Advances in Consumer Research
https://acr-journal.com/
Volume-3 | Issue-11 |0ct: 2026
Original Researcher Article

Emerging Cybersecurity Technologies and Fraud Detection Mechanisms

Dr.B.Navaneetha[1], Dr.K.Latha[2]
Assistant Professors Department of B.Com (Professional Accounting)PSG College of Arts & Science
Coimbatore – 14
Email id –[1]naviravichandar@gmail.com , [2]latha@psgcas.ac.in

ABSTRACT
The rapid expansion of digital technology has increased the use of online banking, digital payments and electronic services, making digital identity security increasingly important. However, cyber threats such as identity theft, phishing, data breaches and financial fraud pose serious challenges to individuals and organizations. This study examines the relationship between cybersecurity, digital identity and fraud prevention, focusing on emerging threats and protective measures. It highlights the role of artificial intelligence, biometric authentication, multi-factor authentication and encryption in securing digital transactions. The study follows a descriptive research approach using secondary data from academic publications, government reports and institutional sources. It emphasizes the need for effective security policies, regulatory measures and digital awareness to minimize cyber fraud and promote a safe and trustworthy digital environment.
Keywords: Cybersecurity, Digital Identity, Fraud Prevention, Identity Theft, Artificial Intelligence, Digital Banking, Data Protection, Digital Authentication.

1. INTRODUCTION

The digital revolution has significantly changed the global economic and social environment. The widespread adoption of internet banking, mobile applications, digital payments, e-commerce, cloud computing and government e-services has increased the importance of digital identity. Individuals increasingly depend on digital platforms to establish their identity, access services and conduct financial transactions. Digital identity refers to the electronic representation of an individual, organization or entity through identifiable information and authentication credentials. It may include personal details, usernames, passwords, biometric information, digital certificates and other electronic identifiers. A secure digital identity enables individuals to access online services while helping organizations verify users and protect confidential information. At the same time, the expansion of digital connectivity has increased exposure to cyber threats. Cybercriminals use sophisticated techniques such as phishing emails, fraudulent websites, identity impersonation, malicious software, SIM swapping and artificial intelligence-based scams to obtain confidential information and commit financial fraud.

In India, the rapid growth of Unified Payments Interface (UPI), internet banking and mobile-based financial services has made digital security particularly important. Although digital transactions provide convenience and financial inclusion, weaknesses in authentication practices, limited cybersecurity awareness and misuse of personal information can expose users to financial losses. Therefore, cybersecurity and digital identity management are no longer merely technical responsibilities. They have become essential components of financial security, consumer protection and sustainable digital development. Effective fraud prevention requires a combination of technological innovation, regulatory compliance, institutional responsibility and individual awareness.

Review of Literature

Al-Hashedi and Magalingam (2021)[1] have conducted a study entitled Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review from 2009 to 2019. The study examined various data mining techniques used to identify financial fraud across different sectors. The findings highlighted the importance of data mining and machine learning in detecting suspicious financial transactions. The researchers emphasized the need for advanced analytical techniques to improve fraud identification and minimize financial losses.

Hernandez Aros et al. (2024)[2] have undertaken a study entitled Financial Fraud Detection through the Application of Machine Learning Techniques: A Literature Review. The study reviewed previous research on the application of machine learning in financial fraud detection. The findings revealed that machine learning algorithms play an important role in identifying fraudulent credit card transactions and unusual financial activities. The study also highlighted the importance of selecting appropriate algorithms and datasets to improve fraud detection accuracy.

Kavya and Sumathi (2024/2025)[3] have conducted a study entitled Staying Ahead of Phishers: A Review of Recent Advances and Emerging Methodologies in Phishing Detection. The study examined different phishing detection methods, including traditional machine learning and advanced deep learning techniques. The findings indicated that intelligent detection systems can help identify fraudulent websites, emails and online activities. The researchers highlighted the importance of developing advanced security mechanisms to protect users from phishing attacks.

Research published in Computers & Security (2024)[4] entitled Machine Learning and Deep Learning for User Authentication and Authorization in Cybersecurity: A State-of-the-Art Review examined the application of

artificial intelligence in digital authentication and access control. The study highlighted the limitations of conventional password-based authentication systems and explained how machine learning and deep learning can strengthen user verification. It emphasized the importance of advanced authentication mechanisms in protecting digital identities and preventing unauthorized access.

