AI-Driven Threat Detection for UPI and ONDC Platforms: An Empirical Study of Cybersecurity Risks, Trust, and Digital Payment Resilience in India

*Siddarth Nagamurthy Madankar**

DOI: https://doi.org/10.5281/zenodo.19499747

ABSTRACT

This empirical research article examines cybersecurity risks in India's Unified Payments Interface (UPI) and the Open Network for Digital Commerce (ONDC), focusing on user-behavior vulnerabilities, platform-level risks, and artificial intelligence's role in threat detection. UPI's rapid expansion has increased exposure to phishing, malicious links, identity compromise, malware, and social-engineering frauds. ONDC's open-network design introduces additional trust, privacy, and security challenges due to multi-participant data exchange. The study uses mixed empirical methods-structured surveys and secondary literature-to assess risk perception, digital-payment trust, cybersecurity awareness, and AI-driven fraud monitoring acceptance. Findings indicate behavioral gaps remain primary vulnerabilities, while AI-driven anomaly detection, continuous authentication, and real-time risk scoring significantly improve fraud prevention and user confidence. The study concludes that cybersecurity in open digital commerce requires technical controls, platform governance, and user education to sustain fintech ecosystem trust.

KEYWORDS: *Upi, Ondc, Cybersecurity, Ai Detection, Payment Trust.*

* **Dr. Siddarth Nagamurthy Madankar,** Assistant Professor, Department of Commerce, Dr. Ambedkar College of Arts, Commerce and PG Centre, Kalaburagi.

Introduction:

India's digital public infrastructure has transformed payments and commerce through scalable, low-friction interoperability across banks, fintech firms, merchants, and consumers. UPI powers everyday transactions while ONDC extends digital openness to commerce, reducing closed-platform dependence. This expansion creates economic opportunities but widens cyber fraud, data misuse, identity deception, and API vulnerability exposure. Recent evidence shows rising UPI usage accompanies increased phishing, fraudulent requests, fake links, identity theft, and human-error exploits. ONDC's networked commerce depends on multi-actor interoperability, where trust hinges on privacy protection, secure data exchange, grievance redressal, authentication controls, and visible fraud prevention. AI-driven detection identifies suspicious patterns, flags anomalous transactions in real time, and supports adaptive responses beyond rule-based systems. This study investigates whether AI-enabled cybersecurity strengthens trust in UPI- and ONDC-linked digital payment environments.

Need for the Study Digital payments growth has elevated cybersecurity to a public trust issue. Government reports show sharp cyber incident rises, reflecting digital exposure and fraud sophistication. ONDC's open design raises governance questions about accountability, secure data-sharing, and user protection in distributed commerce. Empirical research connecting user behavior, platform vulnerabilities, and AI detection within one framework is urgently needed.

Objectives of the Study

- To identify major cybersecurity risks affecting UPI users and ONDC-linked digital commerce participants.
- To examine cybersecurity awareness's relationship with digital payment trust.
- To assess platform security safeguards' influence on UPI/ONDC transaction willingness.
- To evaluate AI-driven fraud detection's effectiveness in strengthening payment trust.
- To propose policy and managerial measures for cybersecurity

resilience in open digital commerce.

Research Questions

- What are the most significant user- and system-level cybersecurity risks in UPI/ONDC ecosystems?
- Does cybersecurity awareness significantly improve digital payment trust?
- Do platform safeguards improve ONDC-linked commerce willingness?
- Can AI-driven threat detection increase perceived safety and trust?

Hypotheses

- H1: Cybersecurity awareness positively relates to UPI digital payment trust.
- H2: Platform security safeguards positively relate to ONDC commerce willingness.
- H3: AI-driven threat detection effectiveness positively relates to digital payment trust.
- H4: Prior cyber fraud exposure negatively relates to digital payment trust.
- H5: AI-driven detection moderates cyber risk's negative effect on payment trust.

Methodology

This descriptive-analytical study uses mixed methods. Primary data come from structured questionnaires administered to 220 UPI users, online buyers, small merchants, and digital consumers in urban/semi-urban India. A five-point Likert scale measures cybersecurity awareness, cyber risk perception, platform safeguards, prior fraud exposure, AI detection effectiveness, and payment trust. Secondary data draw from academic articles, policy reports, and sectoral analyses on UPI fraud, ONDC architecture, and AI fraud detection.

Sample Design

Convenience-purposive sampling targets active digital payment users (students, salaried, self-employed, merchants). This supports behavioral/perceptual assessment in evolving fintech

contexts.

Variables

Variable	Type	Description
Cybersecurity awareness	Independent	Phishing, suspicious links, PIN sharing, app permissions understanding
Perceived cyber risk	Independent	Fraud likelihood, data theft, identity misuse perception
Platform safeguards	Independent	Authentication, alerts, support, grievance redressal perception
Prior fraud exposure	Independent	Experienced/observed digital payment fraud
AI-driven detection	Independent / Moderator	AI anomaly detection, fraud blocking perception
Payment trust	Dependent	UPI/ONDC system confidence
Usage willingness	Dependent	Continued UPI/ONDC channel usage likelihood

Analysis Tools

Percentage analysis, weighted means, chi-square, correlation, multiple regression examine awareness-risk-trust-AI relationships.

Data Analysis and Interpretation

Demographic Profile Sample (n=220): 21-35 age group dominant (48%), reflecting mobile-first digital payment users. Daily UPI usage (64%) indicates deep transaction embedding, increasing cyber exposure.

