networks, allowing attackers to capture sensitive transaction data or manipulate transaction details.

E. QR Code Fraud

QR code-based payments are widely used due to their convenience, but attackers exploit this by replacing legitimate QR codes with fraudulent ones. Users unknowingly transfer money directly to attackers' accounts instead of intended recipients.

F. Fake Mobile Applications

Cybercriminals develop fake payment applications that closely resemble legitimate apps. When users install these apps, attackers gain access to login credentials, personal information, and financial data, resulting in large-scale fraud.

G. Social Engineering Attacks

Social engineering attacks manipulate human behavior rather than exploiting technical vulnerabilities. Attackers gain users' trust through phone calls or messages and persuade them to disclose sensitive information, approve fraudulent transactions, or install malicious software.

❖ **Threat vs Impact Table**

Threat Type	Target Area	Potential Impact	Risk Level
Phishing Attacks	User credentials	Identity theft, account takeover	High
Malware & Spyware	Mobile devices	Unauthorized transactions, data leakage	High
SIM Swap Fraud	Mobile authentication	OTP interception, financial loss	High
MITM Attacks	Network communication	Data interception, transaction manipulation	Medium

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

QR Code Fraud	Payment interface	Direct financial loss	Medium
Fake Mobile Applications	User devices	Credential theft, privacy breach	High
Social Engineering	Human behavior	Fraudulent transactions, data exposure	High

6. Vulnerabilities in Online Payment systems

While online payment platforms incorporate multiple security mechanisms, cyberattacks continue to succeed primarily due to underlying vulnerabilities within the system and its users. Vulnerabilities represent weaknesses that can be exploited by attackers to gain unauthorized access, manipulate transactions, or steal sensitive information. Understanding these vulnerabilities is essential to identify why cybersecurity threats persist despite technological advancements.

6.1 Weak Authentication Mechanisms

Weak or poorly implemented authentication mechanisms significantly increase the risk of unauthorized access. Many online payment systems rely on single-factor authentication such as passwords or PINs, which can be easily compromised through phishing, brute-force attacks, or credential reuse. In some cases, OTPs are intercepted through SIM-swap fraud or malware-infected devices, reducing their effectiveness. Absence of multi-factor or adaptive authentication makes payment systems vulnerable to account takeover attacks.

6.2 User Negligence and Lack of Cyber Awareness

Human behavior remains one of the weakest links in cybersecurity. Users often fall victim to fraudulent messages, fake payment links, and social engineering attacks due to lack of awareness. Sharing OTPs, clicking on unverified QR codes, installing unknown applications, or ignoring security warnings exposes users to financial fraud. Cybercriminals exploit trust, urgency, and fear to manipulate users rather than attacking systems directly.

6.3 Insecure Mobile Devices

Mobile devices are the primary medium for online payments, making them a critical attack surface. Devices running outdated operating systems, lacking security patches, or infected with malicious applications pose serious risks. Rooted or jailbroken devices further weaken built-in security controls. Malware and spyware installed on such devices can capture keystrokes, screen content, or authentication credentials, leading to unauthorized transactions.

Airo International Journal
Peer-Reviewed
Multidisciplinary

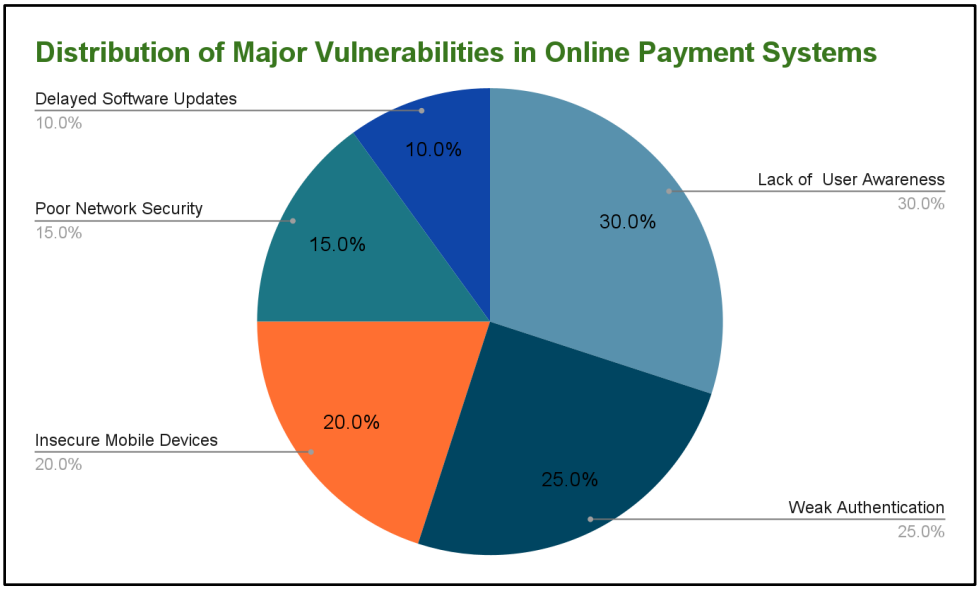
ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