Research Methodology

The study employs a descriptive and analytical approach to examine cybersecurity, digital identity protection and fraud prevention practices.

Research Design

A conceptual research design is adopted to explore existing digital security frameworks, identity verification systems and emerging fraud prevention techniques.

Research Approach

The study is based on secondary data collected from academic journals, government publications, institutional reports and cybersecurity guidelines. The information is analysed to understand current cyber threats, evaluate security measures and suggest strategies for strengthening digital protection.

Note: The study relies exclusively on secondary sources and does not involve primary data collection or statistical hypothesis testing.

Sources of Data

The study uses secondary data collected from the following sources:

Research articles published in national and international journals.

Reports and publications of the Reserve Bank of India (RBI).

Guidelines issued by the National Institute of Standards and Technology (NIST).

Reports published by the Indian Computer Emergency Response Team (CERT-In).

Government publications, cybersecurity frameworks and relevant websites.

Books, conference proceedings and other academic publications.

Objectives of the Study

The major objectives of the study are:

To examine the concept and significance of cybersecurity in the digital economy.

To identify the major cybersecurity threats and online financial transactions.

To analyze the various techniques and methods adopted for preventing cyber fraud.

Analysis and Discussion

The following analysis is designed for a journal article based entirely on secondary data. It examines the growth of digital transactions, cyber financial fraud, digital identity risks and emerging fraud prevention mechanisms in India.

Growth of Digital Payment Transactions in India

The rapid adoption of digital payment systems has transformed India's financial sector. UPI, mobile banking, internet banking and other electronic payment methods have improved transaction convenience and financial inclusion. However, the increasing volume of digital transactions has also created greater requirements for cybersecurity and identity verification.

The following table presents the growth of digital payment transactions in India over five financial years.

Table 1: Growth of Digital Payment Transactions in India

Financial year	Volume (crore)	Value (₹ lakh crore)
2020–21	4,370.68	1,414.58
2021–22	7,197.68	1,744.01
2022–23	11,393.82	2,086.85
2023–24	16,443.02	2,428.24
2024–25*	18,120.82	2,330.72

Source: Ministry of Finance, Government of India, Press Information Bureau, 11 March 2025.

Interpretation:

The above table indicates a substantial increase in digital payment adoption in India. Transaction volume increased from 4,370.68 crore in 2020–21 to 18,120.82 crore in 2024–25 (up to January 2025). This reflects the growing dependence on electronic payment platforms. The expansion of digital transactions also increases the importance of secure authentication, transaction monitoring and identity verification to minimize cyber risks.

1.2 Analysis of Financial Cyber Fraud in India

The increasing use of digital financial services has also resulted in growing exposure to cyber financial fraud. The following data presents the number of financial fraud complaints and the amount reported through India's National Cyber Crime Reporting Portal (NCRP)

Table 2: Financial Cyber Fraud Complaints in India (2021–2025)

Financial year	Number of complaints	Amount reported (₹ crore)
2020–21	2,62,846	551
2021–22	6,94,446	2,290
2022–23	13,10,357	7,465
2023–24*	19,18,835	22,848
2024–25	24,02,579	22,495

Source: Ministry of Home Affairs, Government of India, Rajya Sabha reply, 11 February 2026.

Interpretation:

The data reveal a significant increase in financial cyber fraud complaints during the five-year period. Complaints increased from 2,62,846 in 2021 to 24,02,579 in 2025, representing approximately a nine-fold increase. The reported amount also increased considerably, from ₹551 crore to ₹22,495 crore. Although the reported amount declined slightly in 2025 compared with 2024, the number of complaints continued to increase. This indicates the growing need for effective cyber fraud monitoring, secure digital identity verification and timely reporting mechanisms. The figures represent amounts reported by citizens and should not be interpreted as independently verified financial losses.

.

1.3 Analysis of Digital Identity-Related Cybercrime

Digital identity theft and impersonation have emerged as important concerns in the digital environment. Cybercriminals misuse personal information, online profiles and electronic credentials to deceive individuals and gain unauthorized access to digital services

Table 3: Selected Digital Identity-Related Cybercrime Complaints in India

Type of cybercrime	2021	2022	2023	2024	2025
Email phishing	798	1,364	1,272	2,008	2,240
Cheating by impersonation	12,617	20,041	18,135	19,991	23,252
Fake/impersonating profiles	15,843	23,626	30,234	39,884	46,784
Profile hacking/identity theft	10,650	26,288	33,724	38,297	34,533

Source: Ministry of Home Affairs, Government of India, Rajya Sabha Unstarred Question No. 2954, 18 March 2026.

