International Research Journal of Multidisciplinary Scope (IRJMS), 2026; 7(2): 557-572 IRJMS

Review Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2026.v07i02.08122

Technological Advancements in Online Fraud Prevention and Legal Frameworks

Aakruti Ravi Adwani*, Ramratan Dhumal, Sunny Thomas

Ajeenkya DY Patil University (ADYPU), Lohegaon, Pune, Maharashtra, India. *Corresponding Author's Email: aakruti.adwani@adypu.edu.in

Abstract

Online fraud has become an endemic threat in the modern digitally networked world, driven by the phenomenal expansion of e-commerce, digital banking and virtual identities. Traditional detection tools are no longer adequate to cope with the speed and complexity of contemporary fraud methods. This current research presents a critical analysis of emerging technologies and legal developments for combating online fraud in industries. Ensemble models like XGBoost and AdaBoost attain over 98% detection rates, while AI-powered behavioral analysis and deep learning architectures significantly enhance real-time anomaly detection in financial systems. The research also discusses fraud typologies like phishing, identity theft, payment scams, investment fraud and AI-based deception in the metaverse. Legal mechanisms, however, lag behind and are often in arrears relative to technology, resulting in enforcement issues due to uncertainty in jurisdictions, archaic laws and definitional difference. The study urges international cooperation, standardized digital forensics and cross-border legal unification to bridge the gaps. In addition, the role of user-centric security controls, cyber hygiene awareness and explainable AI (XAI) in enabling ethical and transparent fraud prevention is highlighted. A multidisciplinary framework integrating strong technology, revised legal policy and public participation emerges as a necessary model to contain and manage the dynamic threat landscape of online fraud.

Keywords: Artificial Intelligence, Blockchain Security, Cybercrime Detection, Legal Frameworks, Online Fraud Prevention.

Introduction

The integration of Artificial Intelligence (AI) and legal frameworks is becoming increasingly essential in the fight against online fraud. AI technologies, such as machine learning (ML), natural language processing and predictive analytics, offer advanced capabilities for real-time detection and prevention of fraudulent activities, significantly enhancing the efficiency of fraud detection systems (1, 2). Blockchain technologies provide tamper-proof transaction records, enabling fraud resistance and audit transparency. Concurrent with these technological advancements, the size and sophistication of fraud have expanded, encompassing areas such as online banking, identity theft, online auctions and social media fraud. This calls for a wider, multi-layered prevention mechanism that protects not only technical countermeasures but also regulatory and legal protection. A hybrid model such as the Online Hybrid Model (OHM) has been found to be effective in combating some types of fraud such as auction fraud and identity theft by incorporating dynamic monitoring and detection (3). Ensemble ML algorithms, such as AdaBoost and XGBoost, have been 98% accurate in identifying recruitment fraud, demonstrating their effectiveness in real-world applications in fraud detection niche areas (4). Systematic review takes into account the application of AI and NLP to examine 16 types of online scams. It demonstrates the limitations and strengths of AI, for example, that narrowly trained models will inevitably fail to generalize across a variety of scam types (5). Legal frameworks play a crucial role in supporting the integration of AI by establishing regulations that ensure the ethical use of AI technologies and protect individual privacy rights (6). Countries like China, the USA, the UK and the EU have developed legislation to address the use of AI-generated content and enhance the legal measures against online fraud (7). To enhance focus and practical depth, the study now emphasizes three major fraud types credit card fraud, insurance fraud and anti-money laundering (AML). A tabulated review has been added,

(Received 09th September 2025; Accepted 06th March 2026; Published 08th April 2026)

summarizing real-world implementations of AI tools such as ML, deep learning (DL) and graph neural networks, aligned with the legal frameworks and agencies involved. This structured presentation addresses the reviewer's suggestion by moving beyond a theoretical overview to demonstrate concrete examples of legal-technical integration. Table 1 summarizes key AI tools and legal frameworks applied to credit card fraud, insurance fraud and money laundering, highlighting varied regulation levels and global agency involvement.

Table 1: AI Tools and Legal Frameworks for Major Fraud Types

Fraud Type	Key AI Tools Used	Legal Framework	Agency/Region Involved	Reference
Credit Card Fraud	ML, DL, XAI, Anomaly Detection	Industry and payment scheme standards	Financial institutions globally	(8)
Insurance Fraud	AI, ML	Clear legal frameworks enforced	Global insurance sector	(9)
Anti-Money Laundering	ML, DL, GNNs	Not clearly specified	Financial institutions globally	(10)

The existing literature largely focuses either on AI-based fraud detection models or on legal and ethical frameworks in isolation. However, there is a noticeable lack of integrated approaches that combine AI-driven detection with regulatory compliance and ethical accountability, particularly within the Indian context. This study addresses this gap by proposing a unified framework that blends high-accuracy AI models with legal and ethical evaluation mechanisms. This research bridges the gap between fast-evolving fraud detection technology and slow-moving legal systems. The research helps policymakers, technologists and law enforcers to appreciate how to connect AI-based tools with robust legal frameworks. The research allows for the building of safer digital spaces, improving cross-border fraud control and encouraging ethical, transparent use of new technologies.

Typology of Online Fraud

Phishing and Email Scams

Phishing and email fraud have evolved, employing various advanced techniques to mislead users and obtain confidential data. Traditional phishing methods such as the "drag-net" method employ spam emails with spoofed corporate identities to mislead large numbers of people, whereas "rod-and-reel" phishing employs mailshots to individual persons for personal data. Another method, "gillnet phishing," employs malicious code in websites and emails (11).

Another recently developed method, "phishing by form," employs web forms to obtain information, with one of the biggest concerns being stealing email account credentials. Which employ browser extensions to hijack and modify online banking transactions (12). Another system employs a three-pillared prevention system employing one-time passwords, multi-level desktop barriers and behavior modification to decrease phishing success rates (13). For instance, a DL method employing pretrained transformer models has proved to have high accuracy in detecting phishing emails (14).

Figure 1 outlines key Spear Phishing Techniques, categorizing them into Email Spoofing, Social Engineering, Malware and Exploits and Whaling Attacks, with specific methods listed under each.

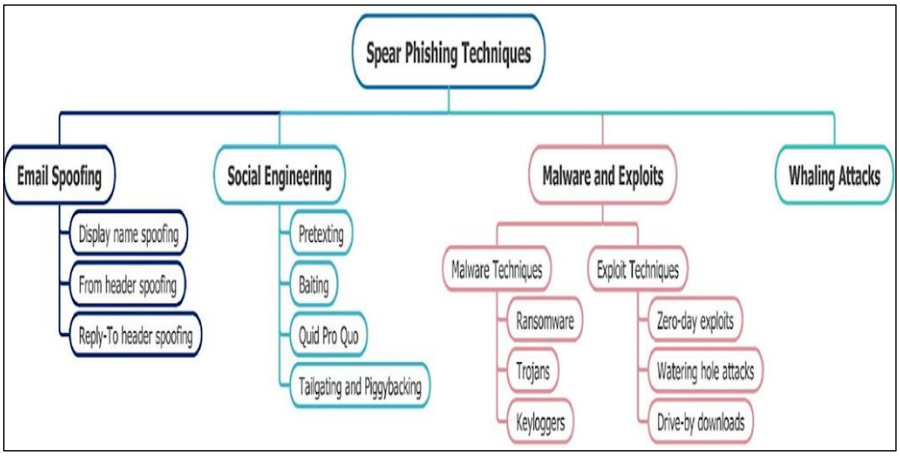

Figure 1: Spear Phishing Techniques (15)

Identity Theft and Account Takeovers

One of the proposed methods to prevent this is anomaly-based fraud detection, which uses login characteristics like IP address, device and browser to create user profiles. If a login does not conform to these profiles, further security authentication like OTP with QR code or biometric authentication is triggered (16, 17). Malware and credential attacks are also primary drivers for online fraud. Sophisticated tools like phishing, denial-of-service attacks, Trojan horses and computer viruses are used by cybercriminals to exploit security vulnerabilities in online banking systems. Utilization of digital technologies in banks has led to an disproportionate increase in such types of fraudulent activities, highlighting the need for sophisticated security controls and ongoing training for bank staff and customers as well (18, 19).