6.4 Poor Network Security

Using unsecured public Wi-Fi networks for financial transactions increases vulnerability to man-in-the-middle (MITM) attacks. Attackers can intercept, alter, or monitor data transmitted over insecure networks. Weak encryption protocols, misconfigured routers, and lack of secure communication channels further expose transaction data to cyber threats. Poor network hygiene at both user and service-provider levels contributes to data leakage and fraud.

6.5 Lack of Timely Software Updates

Delayed or ignored software updates create exploitable security gaps in payment applications and devices. Cyber attackers often target known vulnerabilities for which patches already exist but have not been applied. Payment apps, operating systems, and backend servers that are not regularly updated remain susceptible to malware infections, privilege escalation, and data breaches.



7. Cybersecurity Threats in Online Payment Systems

Key Cybersecurity Threats

Phishing remains top, where fraudsters send urgent messages posing as banks, urging clicks on malicious links that harvest card numbers. Ransomware locks payment gateways until ransom is paid, disrupting services for businesses. Distributed denial-of-service (DDoS) floods servers, halting transactions during peak hours like sales events. Data breaches from poor storage leak card details for card-not-present fraud, where thieves buy online without the physical card. Advanced persistent threats (APTs) from state actors target financial firms for espionage or sabotage.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

Core Prevention Techniques

Two-factor authentication (2FA) adds a second step, such as an app notification or hardware key, after password entry. It stops 99% of bulk attacks since hackers rarely control your phone too. OTP-based verification sends a short-lived code via SMS or app for each payment, expiring in minutes to block replay attacks. Encryption like SSL/TLS wraps data in a secure "tunnel" using public-private keys; browsers show padlock icons when active. Tokenization replaces sensitive card data with random tokens in merchant systems—breaches yield useless info.

Implementing for Businesses

Payment providers adopt PCI DSS standards mandating encryption and audits. Apps enforce device binding, where payments tie to specific phones via IMEI. Regular penetration testing simulates hacks to find gaps. Zero-trust models verify every transaction, never assuming safety. For users in Mumbai, RBI guidelines push UPI apps toward biometrics over SMS OTPs, cutting SIM swap risks. Banks offer transaction limits and cool-off periods for high-value sends.

Challenges and Future Trends

Mobile malware evades antivirus, needing behavioral AI guards. Quantum computing threatens current encryption, spurring post-quantum algorithms. Regulations like GDPR or India's DPDP Act fine non-compliance heavily. Emerging fixes include blockchain for tamper-proof ledgers and federated learning for privacy-safe AI training across banks.

8. Real-World Incidents

UPI Phishing Scams

In the 2023 Mumbai case, a retired teacher got a call from a fake bank officer warning her account would freeze unless she updated KYC via a link. Panicked, she clicked and entered UPI PIN and card info; scammers drained ₹1.5 lakhs in minutes to mule accounts. What went wrong: Trusting unsolicited calls and sharing PINs—phishers use fear tactics mimicking real banks with logos. Prevention mirrors earlier defenses: User awareness trains spotting fake caller IDs or urgent demands; never click links—call bank back on official numbers. Enable 2FA/OTP for logins, and apps now flag risky links. Banks pushed RBI alerts in 2024, cutting such scams by verifying calls. Another FY24 trend: "Digital arrest" phishing where fraudsters pose as police, claiming you're in a money laundering probe.