Interpretation:

The data indicate that fake and impersonating profiles increased from 15,843 cases in 2021 to 46,784 in 2025. Similarly, email phishing complaints increased from 798 to 2,240 during the same period. Profile hacking and identity theft also recorded a substantial increase until 2024, followed by a decline in 2025. These trends highlight the vulnerability of personal information in digital platforms. The misuse of online identities can affect individuals' financial security, privacy and confidence in electronic services. Therefore, stronger identity verification, multi-factor authentication and public awareness are necessary to minimize identity-related cybercrime.

1.4 Role of Technology in Cyber Fraud Prevention

Technological developments have created new opportunities for detecting and preventing cybercrime. Artificial intelligence and machine learning can analyze transaction patterns, identify suspicious activities and generate alerts for potentially fraudulent transactions. The Government of India has reported that NPCI provides AI/ML-based fraud monitoring solutions to banks to generate alerts and decline suspicious transactions. Device binding, two-factor authentication and transaction limits are also among the security measures adopted to protect digital payments.

The major technological measures are presented below

.

Table 4: Technological Measures for Cyber Fraud Prevention

Technology	Application in fraud prevention
Artificial Intelligence	Identifies unusual transaction patterns and suspicious activities.
Machine Learning	Analyses historical data to recognize potential fraud.
Biometric Authentication	Verifies users through fingerprints and facial recognition.
Multi-Factor Authentication	Provides additional verification during account access.
Encryption	Protects confidential information during storage and transmission.
Blockchain Technology	Supports tamper-resistant transaction records and verification.

Source: Press Information Bureau

Interpretation:

The adoption of advanced technologies improves the ability of financial institutions to identify and respond to cyber threats. AI-based monitoring can support early fraud detection, while biometric and multi-factor authentication strengthen digital identity protection. However, these technologies must be supported by privacy safeguards, regular security assessments and human supervision.

1.5 Government Initiatives for Cybersecurity and Fraud Prevention

The Government of India has introduced several initiatives to strengthen cybersecurity and protect digital financial transactions. The Ministry of Home Affairs reported that the Citizen Financial Cyber Fraud Reporting and Management System had helped save more than ₹8,189 crore by 31 December 2025 through timely intervention in reported complaints

Table 5: Government Initiatives for Cybersecurity and Fraud Prevention

Initiative	Purpose
National Cyber Crime Reporting Portal	Enables citizens to report cybercrime incidents.
Helpline 1930	Provides immediate assistance for reporting financial cyber fraud.
Indian Cyber Crime Coordination Centre (I4C)	Coordinates cybercrime prevention and investigation.
CERT-In	Provides cybersecurity advisories and incident response support.
Digital Intelligence Platform	Supports action against suspected fraudulent communication.
Chakshu Facility	Enables reporting of suspected fraudulent calls, SMS and WhatsApp communications.

Source: Press Information Bureau

Interpretation:

These initiatives demonstrate the importance of institutional coordination in preventing financial cybercrime. The availability of reporting platforms and emergency helplines enables citizens to report suspicious transactions and seek timely assistance. However, effective implementation requires greater public awareness, faster complaint resolution and coordination among banks, telecom service providers and law enforcement agencies.

.

1.6 Challenges in Implementing Effective Fraud Prevention

Despite technological improvements, several challenges continue to affect cybersecurity and digital identity management

Table 6: Challenges in Implementing Effective Fraud Prevention

Major challenge	Impact
Lack of digital awareness	Users become vulnerable to phishing and social engineering.
Weak authentication	Increases the possibility of unauthorized account access.
Data privacy concerns	Creates risks associated with the misuse of personal information.
Rapid technological changes	Makes existing security measures less effective against emerging threats.
AI-powered cybercrime	Enables sophisticated impersonation and fraudulent communication.
Inadequate security infrastructure	Increases vulnerability among smaller organizations.
Cross-border cybercrime	Creates difficulties in investigation and enforcement.

These challenges indicate that cybersecurity cannot depend exclusively on technological solutions. It requires continuous improvement in policies, institutional practices, user awareness and incident response mechanisms.

Role of Government and Regulatory Institutions

Government of India:

The government plays a significant role in strengthening digital infrastructure, promoting cyber awareness and developing data protection and cybersecurity frameworks. Effective coordination among regulatory authorities, financial institutions, technology providers and users is essential for reducing cyber risks.