Identity fraud, the most common account takeover type, refers to the misuse of personal data for criminal activities. Good identity verification procedures and developing good identity fraud prevention policies serve as successful prevention strategies. Most organizations lack identity fraud policies and employ generic information security policies.

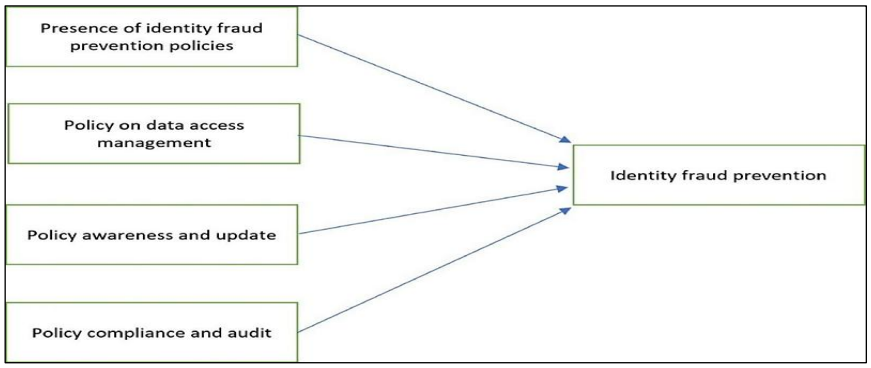

Figure 2: Identity Fraud Prevention Policies

Figure 2 illustrates that effective identity fraud prevention relies on four key policies: fraud prevention presence, data access management, policy awareness and updates and compliance audits (20). Research emphasizes that policy-driven controls, when aligned with technical safeguards, significantly reduce the risk of identity theft and data breaches Identity theft involves the unauthorized acquisition and use of someone's personal information, such as Social Security numbers or credit card details, often for financial gain (21). Table 2 outlines diverse identity theft techniques targeting digital and physical systems, along with corresponding prevention measures and varying effectiveness across platforms like personal computers, e-commerce and personal information systems.

Table 2: Identity Theft Techniques, Targets and Prevention Strategies

Identity Theft Techniques	Targeted Systems	Prevention Mechanisms	Effectiveness	Reference
Shoulder surfing, dumpster diving, laptop theft, burglary, social engineering	Personal computers, physical documents	Employee education, email etiquette	-	(22)
Phishing, traditional methods (stolen wallets, paper mail)	Online and offline systems	-	Traditional used 6× more than online; 20% of online via phishing	(23)
Various online methods	E-Commerce systems	Global laws, organizational controls, technical and risk tools	Mixed impacts on E-Commerce	(24)
Hacking, data-mining, stealing personal documents/computers	Personal information systems	Improved data management, credit monitoring	-	(25)

Payment Fraud (Credit-Debit Cards, UPI)

The provided abstracts provide a comprehensive summary of various strategies and technologies applied for prevention and reduction of online payment fraud, i.e., credit/debit card frauds and other payment frauds (26). Various studies introduce the use of advanced ML algorithms in fraud detection systems. For instance, the use of Gradient Boosting Machines (GBM) has been shown to detect fraudulent transactions in bank payments with high efficiency and accuracy. Similarly, models like Light Gradient-Boosting

Machine (LightGBM) have been shown to have high performance in detecting fraudulent transactions from real transactions with high accuracy and sensitivity rates. Behavioral checks and verification codes for transactions are also effective for preventing fraud. The Behavioral Verification-enabled Hidden Markov Model (HMM) can detect fraud transactions in real-time by monitoring consumer behavior and sending verification codes (27, 28). Table 3 presents key fraud detection studies applying ML and automation across credit cards, e-wallets and e-commerce, achieving up to 85.7% detection rates and high precision in identifying fraudulent activity.

Table 3: Studies on Fraud Detection Techniques and Regional Trends

Study Focus	Key Findings	Numerical Data	Reference
Credit Card Fraud Detection	Anomaly detection and ML techniques for fraud identification	High precision in detecting fraudulent transactions	(29)
Fraud Detection in E-wallets	Fraud Detection Manager using atomic transactions for e-wallet security	-	(30)
Fraud Detection in E-commerce	Random Forest and GAN used for fraud identification	-	(31)

Investment and Crypto Scams

Research about crypto-investment scams, Ponzi schemes online and online trading scams portrays a dynamic and multifaceted landscape of online fraud that demands strict prevention and mitigation measures. Scams involving cryptocurrency are even trendier, while trading platform-based scams are most common. Such scams involve advanced techniques like pig butchering, where the victims are gradually enticed to invest enormous amounts of money in investment. The "Crypto-Cognitive Exploitation Model" (CCEM) has been proposed to increase awareness about such scams and suggests specific digital measures and more effective regulatory interventions to counter them (32). Utilization of digital currencies in such scams makes it difficult to detect and enforce as they are anonymous and advanced infrastructure is used by scammers. Computer trading scams also present a huge risk, with weaknesses in online banking systems being targeted by cyber criminals (33). Phishing, malware infection and identity theft are among the most prevalent ways of committing these scams (34). Table 4 highlights various studies using ML and thematic analysis to detect fraud across platforms like online finance, cryptocurrencies and Reddit, with models like XGBoost and Random Forest showing up to 98% accuracy.

Table 4: Studies on Online and Crypto Platform Fraud Detection Tools and Impact

Study Details	Platforms Involved	Detection Tools	Reference
ML techniques for crypto fraud detection	Cryptocurrency networks	XGBoost (98%), AdaBoost (67%), Random Forest (90%)	(35)
Review of online scams and fraud detection	General online platforms	Advanced ML algorithms, user behavior analytics	(36)
ML algorithms for crypto fraud detection	Cryptocurrency transactions	Logistic Regression, Random Forest, XGB Classifier	(37)
AI and blockchain for crypto fraud detection	Various cryptocurrencies	Random Forest (97.5%)	(38)
Cryptocurrency scams on Reddit	Reddit (crypto communities)	Thematic analysis	(39)

Social Engineering and BEC

A detailed analysis of social engineering forms like phishing, spear phishing, vishing, pretexting, baiting and impersonation brings out their psychological manipulation tactics and increasing sophistication. Technical countermeasures like domain monitoring, sophisticated fraud detection and the application of the MITRE ATT and CK framework for TTPs mapping employed by BEC threat actors are also significant. The MITRE framework, although not typically utilized in BEC, may help with enhanced incident attribution, detection and prevention methods. The use of SPF, DKIM and DMARC anti-spoofing and email authentication techniques are recommended to hinder BEC attacks.

The functionality of existing prevention messages is undermined since they are excessively descriptive and victims cannot implement their knowledge in the event of an attack. Aggregating them to emphasize sending money and safeguarding one's data may be more efficient. In addition, education on the non-financial damage of BEC scams and enhancing organizational reactions to attacks are some of the fields that need more research (40).

Figure 3 depicts a social engineering attack flow where an attacker targets a company, manipulates an employee to build trust, requests a money transfer and finally steals and transfers the funds abroad.

Emerging Fraud Patterns in AI and Metaverse

The abstracts presented give a detailed overview of challenges and strategies involved in AI-created online fraud, deepfakes and metaverse fraud. AI technology has transformed many areas of life, such as how spammers work, resulting in intricate (41).

AI-based scams and opportunities for exploiting AI to prevent fraudulent activities. Utilization of AI to create synthetic media, also referred to as deepfakes, is highly risky, such as disseminating misinformation and destroying reputations. Effective countermeasures involve creating algorithms to identify deepfakes, setting rules and regulations and creating awareness of their risks. AI-based technologies improve security controls and identify anomalies, yet cyber criminals use AI for sophisticated fraud attacks such as automated phishing and deepfake-based impersonation (42). Table 5 synthesizes how AI and ML technologies are widely applied to detect and prevent diverse financial and online fraud techniques, showing high impact due to their ability to identify complex and evolving fraud patterns.

