International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-13, Issue-6, November 2025
DOI: https://doi.org/10.55524/ijircst.2025.13.6.15
Article ID IJIR-1418, Pages 144-150
www.ijircst.org

A Multi-Layered Fraud Detection Framework Integrating Velocity, Identity, and Location Intelligence

Gnanesh Methari[1] and Dr Iqra Rasool[2]

[1]Department of Information Technology (Cybersecurity), Franklin University, Columbus, United States
[2]Department of Hematology, Chughtai Institute of Pathology, Lahore, Pakistan

Correspondence should be addressed to Gnanesh Methari; Metharignanesh770@gmail.com

Received: 1 November 2025 Revised: 15 November 2025 Accepted: 29 November 2025

ABSTRACT- The financial services sector has been largely computerized, as well as the introduction of real-time payment technology on an international scale, which has facilitated the expansion of the modern environment of fraud threats to an impressive degree. Despite the increase in speed and convenience these innovations have demonstrated the weakness of the old rule-based strategies of fraud detection. The contemporary financial fraud is becoming more and more a multi-vector attack, e.g. synthetic identity fraud, account takeovers and organized money mule networks, which take advantage of fragmented security controls and slow detection models.

The present paper proposes a complex, multi-level fraud detection model, where velocity analysis, digital identity intelligence, and location-based risk detection are used in the identical decisioning model, on a real-time basis. These are the device fingerprinting, behavioral analytics, transaction and action velocity monitoring, VIP and geolocation controls, email and phone intelligence to determine the dynamic and context-based risk fraud scores. The proposed solution enables the reduction of false positives and loss of customer experience by continuously with the use of machine learning and artificial intelligence to organize risks and avoid fraud before it strikes. The paper introduces the technical principles of each of the defensive layers, how each may be put together into a single risk engine and how explainable AI, adaptive learning, and regulatory compliance can be applied in a long-term deployment. The new development of federated learning and predictive analytics, Ethics and data privacy issues are also discussed. Overall, this structure demonstrates that the defense-in-depth strategy has the potential to greatly improve the resilience of the evolving fraud risk within the modern banking environment.

KEYWORDS- Real-Time Fraud Detection, Digital Identity Intelligence, Behavioral Analytics, Machine Learning-Based Risk Scoring, Financial Crime Prevention.

I. INTRODUCTION

The introduction of digital transformation of the financial services arena has brought with it a kind of convenience, scalability, and connectivity more than ever. Meanwhile, this transformation has been coupled by a high rate of growing advanced fraud attacks. Outdated, rule-based systems of detection are not working against the adaptive threats: synthetic identity fraud, account takeovers, and organizing money mule activities.

This whitepaper presents a strong and multi-layered fraud detection system that is based on the use of advanced technologies such as; device fingerprinting, behavioral analytics, velocity check, VIP and location monitoring, email and phone intelligence into a single and smart defense architecture [1]. Leveraging machine learning and artificial intelligence in real-time risk orchestration, the framework will give financial institutions the opportunity to preemptively detect and stop fraudulent activity without disrupting the customer experience or violating regulatory standards. The paper explores the technical processes of either side of the layers, how these layers will combine in a centralized decision-making platform, and what ethical and future facing policies will be necessary to implement sustainable security.

The Developing and More Complex Threat Environment.

Financial fraud has taken a new face, as it is no longer a matter of individual identity theft, but an extremely advanced technological, highly organized cybercrime attacks [2]. In 2024 nearly all reported cases were in digital channels with the estimated financial fraud losses worldwide amounting to over 400 billion. This has been escalated through several important factors.

A. Digital Proliferation:

The current popularity of online and mobile banking has greatly increased the area of attack that gives trial to fraudsters more entry points than in the past. The fintech platform development plus open banking APIs have further erased the traditional security boundary and complicated systems.

B. Advanced Attack Tools:

The use of modern frauds is based on more advanced means. Credential stuffing attacks are typically done with automated botnets and advanced phishing kits are designed to appear like legitimate financial institutions. There has been an increase in mobile malware such as Trojan banking applications that have the ability to superimpose fraudulent interfaces on legitimate apps. Moreover, voice and facial biometric verifications are being hacked by using deep-fake technologies.