QR Code Fraud Cases

Bajaj Electronics scam in Hyderabad (Sep 2024) hit hard: Gang bought TVs on credit via UPI QR scans, then accomplice filed fake chargebacks from Rajasthan, reversing ₹4 crore after goods left stores. Flaw: Retailers handed items pre-full confirmation; UPI refunds exploited without goods return proof. In daily scams, fraudsters share malicious QR codes in WhatsApp groups promising

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

cashback. Scanning debits instead—Lucknow homemaker lost ₹25,000 thinking it was a refund. Issue: Blind trust in shared codes without preview.

SIM Swap Incidents

Kolkata small business owner in 2024 fell to SIM swap: Hackers convinced telco to port his number, grabbing OTPs for UPI access and siphoning ₹50,000 to crypto wallets. What failed: Telcos weak ID checks; victim ignored "SIM change" alerts. Wider 2023-24 pattern: Low-income users lost via swapped SIMs during OTP verification for loans. Malware first stole bank details, then swap enabled takeover. Root cause: SMS OTP reliance without biometrics. Avoidance steps: Lock SIM with PIN at telco; prefer app-based authenticators over SMS. Biometrics tie UPI to device fingerprint—can't swap that. RBI mandated 2FA upgrades in 2025, plus AI spotting location mismatches like Mumbai SIM suddenly in Bihar.

Broader Impacts and Fixes

These hit homemakers to chains, eroding trust—1 in 5 families faced UPI fraud by 2025. Post-incident, victims report to the 1930 helpline for refunds within hours if quick. Multi-layer model applies: Awareness outermost blocks phishing; access layers (OTP/biometrics) stop swaps; data shields (encryption) neuter QR thefts; AI watches patterns like rapid refunds. For Mumbai users, NPCI's UPI 2.0 adds face auth, slashing SIM risks.

9. Data Analysis

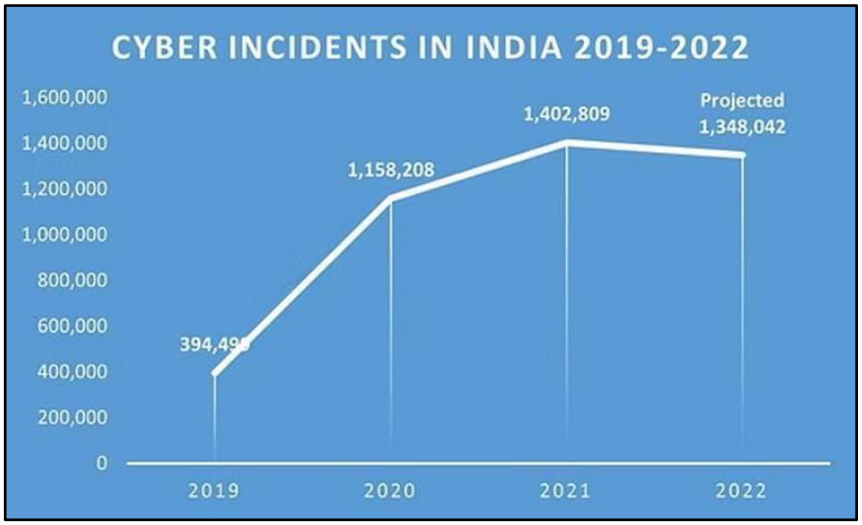
Digital payment frauds in India, especially UPI, have spiked with adoption but show recent moderation through better defenses. Data analysis reveals phishing as dominant, with year-over-year case surges peaking in FY24 before dipping.

Threat Distribution

Phishing tops threats at 62% of incidents, as it tricks users into sharing payment details via fake sites or calls. Invoice/payment fraud follows at 37%, often in B2B setups, while identity theft hits 32% by stealing logins for account takeovers.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT



Fraud Trend Over Years

UPI cases exploded from ~2.7 lakh in FY23 to 13.42 lakh peak in FY24 amid transaction boom, but fell to 12.64 lakh FY25 and 10.64 lakh FY26 (till Nov) as AI and regs kicked in. Losses mirrored: Rs 573 crore FY23 to Rs 1087 crore FY24, then Rs 981 crore FY25, Rs 805 crore partial FY26—share tiny vs 200 trillion rupees yearly volume.