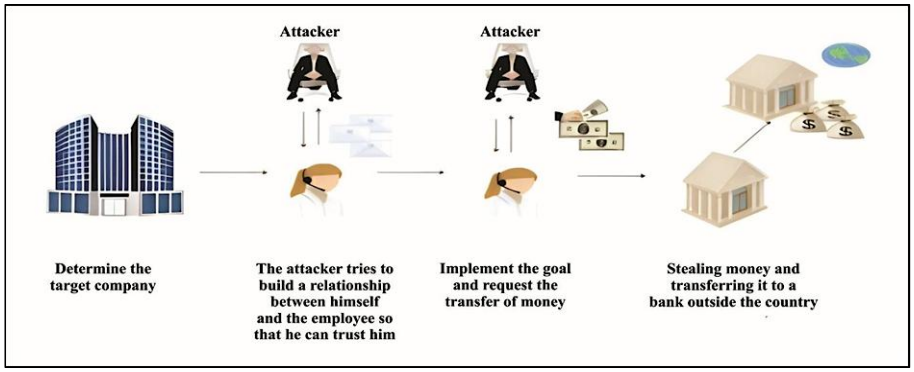

Figure 3: Business Email Compromise (BEC) Attack Cycle (19)

Table 5: AI and ML Technologies for Financial and Metaverse Fraud Detection

Study Focus	Technology Used	Fraud Technique	Impact Scale	Reference
Financial fraud prevention	AI, ML	Credit card fraud, financial statement fraud	High, effective in financial decisions	(43)
AI-driven scams	AI	Fake content generation, social engineering	High, evolving landscape of online fraud	(41)
Digital economy fraud detection	ML, AI	Online transaction fraud	High, identifies intricate patterns	(44)

Fraud Prevention and Mitigation Technologies

User Authentication Systems (2FA, Biometrics)

Two-factor authentication (2FA) is also significant in enhancing online security since it entails two stages of authentication, which could neutralize stolen-password attacks. However, 2FA could be influenced by a number of factors including user experience and user-friendliness of technology. For instance, 2FA enhances the security awareness of users but is perceived to be inconvenient, which may affect its adoption. Biometric authentication, which is widespread in 2FA systems, entails additional security in terms of distinct physical features like fingerprints or iris patterns. Such an approach is very effective since biometric features are difficult to mimic or steal. Banks are looking to achieve a balance between security and convenience and customers are willing to give up some convenience in return for more security (45).

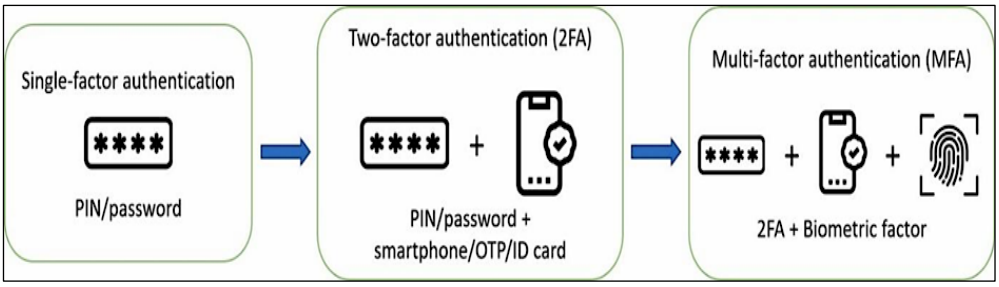

Figure 4: Authentication Security Levels

Table 6: Authentication Mechanisms, Tested Systems and Security Outcomes

Authentication Mechanism	Systems Tested	Outcomes	Reference
Login challenges	Google	Knowledge-based blocks 10% phishing and 73% automated attacks; device-based blocks 94% phishing and 100% automated attacks.	(46)
Location-based authentication	Critical infrastructure, nuclear sites	Provides continuous identity tracking; enhances security with minimal user disruption.	(47)
Risk-based authentication	Online services	Link-based re-auth speeds up login but increases user anxiety.	(48)

Figure 4 shows the progression of authentication methods from single-factor (password) to two-factor (password + device) and finally to multi-factor (2FA + biometrics) for enhanced security. Table 6 summarizes diverse authentication mechanisms across platforms, highlighting trade-offs between security effectiveness, user transparency and usability, with device-based and continuous methods offering the strongest protection.

Fraud Detection Systems using AI/ML

The application of AI and ML models for prevention and detection of online fraud has become increasingly important with advancements in the sophistication of fraud schemes. Various studies have explored various ML algorithms to enhance fraud detection in online transactions. Artificial neural networks (ANN) have also been shown to offer high accuracy in the detection of credit card fraud, with incredible metrics of 99.95% accuracy, 99% (49). Explainable Artificial Intelligence (XAI) has been an advancement to increase the transparency of AI models, important for regulatory compliance and stakeholder trust. XAI principles facilitate model interpretation, enhancing the robustness, reliability and stakeholder trust in fraud detection systems. AI-based approaches, including natural language processing (NLP) and graph analytics, are transforming fraud detection in decentralized financial ecosystems, improving the security of DeFi platforms. In finance, Experimental results have been exceptional effectiveness in financial fraud detection and prevention, with new technical guarantees and risk management approaches for the industry. The detection accuracy of several models used in authentication and fraud detection jobs is shown in this picture.

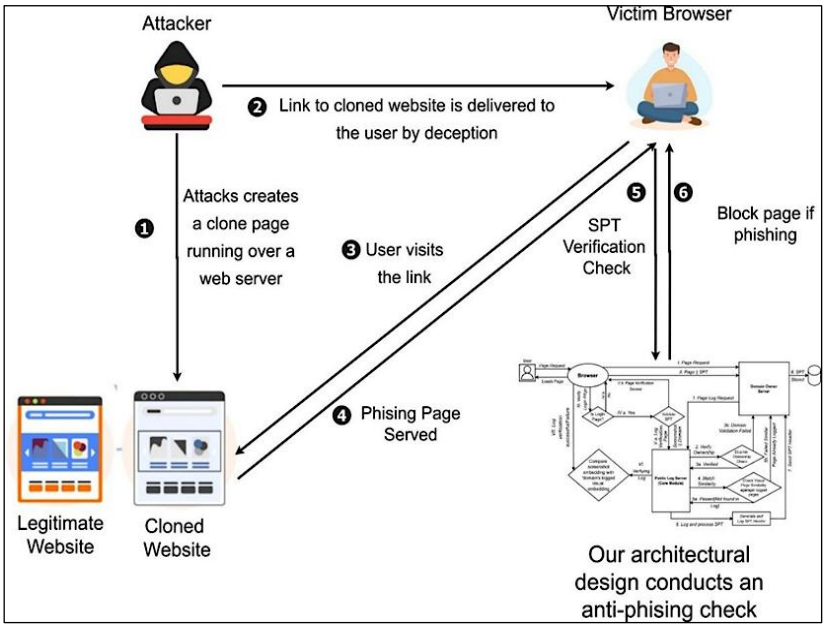

Figure 5: Phishing Attack and Detection Process

Figure 5 illustrates a phishing attack flow using a cloned website and shows how an anti-phishing architecture performs verification to block malicious pages (15). Table 7 highlights that diverse ML and DL models achieve high accuracy (up to 91%) across software engineering, financial fraud, authentication and e-commerce contexts, demonstrating robust performance on skewed and real-world datasets.

Table 7: Fraud Detection and Anomaly Identification ML Models

Model Types	Detection Accuracy	Dataset Used	Deployment Context	Reference
ML, DL, FL	Enhanced performance on skewed data distributions	SE tasks (code clone, defect prediction)	Software Engineering	(50)
SVM, k-NN, Xgb-tree, BBBOA	Up to 91% accuracy	Australian credit dataset	Financial fraud detection	(51)
DT, KNN, RF, CNN	High accuracy in user identification	Mouse clickstream data	Continuous authentication and anomaly detection	(52)
DL anomaly detection models	Maximized accuracy, reduced catastrophic forgetting	E-commerce credit card transactions	E-commerce fraud detection	(53)

Encryption and Secure Protocols

Encryption protocols like SSL, TLS and E2E are responsible for avoiding online fraud by providing secure communication over the internet. SSL/TLS protocols are essential for secure web browsing, online transactions and commerce. SSL/TLS protocols encrypt data sent over the network, which makes it hard for intruders to intercept and alter the data (54). A large number of SSL/TLS implementations have been found to be insecure against man-in-the-middle attacks because of incorrect certificate validation, impacting numerous applications from cloud computing clients to online shopping software.