C. The Metamorphosis of false selves:

Synthetic identity fraud is one of the most harmful and rapidly increasing types of financial crimes. Through such schemes, criminals would join legitimate details like stolen social security's numbers with fake personal data, including names and addresses, to form new identities. These artificial profiles are commonly nurtured for long durations to build good credit records and are then used in massive bunk out operations that end up in big and in most cases irreparable losses [3].

D. Real-Time Payment Systems:

The worldwide trend towards instant payment systems, including the FedNow system in the United States and SEPA Instant in Europe, has made the timeframe during which a person can interfere with a transaction and review it significantly shorter. The non-retractionable character of real-time payment enables fraudulent deals to be accomplished and funds to be dispersed in a few seconds, often before customary detection strategies can even react.

II. THE MORTAL FLAWS OF TRADITIONAL DETECTION MODELS

The conventional fraud detection models that contain mostly of static and pre-programmed criteria and chargeback history are essentially unprepared to face the current dynamic threat landscape. Their constraints are structural and most of the time result in operational inefficiency as well as reputational damage [4].

A. High False-Positive Rates:

Fixed sets of rules are contextually unaware and often consider legitimate customer behavior to be suspicious. Unusual transactions like buying a lot of goods when travelling are usually reduced which causes customer dissatisfaction and loss of profit. Javelin Strategy and Research conducted a study where it was reported that false declines cost an estimated 443 billion in missed merchant sales in 2022 hence the high effect on customer trust and loyalty.

B. Failure to Identify Categories of Novel Attacks:

Rule based systems are reactive and limited to identified patterns of fraud. Consequently, they cannot easily identify new threat, zero-day attack plan, or slow-paced fraud attempt where attackers intentionally replicate the behavior of legitimate users so that they do not kick off a static threshold-based detection mechanism.

C. Deficit of Contextual Awareness:

Such systems are usually functional silos. The signals that occur during the process of logging in or maintaining an account and processing the transactions are not always correlated, and it is impossible to create a complex risk narrative. This fragmentation enables the multi-stage fraud attacks to move on without being detected.

D. Operational Inefficiency:

False alerts are very high, and they clog investigation teams, and this compels analysts to have to waste time on seeing legitimate transactions instead of working on complex and high-risk transactions. This is unproductivity that escalates operational expenses and delay's reaction to real cases of fraud [5].

Multi-Layered Fraud Detection Framework: Paradigm Shift.

The Layered Defense Strategic Imperative.

A multi-layered fraud detection methodology is reflective of the concepts behind physical security, whereby more than one control intersects over important assets. This in a digital context would mean the matching of various streams of data, including device properties, behavior, network, and geographic data, in a unified, real-time risk evaluation engine.

The main element of the suggested structure is a three-fold of velocity, identity and location intelligence that constantly authenticates user identity across the customer lifecycle. Instead of an allow-or-deny decision on the basis of a binary decision, the system builds adaptive risk scores which change with each interaction. The nonlinear pattern is subtle and cannot be depicted as rule-based, but machine learning and artificial intelligence help identify them. Fraud today is not a one-off act of anomaly; it is a sequence with each event that only raises the alarm once the events are put into consideration [6]. The layered defense allows such events to be correlated at various dimensions resulting in a more effective and resilient fraud detection approach [5].

III. BASIC SYNERGISTIC ELEMENTS OF THE FRAMEWORK

The suggested structure has five interdependent elements that feed a centralized decisioning engine, which, as a whole, gives a holistic picture of user risk.

A. Device Fingerprinting:

The layer provides a base digital identity through the analysis of broad coverage of hardware, software and network attributes. The system can confidently detect returning devices, even when cookies are deleted or privacy settings are enabled, and identify a setting that is likely to be fraudulent, like an emulator or virtual machine [7] by analyzing the configuration of the devices, the features of the operating system and browsers, and network activity.