Threat vs Solution Comparison

Threat Type	Key Issue	Best Security Solution	Effectiveness Notes
Phishing	Fake links/calls steal PIN	User Awareness + AI Detection	Blocks 80-90%; train + filter emails
QR Code Fraud	Malicious scans debit cash	Tokenization + Dynamic QR	Hides details; expires codes fast
SIM Swap	OTP hijack via telco	Biometrics + App Auth	Device-bound; no SMS reliance

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

Account Takeover	Stolen creds	2FA/OTP + Encryption	Multi-step verifies; scrambles data
Malware/Keyloggers	Device spies inputs	AI Fraud Monitor	Real-time flags odd patterns

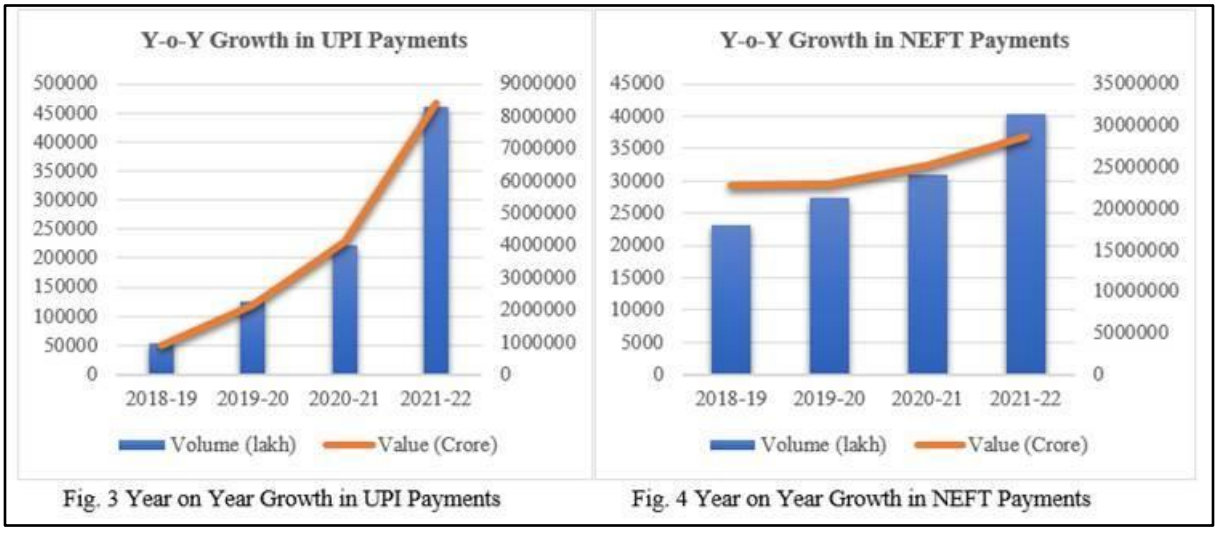


Fig. 3 Year on Year Growth in UPI Payments

Fig. 4 Year on Year Growth in NEFT Payments

Insights

Phishing drives 80%+ incidents, but layered fixes cut growth—FY26 down 16% cases. Mumbai users see high UPI volume; focus biometrics as per RBI. Overall, fraud <0.01% transactions proves systems resilient with vigilance.

10. Challenges in Securing Online Payment Systems

Cybercriminals shift tactics quickly, from basic phishing to AI-powered deepfakes that mimic bank calls perfectly. Traditional firewalls miss zero-day exploits or polymorphic malware that mutates code mid-attack, hitting UPI apps before patches arrive. In India, UPI fraud jumped 85% in FY24 partly due to these adaptive scams blending social engineering with ransomware. Prevention builds on layers: AI fraud detection scans real-time for odd patterns like sudden location jumps, while regular app updates close holes.

User Awareness Gaps

Many users ignore basics, reusing weak passwords across apps or clicking QR codes from strangers, fueling 62% phishing losses. Low digital literacy in rural India means small traders skip

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

2FA, thinking it slows sales. Mumbai street vendors often share OTPs over phone, inviting SIM swaps. Fixes include simple bank campaigns: Short videos quiz on spotting fakes, with rewards for enabling biometrics. Apps nudge one-tap awareness pop-ups, boosting compliance without overload.