Threat Awareness

Profile	Category	Percentage
Age	18-20	14%
	21-35	48%
	36-50	26%
	>50	12%
Occupation	Student	22%
	Salaried	38%
	Self-employed	21%
	Merchant	19%
UPI Frequency	Daily	64%
	Weekly	24%
	Occasional	12%

High OTP/PIN awareness (84%), lower QR/malicious-link recognition (59%).

The data shows that UPI users are predominantly young adults (21–35 years), with a strong presence of salaried professionals, indicating a financially active and digitally comfortable group. Usage is very high, with most users making daily transactions, reflecting strong adoption of digital payments. Overall, the audience is diverse but centered around working individuals who rely heavily on UPI for regular financial activities.

Threat	Aware
Fake link/APK	71%
Fraudulent collect	67%
OTP/PIN sharing	84%
QR-code	59%
Impersonation	76%

The data indicates a high overall risk of digital fraud, with all categories showing significant vulnerability (59%–84%). The highest risk is OTP/PIN sharing (84%), followed by impersonation (76%) and fake links/APK (71%), highlighting that scams exploiting human trust and awareness gaps are most effective. While QR code (59%) and fraudulent collect (67%) scams are slightly lower, they still pose notable threats. Overall, the interpretation shows that behavior-based scams are more successful than purely technical ones, emphasizing the need for better user awareness and caution.

Weighted Means (1-5 Likert)

Statement	Mean	Interpretation
UPI convenient but vulnerable	4.18	High
ONDC needs visible security	4.26	High
AI detects real-time behavior	4.31	Very high
Awareness campaigns sufficient	2.64	Low
Grievance redressal builds trust	4.09	High

The data indicates that users place strong emphasis on security and trust in digital platforms. The highest rating is for AI-based real-time behavior detection (4.31), suggesting a very high level of confidence in advanced technological solutions for fraud prevention. Similarly, the need for visible security measures

in ONDC (4.26) and concerns about UPI being convenient yet vulnerable (4.18) reflect that users are highly aware of security risks and expect stronger safeguards. Grievance redressal systems (4.09) are also considered important, showing that efficient complaint handling contributes significantly to building user trust. In contrast, awareness campaigns received a low rating (2.64), indicating that current efforts to educate users about security and safe practices are perceived as insufficient. Overall, the findings highlight that while users appreciate convenience, their trust depends heavily on robust security systems, transparency, and effective support mechanisms, with a clear need for improved awareness initiatives.

Correlation Matrix:

Variables	Trust
Awareness	0.58
Safeguards	0.62
AI effectiveness	0.69
Cyber risk	-0.51
Prior fraud	-0.44

Positive factors (Awareness, Safeguards, AI Effectiveness) strengthen outcomes, while negative factors (Cyber Risk, Prior Fraud) weaken them. The strongest drivers are AI effectiveness (positive) and Cyber Risk (negative). Efforts to improve awareness, safeguards, and AI, while mitigating cyber risk and addressing past fraud, would likely have the greatest impact on success. AI effectiveness shows strongest trust correlation.

Regression Results AI detection and safeguards strongest trust predictors. Supports H1-H5.

Findings

- Behavioral gaps drive UPI vulnerability (phishing, QR scams).
- ONDC interoperability creates trust opportunities but governance challenges.
- Awareness improves trust but insufficient alone.
- Safeguards (alerts, authentication) boost transaction willingness.
- AI detection most promising trust-builder via anomaly recognition.

- Prior fraud reduces trust, emphasizing recovery systems.

Limitations:

Perception-based survey misses technical complexity. Convenience sampling limits generalizability. Evolving ONDC alters security expectations. AI assessment perception/secondary-based, not proprietary data.

Suggestions:

- Intensify behavior-based cybersecurity education.
- The Open Network for Digital Commerce (ONDC) adopt API/ identity/verification standards.
- Integrate AI for real-time anomaly detection.
- Implement visible safeguards (alerts, authentication).
- Promote interoperable cyber governance.
- Future: larger samples, longitudinal, merchant data.

Conclusion:

Cybersecurity is strategic for India's digital infrastructure growth. Unified Payments Interface (UPI) and the Open Network for Digital Commerce (ONDC), depend on user trust, secure exchange, rapid fraud response. Empirical model shows awareness, safeguards, AI positively shape trust; risk/exposure weaken it. AI threat detection enables trust in open fintech ecosystems.

References:

1. A review of ONDC's digital warfare in India taking on the e-commerce giants. (2022, October 29). SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323963
2. An empirical study on cybersecurity risks in UPI-based digital payments. (2026, February 28). International Journal of Science and Research. https://www.ijsr.net/getabstract.php?paperid=SC26210223931
3. Nageshnanda. (2026, February 28). World Bank's 2026 report exposes UPI fraud risks in India. LinkedIn. https://www.linkedin.com/posts/nageshnanda_upi-fintech-cyberfraud-activity-7433853729281318912-pRoR
4. Press Information Bureau. (2025, November 19). Curbing cyber frauds in Digital India. Government of India. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146
5. PwC India. (n.d.). The five Es to drive digital commerce. https://www.pwc.in/assets/pdfs/research-insights/research-insights-hub/the-five-es-to-drive-digital-commerce.pdf
6. RMA India. (2026, March 22). India cybersecurity spending to hit $3.4 billion. https://rmaindia.org/indias-information-security-spending-set-to-reach-3-4-billion-in-2026/