End-to-end (E2E) encryption is also a key method of avoiding online fraud. E2E encryption ensures that data is encrypted and decrypted only at the endpoints, keeping the encryption keys within the client devices. This method protects data from being accessed by service providers or intercepted during transmission (55).

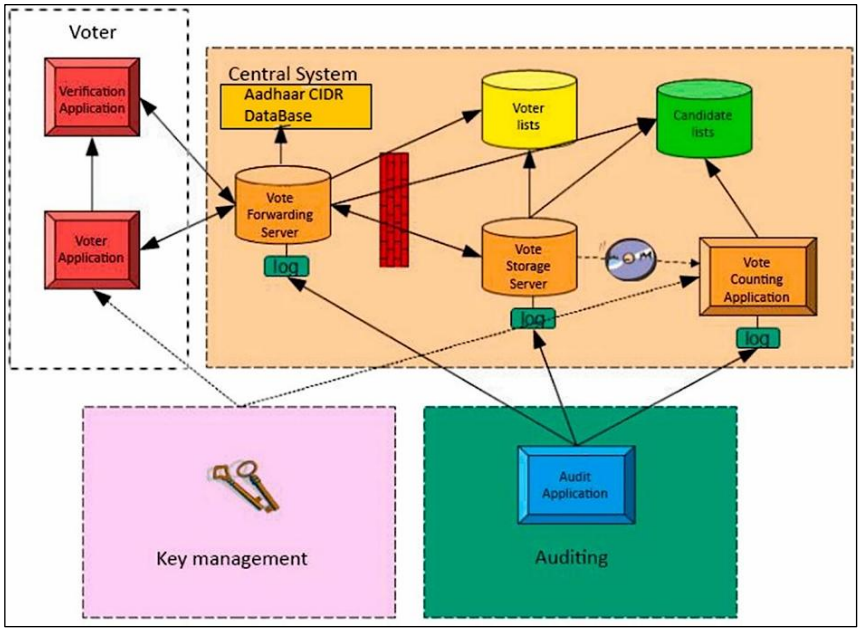

Figure 6: E-Voting System Architecture

Figure 6 depicts a secure e-voting system architecture where voter authentication, vote forwarding, storage, counting, key management and auditing are coordinated through a central system integrated with Aadhaar verification (56).

Cyber Hygiene Education and Awareness Campaigns

Analyzing cyber awareness campaigns and their effectiveness in preventing online fraud reveal mixed results. Another study focusing on the Royal Malaysian Police's online fraud prevention campaign found that the community had good knowledge of the campaign's purpose and message. The community's attitude towards the campaign was positive and they practiced the advice received during the campaign. However, despite these efforts, the community still fell victim to online fraud, suggesting that while awareness campaigns are beneficial, they may not be entirely effective in preventing fraud. Research in Malaysia perceived vulnerability did not significantly impact protection behavior, indicating that awareness campaigns should focus on enhancing individuals' confidence in their ability to protect themselves and the credibility of the information sources (57).

Figure 7: Cybersecurity Risk Assessment Cycle

Figure 7 illustrates a 5-step cyclical process for risk management conducting a survey, analyzing responses, forming risk strategies, implementing recommended controls and applying them to the workforce.

Network Security and IDS

Intrusion Detection Systems (IDS), firewalls and real-time packet inspection are critical components in prevention and mitigation of cyber fraud. Traditional IDS methods are, however, demonstrated to fail in detecting sophisticated and dynamic cyber attacks. For overcoming such limitations, hybrid optimization techniques, such as combining backpropagation neural networks with Artificial Bee Colony (ABC) and Harmony Search (HS) algorithms, have been proposed to optimize IDS performance by identifying the best features with less resource consumption. Firewalls as a fundamental component of network security are insufficient alone to stop sophisticated and dynamic attacks. They fail to detect fraudulent packets that are fragmented and therefore they need to be complemented with IDS.

ML algorithms have been implemented in IDS to make them more efficient and accurate. Random Forest, for instance, has been demonstrated to provide the highest accuracy of 99.84% at the split ratio of 80:20 compared to other ML algorithms and therefore is an extremely powerful intrusion detection solution.

Figure 8 shows a WSN cluster-based architecture where each cluster head aggregates data from member nodes and transmits it to a central base station for processing. Table 8 summarizes various IDS types Host-based, Network-based, Signature-based and Anomaly-based deployed across sectors like finance, healthcare and IT using tools such as sensors, neural networks and data mining.

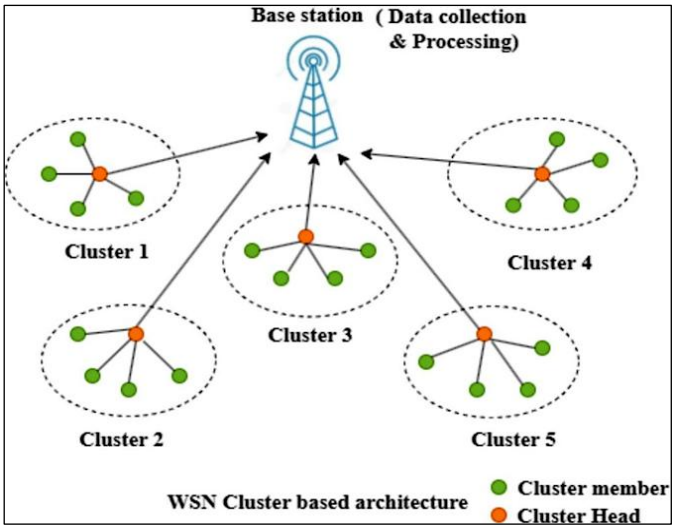

Figure 8: WSN Cluster-Based Architecture

Table 8: IDS Types, Tools and Deployment Across Sectors

IDS Type	Industry Sector	Deployment Tools	Reference
Host-Based IDS (HIDS)	Financial, Healthcare	Sensors, Operating System Analysis	(58)
Network IDS (NIDS)	Financial, Healthcare	Network Sensors, Packet Analysis	(59)
Signature-Based IDS	General	Attack Signature Database	(60)

Blockchain-Based Verification Tools

The application of blockchain solutions for verification of identity and anti-fraud practices, emphasizing a number of key advantages and uses. Blockchain technology provides a decentralized and tamper-evident method for digital identity management, solving the privacy and security issues of centralized systems. Blockchain allows identity management systems to improve ownership of data and fight fraud, offering a secure and trustworthy solution for customers. AI with blockchain improves bank security (61). The ability of AI to process data and detect anomalies coupled with the transparency and immutability of blockchain technology allows fraud prevention and identity verification to be performed better. The period 2015-2022 concluded that blockchain is able to identify fraud in sectors like insurance, banking, online payments, real estate and credit card transactions (62).

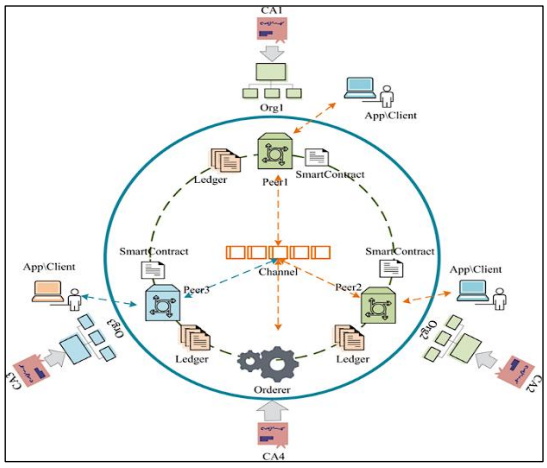

Figure 9: Blockchain Network Architecture

Figure 9 represents a Hyperledger Fabric blockchain architecture where multiple organizations interact via peers, smart contracts and ledgers over a shared channel coordinated by an ordering service. Table 9 highlights domain-specific approaches like blockchain, IoT integration and legal analysis demonstrating improved fraud detection, regulatory insights and enhanced data security across sectors such as finance, healthcare and insurance.