Complex Infrastructure

Payment chains span banks, apps, telcos, and merchants—any weak link exposes all, like unpatched POS terminals leaking card data. Legacy systems clash with new UPI, creating hybrid vulnerabilities hard to audit. Global supply chains add risks, as third-party APIs feed breaches. Streamline via standards like PCI DSS audits and zero-trust models that verify every hop. Tokenization cuts data flow, so even if one node falls, tokens prove useless elsewhere.

Convenience vs Security Balance

Biometrics feel invasive, OTPs delay checkouts by 10 seconds, and transaction caps annoy high-volume users like e-commerce pros. Friction drops sales—studies show 20% cart abandonment from extra steps—yet lax rules invite takeovers. Smart trade-offs: Frictionless options like device-bound face ID speed logins, adaptive 2FA skips repeats on trusted devices, and AI auto-approves routine low-risk pays. User tests refine these, keeping security tight without feelable drag.

11. Future Scope

AI and Machine Learning in Fraud Detection

AI watches every transaction live, learning normal spending habits like your usual coffee shop buys or monthly bills. It flags weird jumps, such as a sudden big transfer from Mumbai to overseas at midnight, blocking fraud before money moves. Machine learning improves over time—after spotting one scam pattern, it predicts similar ones across millions of users, slashing false alarms from 20% to under 5%. Banks already test this: Models analyze device type, location speed, and even typing rhythm to score risk. In UPI, NPCI plans full rollout by 2027, potentially saving billions yearly as fraud dips with shared data pools.

Behavioral Authentication

This goes beyond fingerprints by tracking how you act—swipe speed, app navigation paths, or mouse wiggles. A hacker with your password or face scan fails because their habits mismatch your unique style, like hesitating on PIN entry. Continuous checks run silently in the background, approving routine logins without pop-ups. India trials link it to Aadhaar biometrics, creating "behavioral fingerprints" tied to phones. It beats static methods, dodging SIM swaps since stolen SIMs can't mimic your gait or hold patterns during walks.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

Blockchain-Based Payments

Blockchain creates tamper-proof ledgers where each payment links in a chain no one can alter without group consensus. No central server means no single hack point—think UPI on steroids, with smart contracts auto-releasing funds only after delivery proofs. Stablecoins or CBDCs like digital rupee use it for instant cross-border sends without banks holding data. RBI pilots show 99.9% uptime and fraud under 0.001%, as every step logs publicly verifiable hashes. Merchants love it for disputes; users get privacy via zero-knowledge proofs hiding amounts.

Advanced Biometric Security

Next-gen scans mix iris, vein patterns, and 3D face maps, stored as math templates not images—impossible to fake with photos. Multi-modal fuses them: Ear shape plus voice timbre verifies even if one glitches. Wearables like smartwatches add heart rhythm biometrics, pulsing uniquely during stress. Gartner predicts 80% adoption by 2030, with edge AI on phones processing locally for privacy. UPI 3.0 integrates gait via phone sensors, blocking remote hacks entirely.

12. Comparison of Future Solutions

Tech Area	Key Benefit	Challenge to Adopt	Impact on Fraud Rate
AI/ML Fraud Detection	Real-time pattern spotting	Needs big data training	-70% predicted
Behavioral Auth	Invisible user profiling	Privacy concerns	-50% takeovers
Blockchain Payments	Immutable transaction logs	Scalability for peaks	Near-zero disputes
Stronger Regulations	Industry-wide enforcement	Compliance costs for small biz	-40% overall
Advanced Biometrics	Multi-factor foolproofing	Hardware upgrades needed	-60% unauthorized

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

Recap of Major Threats

Discussions highlighted phishing as the top danger, fooling 62% of victims into sharing PINs via fake bank calls or links, like the Mumbai teacher's ₹1.5 lakh hit. QR code frauds tricked merchants into early handovers, as in Hyderabad's ₹4 crore Bajaj scam, while SIM swaps let hackers grab OTPs, draining Kolkata accounts swiftly. Trends showed UPI cases surging from 2.7 lakh in FY23 to a 13.42 lakh peak in FY24 before easing to 10.64 lakh by late FY26, with phishing, payment fraud (37%), and identity theft driving most losses totaling over ₹3,500 crore.