B. Behavioral Analytics:

Behavioral analytics records user-interaction with digital interfaces, constructing distinct behavioral patterns by the dynamic of typing, mouse or touchscreen movement, navigation history and session behavior. Such behavioral biometrics cannot be duplicated in a regular manner and they are especially useful in detecting account steal and session injection attempts [6].

C. Velocity Checks:

Velocity analysis is a means that tracks the rate and timing of the user action such as transactions, attempts to log in as well as sensitive account modifications. Through a set of personalized baselines, the system will be capable of separating bona fide high-activity users and malformed behavioral evidence of credential stuffing, bust-out fraud, or money mule behavior [8].

D. VIP and Location Monitoring:

This layer provides geographical and privilege context by comparing the access points with the past trends, identifying impossible travel routes and identifying links

with high-risk networks like VPNs and anonymizing services. Tight controls and reduced thresholds of anomalies are placed on high-value or privileged accounts.

E. E-mail and Telephone Intelligence:

Digital identity credentials are legitimized via email and phone intelligence which measures the aspects of domain age, breach exposure, syntactic, line type, number longevity, and SIM swap indicators. These indicators can be used especially to detect synthetic identities during onboarding and account takeover attempts during the customer lifecycle [9].

The power of the framework is attributed to the correlation of such components. A composite risk score offers some sense of confidence that would be far beyond that offered by individual indicators.

IV. THE BASICS OF DIGITAL IDENTITY: DEVICE FINGERPRINTING

Idea and Mechanical Process-

The device fingerprinting process involved the use of systematic gathering of a wide range of configurational and environmental properties of a device owned by a user a desktop computer, smartphone, or tablet to produce a unique and durable identifier. It is an identifier that is usually called a device fingerprint and is based on hundreds of stable and variable data points, which include:

A. Hardware Attributes:

These are: CPU type, architecture, graphics card vendor and graphics card capability, screen resolution, color depth, fonts available and media devices [10] that these devices are connected to.

B. Software Attributes:

Some of the information that will help distinguish one device environment to another will include the operating system and exact version, the type and version of the browser used, installed extensions and plugins and the language settings.

C. Network Attributes:

Network level indicators involve IP address, TCP sequence anomaly, accepted types of the HTTP header and network latency peculiarities.

D. Configuration Attributes:

Other identifiers are time zone, keyboard layout, and HTML5 canvas fingerprinting, which render the hidden graphics to identify the slightest variations in rendering engine and anti-aliasing behavior.

More sophisticated tricks like audio context analysis searching the audio processing stack to find small differences in hardware, and WebGL fingerprinting - even subtractively enhance the finger print. Collectively, these signals are a composite identifier which is highly hard to spoof on a session-by-session, or environment-by-environment basis by fraudsters.

V. FRAUD DETECTION ADVANCED APPLICATIONS

In addition to mere device identification, device intelligence is vital in the process of unifying intricate and coherent fraud activities.

The second type of synthetic identity detection is known as Synthetic Identity Detection.

Using patterns of device fingerprints, financial institutions are able to associate big groups of newly opened synthetic accounts with either a single physical device or a small set of devices. This association tends to expose the factory of frauds of artificial identity movements.

A. Botnet Identification:

There is the possibility of device fingerprinting to detect a slight similarity between thousands of affected devices (zombies) which are managed by central command and control facilities when they are geographically spread.

B. The prevention of Account Takeover (ATO):

The logins by new devices and those by already suspicious devices can be flagged instantly, giving a consistent indicative alarm on attempting to take up an account [11].

C. Trusted Device Profiling:

Defining a policy of trusted devices is one way in which institutions can create friction against legitimate users by allowing lower-friction authentication of known-endpoints, and a higher-level of scrutiny to unknown devices.

The intelligence platform of modern devices is based on probabilistic matching algorithms, machine learning models that can tolerate minor variations e.g. software updates or new plugins installed but at the same time be able to detect the underlying device, reliably over time. Such a trade-off between perseverance and flexibility is crucial towards being accurate in a dynamic environment.