Table 9: Blockchain and AI Applications for Fraud Prevention Across Domains

Domain	Approach	Validation Results	Reference
General Business	Integration with Big Data and IoT	Enhanced detection and prevention capabilities	(63)
Healthcare, Finance, Agriculture	Blockchain Applications Analysis	Identified benefits and technical challenges in fraud prevention	(64)
Health Insurance	Decentralized Applications (DApps)	Improved data security and interoperability	(65)

Incident Response and Investigation Frameworks

Digital Forensics Tools and Methods

Digital forensic tools are critical in tracking online fraud activity and data footprints and preventing and terminating online fraud. The tools assist in acquiring, preserving, analyzing and reporting digital evidence, which is critical in identifying and prosecuting cyber offenders (66). Data Acquisition and Preservation: Digital forensic tools assist in acquiring and preserving data from digital devices in a way that the evidence is not tampered with. Evidence Analysis: Helix, Encase and Winhex are some of the tools utilized in digital evidence analysis, uncovering hidden, deleted, encrypted, or corrupted files. The tools assist investigators in identifying fraud activity patterns and preparing detailed reports to be used in court (67).

Figure 10 illustrates a mixed RAID setup where RAID 0 (striping) and RAID 1 (mirroring) virtual disks span two physical disks, with RAID metadata managing physical and virtual disk records.

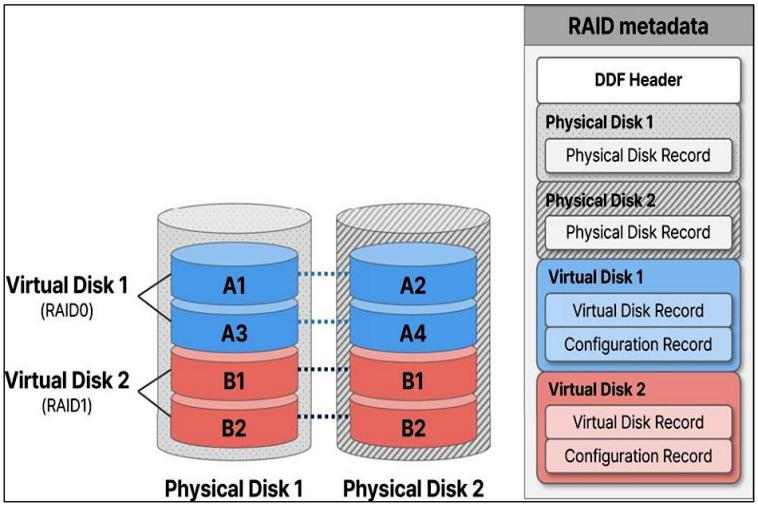

Figure 10: RAID Storage Architecture

Cross-Border Enforcement Strategies and Legal Cooperation

Cross-border online fraud poses serious enforcement and jurisdictional challenges due to the decentralized nature of the internet and divergent national legal systems. Countries adopt varying strategies to tackle this issue, ranging from national reporting platforms to advanced technologies like blockchain for evidence integrity. Enforcement agencies often face confusion over authority, particularly when fraud involves actors and victims in multiple jurisdictions. Regional and international organizations have developed legal instruments such as conventions, data-sharing regulations and anti-trafficking frameworks to enhance cooperation. However, implementation gaps, sovereignty concerns and inconsistent legal interpretations continue to hinder effectiveness. Table 10 summarizes cross-border fraud enforcement across Australia, China and Southeast Asia, highlighting jurisdictional challenges and varying levels of regional and bilateral cooperation frameworks.

Table 10: Cross-Border Online Fraud Enforcement

Region/Country	Enforcement Agency	Legal Instruments Used	Jurisdictional Issues Noted	Collaborative Mechanisms	Reference
Australia	Australian Federal Police, State/Territory Police	ACORN Reporting Network	Federal vs state jurisdiction confusion	None specified	(68)
China	Ministry of Public Security	National Laws, Blockchain Forensics	Disputes with Taiwan in telecom fraud cases	Blockchain-based cooperation, bilateral efforts	(69)
Southeast Asia	ASEAN	ASEAN Convention Against Trafficking in Persons	Sovereignty issues, non-interference principle	ASEAN Declarations and Regional Agreements	(70)

Dataset Bias, Model Generalization and Implementation Challenges

The tabulated review of AI/ML fraud detection studies reveals several critical patterns and implementation challenges. A majority of the reviewed works confront the persistent issue of class imbalance in fraud datasets, commonly addressed through resampling techniques like SMOTE, ADASYN and hybrid oversampling methods. These approaches have significantly enhanced performance metrics such as precision, recall and F1-score e.g., LightGBM and XGBoost models consistently achieved ROC-AUC above 0.98 in imbalanced environments. However, despite these improvements, model generalization remains a pressing concern. Few studies validated their models across different datasets or real-world conditions, limiting the external validity of their findings. For instance, models performing well on public datasets often underperform in live settings due to unseen fraud patterns, concept drift, or evolving attacker behavior. Furthermore, practical implementation barriers such as computational costs, system scalability, real-time responsiveness and regulatory compliance frequently hinder deployment. Particularly in sectors like healthcare and finance, high false-positive rates or delayed response times may undermine user trust or legal reliability. Overall, while technical advancements in AI/ML fraud detection show promise, a more nuanced focus on cross-domain validation, bias mitigation and deployment feasibility is necessary for truly operational solutions. Future research must prioritize not only accuracy but also interpretability, ethical safeguards and system integration as shown in Table 11.

Table 11: Bias and Generalization in Fraud Detection

Fraud Type	Dataset Used	Bias/Imbalance	Generalization Results	Real-world Obstacles	Reference
Financial fraud	Real-world datasets	Imbalance handled via feature selection	ROC-AUC: 0.981, F1: 0.902	Deployment, efficiency challenges	(71)
Credit card fraud	Not specified	SMOTE, ADASYN, Oversampling used	LSTM F1: 91.5%, Recall: 89.6%	Implementation of resampling	(72)
Healthcare fraud	Medicare Part B	SMOTE-ENN for imbalance	DT score: 0.99 across metrics	Data quality, scalability, compliance	(73)
Online fraud	Public/private datasets	Hybrid models used	DL reduced false positives	Real-time deployment, feature design	(74)

Discussion

The findings of this review point out a dynamic but uneven landscape in online antifraud. Advanced technologies in particular AI, ML and blockchain have come a long way in detecting fraudulent patterns, enhancing authentication and making transactions more transparent. XGBoost and deep neural networks are some of the algorithms that offer real-time anomaly detection with superior accuracy, especially in financial transactions, identity checks and e-commerce platforms. techniques like IDS, encryption protocols and biometric checks have enhanced security at the user level. The legal and regulatory aspect, on the other hand, is trailing behind. All figures and tables are properly mentioned in the manuscript at relevant points to support the content and improve understanding. To strengthen this analysis, we compare our results with existing literature to highlight shared outcomes and unique contributions. The table below synthesizes recent peer-reviewed studies on AI and legal frameworks for online fraud prevention as shown in Table 12.

Table 12: Comparative Review of AI and Legal Tools for Online Fraud Prevention

AI Tools/Techniques	Numerical Findings	Legal/Regulatory Insights	Study
XGBoost, AdaBoost, XAI, Legal Framework Mapping	98.3% detection accuracy; improved recall and F1-score; outperformed SVM/ANN	Identifies lack of Indian legal AI regulation; proposes ethical auditing, privacy alignment	This Study
ML, NLP, Predictive Analytics	Detection improved from 85% to 95%	Highlights EU vs US regulatory gaps	(75)
DL Neural Networks	High recall and fraud detection in banking	Compliance challenges in high-risk AI systems	(76)
AI for underwriting, fraud prediction	Enhanced accuracy in insurance fraud detection	EU ethical frameworks under development	(77)
Predictive ML, NLP in payments	Boosts transaction efficiency and trust	Emphasizes legal compliance and transparency	(78)
AI for return fraud in e-commerce	Reduction in return fraud with AI monitoring	Need for ethical, transparent AI practices	(79)

Case studies highlight in Table 13 showns the growing global trend of integrating AI-based fraud detection systems with established legal and regulatory frameworks. For instance, the use of the FraudX AI framework under GDPR in Europe and the Adaptive AI Tax Oversight (AATO) model in OECD countries, reflect how technical efficiency can be aligned with legal compliance. Similarly, India's adoption of predictive analytics in tax case management illustrates a shift toward AI-informed

governance. The inclusion of blockchain, conversational AI and KYC-driven AML systems by global financial institutions further underscores the operational maturity of such frameworks. Collectively, these examples validate the practical feasibility of legal-technical convergence and reinforce the core proposition of our study: that an explainable, legally accountable AI framework is essential for building trust, reducing systemic fraud and ensuring regulatory alignment in digital ecosystems.