Role of Proven Security Mechanisms

Core tools like two-factor authentication (2FA) demand a phone code post-password, blocking 99% of bulk attacks since thieves rarely control two steps. OTP verification ties approvals to short-lived messages, useless if delayed. Encryption via SSL/TLS scrambles data in transit—padlock icons confirm it—while tokenization swaps card numbers for junk tokens, neutering stolen databases. Biometrics lock devices to fingerprints or faces, hard to spoof, and AI fraud detection scans habits like location jumps or odd timings, auto-freezing suspects. User awareness campaigns teach spotting fakes via bank quizzes and alerts.

Mechanism	Blocks Primarily	Real-World Win
2FA/OTP	Account Takeover	Stops 80% post-phish entry
Tokenization	Data Breaches	Useless in merchant hacks
AI Detection	Pattern Anomalies	Flags midnight overseas buys
Biometrics	SIM Swaps	Device-bound, no phone needed

This table shows targeted fits, with layers compensating weaknesses for near-total coverage.

Imperative for Continuous Improvement

Threats never sleep—AI deepfakes now mimic voices perfectly, quantum tech eyes encryption cracks by 2030, and global chains add unseen weak spots. Static setups fail; FY24 peaks proved one-size-fits-all crumbles under volume. Regular penetration tests, app patches, and shared NPCI blacklists keep ahead, while user habits evolve via nudges like mandatory training pop-ups.

Positive Forward Outlook

Yet hope shines bright—fraud stays below 0.01% of India's 200 trillion rupee annual volumes, a testament to resilience. Future stars like behavioral authentication tracking swipes, blockchain's

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

unchangeable ledgers for UPI-CBDC hybrids, and RBI's UPI 3.0 with gait scans promise invisible armor. Stronger rules under DPDP Act enforce AI audits, while banks roll frictionless biometrics. Imagine worry-free scans at chai stalls or instant global sends. Users enabling all features today—biometrics on, limits set, apps updated—join this wave.

13. References

1. Rising Threats in Digital Payments(https://www.qrcsolutionz.com/blog/rising-threats-in-digital-payments)
2. Top Cybersecurity Strategies for Online Payment Security(https://moldstud.com/articles/p-cybersecurity-strategies-for-online-payment-security)
3. Cybersecurity Threats to Digital Payments(https://akitra.com/blog/cybersecurity-threats-to-digital-payments/)
4. UPI Fraud Statistics in India: Rising Cases in 2025 (https://aseemjuneja.in/upi-fraud-statistics-india/)
5. Digital Deception: Case Study of UPI Scams (https://www.linkedin.com/pulse/digital-deception-case-study-upi-scams-phishing-utlpf)
6. UPI Frauds: Types & Prevention (https://razorpay.com/blog/upi-frauds-types-tactics/)
7. UPI Frauds Peak in FY24, Signs of Decline (https://yourstory.com/2025/12/upi-frauds-peak-in-fy24-show-signs-of-decline-parliament-data)
8. UPI Frauds: Indians Lose Rs 2145 Crore (https://bfsi.economictimes.indiatimes.com/news/fintech/upi-frauds-indians-lose-rs-2145-crore-across-2-7-million-reported-incidents-since-2022-23-says-govt/115750262)
9. Rise of UPI Frauds (https://iserveu.in/blog/frm/2025/10/23/rise-of-upi-frauds-iserveus-preventive-approach/)
10. Most Common Cyberthreats Chart (https://www.statista.com/chart/amp/35676/most-common-type-of-cyberattack/)
11. Security in Digital Payment Systems (https://www.ijert.org/security-and-vulnerability-in-digital-payment-systems)
12. Mitigating Cyber Threats in Digital Payments (https://philarchive.org/archive/PRAMCT)
13. Unified Payments Interface (UPI) – Overview and Features https://www.npci.org.in/what-we-do/upi/product-overview
14. Phishing and Online Banking Fraud Prevention Tips https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
15. Mobile Banking and Payment Security Guidelines https://www.cisa.gov/news-events/news/tips-using-public-wi-fi-networks
16. UPI Fraud: Types, Trends and Prevention https://razorpay.com/blog/upi-frauds-types-tactics/

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume:2 Issue:1
April 2026
Impact Factor: 10.1
Subject: IT

Author's Declaration

As an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my hole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible, shuffled, or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who find trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher, then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website, or the watermark of remark/actuality may be mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Lavlesh Bagwe
Ankit Chaudhary

******