Regulatory Institutions

Government institutions and regulatory authorities play an important role in creating a secure digital ecosystem.

Reserve Bank of India (RBI): RBI promotes secure digital payment systems through regulatory directions, security standards, fraud risk management and customer protection measures.

Indian Computer Emergency Response Team (CERT-In): CERT-In coordinates cybersecurity incident response, issues security advisories and promotes awareness of emerging cyber threats. Its annual reports provide information on incidents handled and cybersecurity initiatives.

National Institute of Standards and Technology (NIST): NIST provides internationally recognized cybersecurity and digital identity guidelines that support secure identity proofing and authentication.

2.FINDINGS

Based on the analysis of secondary data, the following findings are identified:

Digital payment transactions have increased significantly, indicating the growing importance of cybersecurity in India's financial ecosystem.

Financial cyber fraud complaints increased substantially between 2021 and 2025.

Fake profiles, impersonation and identity theft represent significant threats to digital identity protection.

AI and machine learning provide useful mechanisms for

identifying suspicious financial transactions.
Multi-factor authentication and biometric verification can strengthen digital identity security.
Government initiatives such as NCRP, I4C and the 1930 helpline contribute to cyber fraud reporting and prevention.
Digital literacy and consumer awareness remain essential for reducing phishing, impersonation and online payment fraud.

3.SUGGESTIONS

Based on the findings, the following suggestions are proposed:
Financial institutions should strengthen digital identity verification and authentication systems.
Banks should improve real-time monitoring of suspicious financial transactions.
Individuals should avoid sharing OTPs, passwords, UPI PINs and confidential banking details.
Educational institutions should organize cybersecurity awareness programmes for students.
Organizations should conduct regular cybersecurity audits and employee training.
AI-based fraud detection systems should be adopted with appropriate privacy and accountability safeguards.
Citizens should immediately report financial cyber fraud through the 1930 helpline and the National Cyber Crime Reporting Portal.

4.CONCLUSION

The increasing complexity of cyber threats highlights the need for advanced security technologies and effective fraud detection systems. Artificial intelligence, machine learning and secure authentication methods can strengthen digital protection and minimize financial risks. The study emphasizes that continuous technological improvements, regulatory support and user awareness are essential to address emerging cybersecurity challenges. A proactive and integrated security framework will contribute to protecting digital transactions and ensuring trust in India's digital economy

REFERENCES

1. NIST Digital Identity Guidelines.
2. CERT-In Annual Reports.
3. NIST Authentication Guidelines.
4. RBI Digital Payment Security Controls.
5. Ministry of Home Affairs – Cybercrime Reporting and Investigation, 2026.
6. Ministry of Finance – Digital Payment Transactions, 2025.
7. Ministry of Home Affairs – Cybercrime Category Statistics, 2026.
8. NPCI – UPI Product Statistics.
9. Department of Financial Services – Annual Report 2024–25.
10. Journal References
11. Al-Hashedi, K.G. and Magalingam, P. (2021). Financial Fraud Detection Applying Data Mining Techniques: A Comprehensive Review from 2009 to 2019. Computer Science Review, Vol. 40, Article 100402. DOI: 10.1016/j.cosrev.2021.100402.
12. Hernandez Aros, L., Bustamante Molano, L.X., Gutierrez-Portela, F., Moreno Hernandez, J.J. et al. (2024). Financial Fraud Detection Through the Application of Machine Learning Techniques: A Literature Review. Humanities and Social Sciences Communications, Vol. 11, Article 1130. DOI: 10.1057/s41599-024-03606-0.
13. Kavya, S. and Sumathi, D. (2025). Staying Ahead of Phishers: A Review of Recent Advances and Emerging Methodologies in Phishing Detection. Artificial Intelligence Review, Vol. 58, Article 50.
14. DOI: 10.1007/s10462-024-11055.
15. Hafez, I.Y., Hafez, A.Y., Saleh, A. et al. (2025). A Systematic Review of AI-Enhanced Techniques in Credit Card Fraud Detection. Journal of Big Data, Vol. 12, Article 6. DOI: 10.1186/s40537-024-01048-8.
16. Reserve Bank of India (2024). Master Directions on Cyber Resilience and Digital Payment Security Controls for Non-Bank Payment System Operators. RBI/DPSS/2024-25/123, 30 July 2024.