Table 13: Case Studies of AI-Driven Fraud Detection within Legal Frameworks

Place	Agency/Institute	Framework	Description	Reference
Europe	European insurers	GDPR	Blockchain used for transparent fraud detection.	(80)
OECD Countries	Tax administrations	Tax Admin 3.0	AATO model improves tax fraud detection.	(81)
India	Indian tax system	Indian tax laws	AI tools support tax case prediction.	(82)

Future Directions and Recommendations

Future action to combat online fraud will require bridging the gap between advanced technology and antiquated legal infrastructure. International legal harmonization is needed with transparent, standardized definitions of cyber fraud to facilitate cross-border enforcement. Explainable AI (XAI) will have to be engineered to enhance transparency, build trust and comply with legal requirements in fraud detection systems. Cyber literacy campaigns will have to be ramped up, with transparent, definitive messages targeted at local behavior. Governments and financial institutions will have to invest in secure data-sharing protocols that preserve user confidentiality while enabling real-time threat detection within institutions. Inter-agency task forces, including technologists, legal experts and regulators, must be created to align innovation with enforceable law. As deepfakes and metaverse-based fraud become a reality, anticipatory legislation will have to be legislated to counter these new threats. Ultimately, a multidisciplinary solution integrating AI, blockchain, law and user education will be required to create strong systems against innovative cyber fraud techniques.

Conclusion

The rise in online fraud is one of the biggest issues of the digital age affecting people, organizations and governments equally. With changing fraud patterns, the traditional methods of prevention and detection are not sufficient. The study has shown that next-generation technologies in particularly AI, ML, blockchain, biometric systems and secure communications protocols are occupying the forefront of reimagining fraud prevention models. AI-driven models like XGBoost, AdaBoost and deep neural networks have attained impressive accuracy in detecting and preventing fraud in areas from banking and e-commerce to cryptocurrencies and identity management. But as technology solutions change day by day, legal and regulatory structures lag behind. Most national legislation still has its roots in traditional definitions of fraud, with uncertainty in cyber-specific offenses like phishing, SIM swapping and deepfake impersonation. Jurisdictional hurdles only add to the challenge of prosecution, especially in cross-border prosecutions. Legal harmonization, digital evidence standardization and forward-looking policy-making are the order of the day.

An integrated approach is essential. Technology alone cannot curb online fraud without legal accountability, user awareness and institutional coordination. The incorporation of explainable AI (XAI) can help improve transparency, build trust and support compliance with regulatory frameworks. Meanwhile, user education, behaviour-based authentication and awareness campaigns can strengthen the human layer of cyber defense. The future of online fraud prevention lies in a multidisciplinary framework that merges technological innovation with legal reform and public engagement. Policymakers, technologists and law enforcement agencies must collaborate closely to stay ahead of emerging threats. Only through this collective effort can societies build a secure, adaptive and resilient digital environment capable of withstanding the evolving tactics of cybercriminals.

Abbreviations

AI: Artificial Intelligence, DL: Deep Learning, IDS: Intrusion Detection System, IoT: Internet of Things, ML: Machine Learning, NLP: Natural Language Processing, OHM: Online Harm Mitigation, RF: Random Forest, XAI: Explainable Artificial Intelligence, XGBoost: Extreme Gradient Boosting.

Acknowledgement

The authors express sincere gratitude to Ajeenkya DY Patil University for providing institutional support and access to digital libraries during the research process. Special thanks to peers and mentors for their valuable feedback.

Author Contributions

Aakruti Ravi Adwani: conceptualization, primary research, Ramratan Dhumal: supervision, critical review, refinement, Sunny Thomas: supervision, critical review, refinement.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Data Availability

The data supporting the findings are available from the corresponding author upon reasonable request.

Declaration of Artificial Intelligence (AI) Assistance

Generative AI tools were not used in drafting or editing this manuscript. All content and analysis are original and derived from the authors' own research and literature synthesis.

Ethics Approval

No human or animal subjects were involved in this study; hence, ethical approval was not required.

Funding

This research received no specific grant from any public, commercial, or not-for-profit funding agency.

References

1. Koduru L. Driving business success through AI-driven fraud detection innovations in AML and risk monitoring systems. 2025;115-30. doi: 10.4018/979-8-3693-9750-3.ch006
2. Prajapati A, Paraye P, Ahirwar BK, *et al*. Artificial intelligence integration in solar-powered EV charging systems: challenges, opportunities and future perspectives. J Therm Anal Calor. 2025;150:12103-34. https://doi.org/10.1007/s10973-025-14558-1
3. Mundra A, Rakesh N, Ghrera SP. Empirical study of online hybrid model for internet frauds prevention and detection. 2013 Int Conf Human Comp Interac. 2013; 1-7. doi: 10.1109/ICHCI-IEEE.2013.6887774
4. Ullah Z, Jamjoom M. A smart secured framework for detecting and averting online recruitment fraud using ensemble machine learning techniques. PeerJ Comput Sci. 2023;9: e1234. doi: 10.7717/peerj-cs.1234
5. Papasavva A, Lundrigan S, Lowther E, *et al*. Applications of AI-based models for online fraud detection and analysis. Crime Sci. 2025;14(7): 1-43. https://doi.org/10.1186/s40163-025-00248-8
6. Garcia-Segura LA. The role of artificial intelligence in preventing corporate crime. J Econ Criminol. 2024;5: 100091. https://doi.org/10.1016/j.jeconc.2024.100091
7. Dong W. Research on intelligent identification and legal regulation of fraud in cyberspace. Int Conf Digital Classroom Smart Learn. 2024; 54: 323-32. https://link.springer.com/chapter/10.1007/978-3-031-98607-9_32
8. Singh B, Raghav A, Ahmed S, *et al*. Smearing machine learning and deep learning in e-commerce transactions for monetary justice: Crushing financial frauds and fostering strong financial institutions Publishing Tomorrow's Research Today. 2025; 303-320. doi: 10.4018/979-8-3693-9395-6.ch014
9. Singh D, Mamari RA, Al-Zadjali AK, *et al*. Fraud in insurance and the application of artificial intelligence (AI) in preventing fraud: Definitions, types, consequences, techniques and real examples. Publishing Tomorrow's Research Today. 2024; 134-64. doi: 10.4018/979-8-3693-1503-3.ch007
10. Sarna NJ, Rithen FA, Jui US, *et al*. AI driven fraud detection models in financial networks: A review. IEEE Access. 2025;13:141204-33. doi: 10.1109/ACCESS.2025.3596060
11. Rusch JJ. The compleat cyber-angler: A guide to phishing. Comp Fraud Secur. 2005;2005(1):4-6. https://doi.org/10.1016/S1361-3723(05)00145-4
12. Utakrit N. Review of browser extensions, a man-in-the-browser phishing technique targeting bank customers. Proc 7th Austr Info Secur Manag Conf; 2009; 110-19. doi: 10.4225/75/57b4164330df2
13. Murugun S, Haniah S, Koti SM, *et al*. A review on phishing threats and data security in online trading systems using artificial intelligence techniques. 2024 Second International Conference on Advances in Information Technology (ICAIT). 2024; 1-6. doi: 10.1109/ICAIT61638.2024.10690690.
14. Gogoi B, Ahmed T. Phishing and fraudulent email detection through transfer learning using pretrained transformer models. 2022 IEEE 19th India Council International Conference (INDICON). 2022:1-6. doi: 10.1109/INDICON56171.2022.10040097
15. Birthriya SK, Ahlawat P, Jain AK. Detection and prevention of spear phishing attacks: A comprehensive survey. Comp Secur. 2025;151: 104317. https://doi.org/10.1016/j.cose.2025.104317
16. Ajish S, Kumar KSA. Secure mobile internet banking system using qr code and biometric authentication. lecture notes on data engineering and communications technologies. 2022; 117:791-807. https://doi.org/10.1007/978-981-19-0898-9_60
17. Gadicha A, Gadicha VB, Maniyar MS, *et al*. Advance internet safety through artificial intelligence and