D. QI Case Study and Measurable Impact.

In response to a significant accounting takeover movement, a large multinational bank implemented a device intelligence system of ThreatMetrix (since acquired by LexisNexis Risk Solutions) to counter the threat. The solution was incorporated into both log-in and transaction workflows and each access request would be compared against a global consortium database that contained over five billion devices.

The system disclosed that, about 15 percent of the credential-stuffing attacks were initiated by the devices that are already in the high-risk category on the global network. With this intelligence coupled with other layers like behavioral analytics, the bank realized a 40 percent decrease in successful ATO incidents and 60 percent decline in false positives in the first year of operation. The gains achieved out of these improved millions of dollars of lost fraud and a quantifiable rise in customer satisfaction because of less authentication friction among legitimate users [12].

VI. BEHAVIORAL ANALYTICS: THE UNSEEN BIOMETRIC SHIELD

Cognitive Profiling and Behavioral Biometrics-

Whereas device fingerprinting ensures the establishment of the what, behavioral analytics aims at ensuring the identification by analyzing the subconscious manner in which users engage with digital systems. This type of biometric authentication is a continuous, passive authentication that works transparently in the background, without the explicit input of the user.

Major behavioral indicators help make up an individualized and rich portrait:

A. Keystroke Dynamics

Special motor patterns are recorded as metrics like typing rhythm, flight time of the keys, and dwell time in the keys and are extremely hard to imitate.
Mouse and Touchscreen: The ability to use a mouse or touchscreen is also available.<|human|>Mouse and

B. Touchscreen Gestures

The study of the movement speed, acceleration, path curvature and touchscreen pressure points out the inherent difference between human behavior and an automated script.

C. Navigation Patterns

Scroll behavior, number of clicks, sequences on page traversal and time on page in the review of transaction confirmations give evidence of user intent and interface familiarity [13].

D. Interaction Characteristics of devices

The behavioral signature is further narrowed by factors like preferred orientation of devices, angle of handling and common period of session that the user goes through.
A combination of these cognitive and motor-skill characteristics forms the biometric profile that is more resistant to imitation than commonly used and is highly effective against session hijacking and man-in-the-browser attacks behavioral analytics is also effective against [6].

VII. ARTIFICIAL INTELLIGENCE AND PATTERN RECOGNITION

The behavioral analytics systems are based on unsupervised machine learning model mostly to create individualized norms of normal behavior. All these models keep on changing with the change in habits of the users like due to an injury or a change in device. Hundreds of behavioral signals are recorded in real time during every session and compared to the predetermined baseline used by the user.
Significant deviations are detected using anomaly detection techniques [6], such as isolation forests, one-class support vectors machines (SVMs) including:

- A user who usually moves at a slow pace suddenly involved himself in a complicated funds transfer procedure.
- Artificially linear and repetitive mouse movements, which are not typical of the human interface but of automation.
- Registering sessions that take place at the time that is well out of the historical proceeding of the user.
- The behavioral risk score that results give a potent continuous indicator, which puts significant context to other authentication and risk indicators.

Integration to improve Precision
Behavioral analytics has a complete value when correlated with other layers of defense. As an example, a user can log-in on an identified home device with valid credentials-positive device fingerprint signal. But when behavioral analysis shows erratic mouse behavior and extremely fast navigation to a high value wire transfer page, then this discrepancy between trusted hardware and unexpected deviant behavior is very suggestive of compromise [7].
In this scenario, the system will have the ability to initiate step-up authentication, including mobile push notification or a biometric challenge. This stratified corroboration is especially useful in thwarting those fraudsters who have installed malware or keyloggers on legitimate computing devices, and at the core of minimizing false positives and ensuring high-security levels.
Velocity Checks Velocity Checks: The Temporal Firewall.
Velocity analysis is used to determine the frequency, speed, and sequence of user activity to determine patterns that portray automation, panic, or organized fraud. This temporal aspect is a very important last line of defense in the real time payment system. It will respond to one of the basic questions: Is this action carried out on a speed and volume that is feasible by this user? The speed is essential to the fraudsters, as they take advantage of the short execution windows and that is why velocity analysis is one of the main countermeasures [14].