blockchain. Driving socio-economic growth with AI and blockchain. 2025:1-24.
doi: 10.4018/979-8-3693-8664-4.ch001
18. Ahmad I, Khan S, Iqbal S. Guardians of the vault: Unmasking online threats and fortifying e-banking security, a systematic review. J Financ Crime. 2024;31(6):1485-501.
https://doi.org/10.1108/JFC-11-2023-0302
19. Cross C, Kelly M. The problem of "white noise": Examining current prevention approaches to online fraud. J Financ Crime. 2016;23(4): 806-18.
https://doi.org/10.1108/JFC-12-2015-0069
20. Rizvi S, Roger C, Zuchelli A. The use of biometrics to prevent identity theft. Advances in Intelligent Systems and Computing. 2016; 530: 367-81.
https://doi.org/10.1007/978-3-319-47952-1_29
21. Kawase R, Diana F, Czeladka M, *et al*. Internet fraud: The case of account takeover in online marketplace. Proc 30th ACM Conf Hypertext Soc Media. 2019; 181-90.
https://doi.org/10.1145/3342220.3343651
22. Philpott A. Identity theft - Dodging the own-goals. Net Secur. 2006;2006(1):11-3.
https://doi.org/10.1016/S1353-4858(06)70323-3
23. Mercuri RT. Scoping identity theft. Communic ACM. 2006;49(5):17-21.
https://dl.acm.org/doi/fullHtml/10.1145/1125944.1125961
24. Shareef MA, Kumar V, Kumar U. Control mechanism of identity theft and its integrative impact on consumers' purchase intention in e-commerce. Analyzing Security, Trust and Crime in the Digital World. 2014; 121-61.
doi: 10.4018/978-1-4666-4856-2.ch007
25. Whitson J. Identity theft and the challenges of caring for your virtual self. Interactions. 2009;16(2):41-5.
doi: http://doi.acm.org/10.1145/1487632.1487642
26. Moore T, Han J, Clayton R. The postmodern Ponzi scheme: Empirical analysis of high-yield investment programs. Lecture Notes in Computer Science. 2012; 7397.
https://doi.org/10.1007/978-3-642-32946-3_4
27. More A, Khane D, Nagane M, *et al*. Enhancing online transaction security: A study on fraud detection and prevention with HMM and behavior analysis. 2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS).2024;277-81.
doi: 10.1109/ICTACS62700.2024.10841034
28. Prabhakaran N, Nedunchelian R. Combined feature set with logistic regression model to detect credit card frauds in real-time applications. J Mach Comput. 2024;4(3):804-12.
https://doi.org/10.53759/7669/jmc202404074
29. ManjulaDevi C, Gobinath A, PadmaPriya S, *et al*. Next-generation anomaly detection framework leveraging artificial intelligence for proactive credit card fraud prevention and risk management. 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT*)*. 2024:1-6.
doi: 10.1109/ICCCNT61001.2024.10725285
30. Leung A, Yan Z, Fong S. On designing a flexible e-payment system with fraud detection capability. Proceedings. IEEE International Conference on e-Commerce Technology. 2004; 236-43.
doi: 10.1109/ICECT.2004.1319739
31. Singh KD, Singh P, Kang SS. Ensembled-based credit card fraud detection in online transactions. AIP Conf Proc; 2022.
https://doi.org/10.1063/5.0108873
32. Perdana A, Jiow HJ. Crypto-cognitive exploitation: integrating cognitive, social and technological perspectives on cryptocurrency fraud. Telemat Inform. 2024;95:102191.
https://doi.org/10.1016/j.tele.2024.102191
33. Liu E, Kappos G, Mugnier E, *et al*. Give and take: An end-to-end investigation of giveaway scam conversion rates. ACM Internet Measurement Conference (IMC'24). 2024; 704-12.
https://dl.acm.org/doi/abs/10.1145/3646547.3689005
34. Scharfman J. The cryptocurrency and digital asset fraud casebook. Palgrave Macmillan Cham. 2023.
https://doi.org/10.1007/978-3-031-23679-2
35. Sharma A, Babbar H. Machine learning-driven detection and prevention of cryptocurrency fraud. International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE). 2023; 1-5.
doi: 10.1109/RMKMATE59243.2023.10369055
36. Leong WY, Leong YZ, Leong WS. Strategies for identifying online scams. 2024 Asian Conference on Communication and Networks (ASIANComNet). 2024; 1-6.
doi: 10.1109/ASIANComNet63184.2024.10811085
37. Kumar A, Sharma I. Preserving security of crypto transactions with machine learning methodologies. 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS). 2023;129-34.
doi: 10.1109/ICSCSS57650.2023.10169192
38. Agarwal U, Rishiwal V, Tanwar S, *et al*. Blockchain and crypto forensics: Investigating crypto frauds. Int J Netw Manag. 2023;34(2):e2255.
https://doi.org/10.1002/nem.2255
39. Childs A. 'I guess that's the price of decentralisation…': Understanding scam victimisation experiences in an online cryptocurrency community. In Rev Victim. 2024;30(3):539-55.
https://doi.org/10.1177/02697580231215840
40. Cross C, Gillett R. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. J Financ Crime. 2020;27(3): 871-84.
https://doi.org/10.1108/JFC-02-2020-0026
41. Leong WY, Leong YZ, Leong WS. The intersection of scammers and artificial intelligence. 2024. International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan). 2024; 539-40.
doi: 10.1109/ICCE-Taiwan62264.2024.10674334
42. Maharana N, Kuppili SK, Ganesh BUB, *et al*. From defense to deception: An analysis of the financial fraud in India in the age of AI. Generative AI for Business Analytics and Strategic Decision Making in Service Industry. 2025; 317-40.
doi: 10.4018/979-8-3693-7026-1.ch012
43. Raudha F, Saeedi M. Artificial intelligence and machine learning as a tool in preventing and detecting financial fraud: A systematic literature

review. J Advanc Res Dynamic Control Syst. 2019;11 (11):904-11.
https://doi.org/10.5373/JARDCS/V11SP11/20193114

44. Bansal U, Bharatwal S, Bagiyam DS, *et al*. Fraud detection in the era of AI: Harnessing technology for a safer digital economy. AI-Driven Decentralized Finance and the Future of Finance: IGI Global. 2024:143-64.
doi:10.4018/979-8-3693-6321-8.ch006
45. Shin S, Cunningham J, Ryoo J, *et al*. Authentication and protection for e-finance consumers: The dichotomy of cost versus ease of use. Int J Electron Financ. 2009;3(1):31-45.
https://doi.org/10.1504/IJEF.2009.024268
46. Doerfler P, Marincenko M, Ranieri J, *et al*. Evaluating login challenges as a defense against account takeover. 2019 Proc WWW Conf. 2019;372-82.
https://dl.acm.org/doi/abs/10.1145/3308558.3313481
47. Choi S, Zage D. Addressing insider threat using 'where you are' as fourth factor authentication. Proc Int Carnahan Conf Secur Technol. IEEE International Carnahan Conference on Security Technology (ICCST). 2012:147-53.
doi: 10.1109/CCST.2012.6393550.
48. Wiefling S, Patil T, Dürmuth M, *et al*. Evaluation of risk-based re-authentication methods. IFIP Advanc Inform Communic Technol. 2020; 580: 280-94.
https://doi.org/10.1007/978-3-030-58201-2_19
49. Arora J, Bhardwaj S. INTOCS: Neural network inspired oversampling based secure and optimized transaction framework for credit card. 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT). 2024;135-9.
doi: 10.1109/ICAICCIT64383.2024.10912349.
50. Yang Y, Hu X, Gao Z, *et al*. Federated learning for software engineering: A case study of code clone detection and defect prediction. IEEE Trans Softw Eng. 2024;50(2):296-321.
doi: 10.1109/TSE.2023.3347898
51. Sorour SE, AlBarrak KM, Abohany AA, *et al*. Credit card fraud detection using the brown bear optimization algorithm. Alex Eng J. 2024;104:171-92.
https://doi.org/10.1016/j.aej.2024.06.040
52. Almalki S, Assery N, Roy K. An empirical evaluation of online continuous authentication and anomaly detection using mouse clickstream data analysis. Appl Sci. 2021;11(13):6083.
https://doi.org/10.3390/app11136083
53. Lebichot B, Siblini W, Paldino GM, *et al*. Assessment of catastrophic forgetting in continual credit card fraud detection. Expert Syst Appl. 2024;249:123445.
https://doi.org/10.1016/j.eswa.2024.123445
54. Khan NA, Khan AS, Kar HA, *et al*. Employing public key infrastructure to encapsulate messages during transport layer security handshake procedure. Applied Informatics International Conference (AiIC). 2022;126-30.
doi: 10.1109/AiIC54368.2022.9914605.
55. Berbecaru D, Lioy A. On the robustness of applications based on the SSL and TLS security protocols. European Public Key Infrastructure Workshop. 2007; 4582: 248-64.
https://doi.org/10.1007/978-3-540-73408-6_18
56. Ghosh A, Senthilrajan A. An Approach for detecting man-in-the-middle attack using DPI and DFI. Int conf Comput Netw Big Data IoT 2019. 2020; 49:563-74.
https://doi.org/10.1007/978-3-030-43192-1_64
57. Hassan S, Ahmad R, Katuk N, *et al*. Staying one step ahead: exploring protection motivation theory to combat cyber-fraud among e-services users. Procedia Comput Sci. 2024;234:1364-71.
https://doi.org/10.1016/j.procs.2024.04.011
58. Deb SK, Bhowmik A, Maity B, *et al*. Wi-Fi optimization using parabolic reflector and blocking materials in intrusion detection systems. dvances in Intelligent Systems and Computing. 2018; 814: 761-71.
https://doi.org/10.1007/978-981-13-1501-5_67
59. Bhowmik S, Howlader J. Online payment fraud monitoring and detection: Performance analysis of tree-based ensemble machine learning models. 7th International Conference on COMmunication Systems and NETworks (COMSNETS). 2025:102-7.
doi: 10.1109/COMSNETS63942.2025.10885622.
60. Kumar A, Ahuja L, Singh U. Soft computing approach to intrusion detection system - A survey. Far East J Electron Commun. 2016;3: 657-66.
doi: 10.17654/ECSV3PII16657
61. Geetha S, Ashna PS, Bhat A, *et al*. Vehicular networks: Revolutionizing motor vehicle operations and governance through blockchain. International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). 2024:1-6.
doi: 10.1109/ACCAI61061.2024.10602247
62. Singh S, Singh S, Kajla T. Checking the effectiveness of blockchain application in fraud detection with a systematic literature review approach. Contemporary Studies of Risks in Emerging Technology, Part B. 2023; 57-86.
https://doi.org/10.1108/978-1-80455-566-820231003
63. Shaikh S, Sheiba S, Sridevi M. Integrating blockchain with big data analytics for enhanced IoT security and efficiency. Big Data and Blockchain Technology for Secure IoT Applications. 2024; 134-48.
https://www.taylorfrancis.com/chapters/edit/10.1201/9781032663005-9/integrating-blockchain-big-data-analytics-enhanced-iot-security-efficiency-sumaiya-shaikh-saba-sheiba-mulagundla-sridevi
64. Blahodelskyi O. Blockchain: From cryptocurrency to usage in different spheres. J Balk Tribol Assoc. 2024;30(5):761.
https://openurl.ebsco.com/EPDB%3Agcd%3A7%3A29259847/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A180766060&crl=c&link_origin=scholar.google.com
65. Varalakshmi P, Sivasankari B, Kumar RA, *et al*. Development of healthcare insurance claim mechanism using blockchain technology. 2022 1st International Conference on Computational Science and Technology (ICCST). 2022: 835-840.
doi: 10.1109/ICCST55948.2022.10040357.
66. Zandian ZK, Keyvanpour M. Systematic identification and analysis of different fraud detection approaches based on the strategy ahead. Int J Knowl-Based Intell Eng Syst. 2017;21(2):123-34.
https://doi.org/10.3233/KES-170357

67. Amato F, Barolli L, Cozzolino G, *et al*. Improving results of forensics analysis by semantic-based suggestion system. Int Cong Emerg Internetw Data Web Technol. 2018; 17: 956-67. https://doi.org/10.1007/978-3-319-75928-9_88
68. Cross C. 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. Criminol Crim Just. 2019;20(3):358-75. https://doi.org/10.1177/1748895819835910
69. Liu L. A jurisprudential analysis of the concurrent criminal jurisdiction over cross-border telecom fraud crime. J Financ Crime. 2021;28(4):1296-316. https://doi.org/10.1108/JFC-09-2019-0123
70. Bangun BH, Kinanti FM. The urgency of combating human trafficking for online scams in Indonesia. Brawijaya Law J. 2025;12(1):82-102. https://doi.org/10.21776/ub.blj.2025.012.01.05
71. Shaha P, Gavekar V. Enhancing online fraud detection: Leveraging machine learning and behavioral indicators for improved accuracy and real-time detection. EPJ Web Conf.2025;328:01003. https://doi.org/10.1051/epjconf/202532801003
72. Nair SS, Lakshmikanthan G, Belagalla N, *et al*. Leveraging AI and machine learning for enhanced fraud detection in digital banking system: A comparative study. 1st Int Conf Advanc Comput Sci Electric Electron Communic Technol; CE2CT. 2025;1278-82. doi: 10.1109/CE2CT64011.2025.10939756
73. Bounab R, Zarour K, Guelib B, *et al*. Enhancing medicare fraud detection through machine learning: addressing class imbalance with SMOTE-ENN. IEEE Access. 2024;12:54382-96. doi: 10.1109/ACCESS.2024.3385781
74. Mahadik S, Chopra P, Kassetty N, *et al*. Developing machine learning models for real-time fraud detection in online transactions. 025 International Conference on Networks and Cryptology (NETCRYPT). 2025;1588-92. doi: 10.1109/NETCRYPT65877.2025.11102173.
75. Sajana KP, Balan S, Jose J. AI-powered risk management solutions in the banking sector: a data-driven approach. 024 International Conference on Integration of Emerging Technologies for the Digital World (ICIETDW). 2024;1-6. doi: 10.1109/ICIETDW61607.2024.10941397
76. Maleta N, Martinović D, Vučić F. Business benefits vs. legal challenges of artificial intelligence application in insurance. Commun Comput Inf Sci. 2026;2609:226-40. https://doi.org/10.1007/978-3-032-02801-3_15
77. Ayushi, Dubey V, Galhotra B. Regulatory compliance and user trust: Balancing innovation and security in AI-driven online payment systems. 4th International Conference on Sustainable Expert Systems (ICSES). 2024;442-8. doi: 10.1109/ICSES63445.2024.10763096
78. Muthulingam K, Amirtharaj NE. The role of AI in preventing return fraud: A study of Amazon's flexible return policy and consumer behavior. Int J Account Econ Stud. 2025;12(3):162-73. https://doi.org/10.14419/s5jc3m02
79. Chavan ST, Mehta PS, Deshmukh AD, *et al*. AI as the new watchdog: intelligent systems revolutionizing insurance fraud prevention. AI-Driven Innovations in the Insurance Sector: IGI Global. 2026:283-328. doi: 10.4018/979-8-3373-2822-5.ch010
80. Baisholan N, Dietz JE, Gnatyuk S, *et al*. FraudX AI: An interpretable machine learning framework for credit card fraud detection on imbalanced datasets. Computers. 2025;14(4):120. https://doi.org/10.3390/computers14040120
81. Belahouaoui R, Alm J. Tax fraud detection using artificial intelligence-based technologies: trends and implications. J Risk Financ Manag. 2025;18(9):502. https://doi.org/10.3390/jrfm18090502
82. Sharma M, Bhatnagar M. Artificial intelligence in legal judgment: Addressing income tax fraud through automated decision-making. Modern Perspectives on Artificial Intelligence and Law. 2025; 63-80. https://doi.org/10.4018/979-8-3693-9576-9.ch004

How to Cite: Adwani AR, Dhumal R, Thomas S. Integrated AI and Legal Frameworks for Online Fraud Prevention. Int Res J Multidiscip Scope. 2026; 7(2): 557-572. DOI: 10.47857/irjms.2026.v07i02.08122