VIII. VIP AND LOCATION MONITORING: LOCATING ACCESS AND PRIVILEGE

State of the art Geo-Behavioral Intelligence
Location intelligence goes far beyond fundamental IP-to-country mapping. Contemporary systems construct a behavioral knowledge of how, where, and what environments are usually used by the users in seeking financial services. Such more geographically diverse environment is the key to differentiating legitimate travel and malicious access attempts.

A. IP Geolocation: IP Geolocation is detected as false.<|human|>Proxy/VPN Detection:

Connections are assessed to establish their actual source, traffic routing via data centers, anonymizing proxy services, tor exit nodes or commercial VPNs. Fraudsters often use these infrastructures to hide location and evade detection [16].

B. GPS and Wi-Fi Triangulation (Mobile Environments):

In the case of mobile applications, GPS signals and Wi-Fi triangulation may offer the location signal that is far more accurate than the use of the IP address. Due to the sensitivity of these signals, strict privacy regulations and direct user consent should be used to at least control their usage.

C. Travel Velocity Analysis:

Systems may determine the existence of an impossible travel scenario by computing the physical impracticability of successive events in a sequence of login events. Suppose that a user is authenticated by New York, and then logs in by London, minutes later, it is a good indication that they have compromised their credentials or are sharing the account.

D. Profiling of the Historical Place:

Eventually, the system gets to know the common geographical ranges of a user like his or her home or workplace or his or her regular travel points and sets a groundwork of what is considered usual site of access.

Evaluation against this history is then done on new locations to identify the level of risk [17].

IX. ACTIVE SURVEILLANCE OF RISKY AND PRIVILEGED ACCOUNTS

Account compromise can have much more far-reaching repercussions than just immediate financial loss to high-net-worth people (HNWIs), corporate executives, and users at the top of the system privilege hierarchy. These patients thus need sensitive monitoring plans.

A. Stricter Geo-Fencing:

The attempts of access by the country that is not included in a predefined list of the safe countries are immediately followed by a high-priority alarm and required step-up authentication, e.g. biometric authentication or out-of-band authentication.

B. Device Whitelisting:

Transactions that use high values can be limited to a list of trusted devices. Any efforts to activate an activity of a device unknown or unmanaged are automatically blocked and escalated to investigate it [18].

C. Reduced Behavioral Thresholds:

In case of VIP accounts, any slight deviation including but not limited to the changes in time of transaction, destination and amount of money ought to be related by two authorization or even by a special security team.
Internationalization with Global Threat Intelligence.
Monitoring of locations and VIPs is made significantly more efficient with the supplement of external threat intelligence feeds. This integration enables systems to be shifted out of reactive detection to proactive defense by:

- Blocking or disallowing attempts of access done by IP ranges that are identified with known botnets, cybercrime organisations or command-and-control infrastructure.
- The flagging of access originating in areas or provider of services to which a financial institution is now or currently targeted by phishing or malware attacks.
- A comparison between internal anomalies and external intelligence which might point to insider collusion or external multilateral attacks [8].

X. EMAIL AND PHONE INTELLIGENCE: AUTHENTICATION OF THE DIGITAL PERSONA

Data Enrichment and Deep Identity Correlation
Primary identity anchors used in the process of onboarding, authentication, and recovering accounts include email addresses and phone numbers. The intelligence gained out of these features is thus essential throughout the customer lifecycle [9]. The analysis goes far beyond the syntactic validation to behavioral and historical risk pointers.

A. Email Intelligence:

Domain Age and Reputation: Fraudsters often use new email accounts that have been created freely at the time when legitimate users normally have old addresses. Risk is also improved with domain-level reputation scores.

B. Breach Exposure:

When the Emails are found in more than one public or private breach repository, it is a sign of high risk because of using the same credential.
Auto-generated usernames or too much aliasing: Feature Custom started by this type of auto-generated usernames or excessive aliasing can be an indicator of mass testing out of the system or identity fabrication.

C. Phone Intelligence:

Type of Line: It is important to distinguish between the mobile numbers on contract basis and high-risk prepaid, VoIP, or virtual numbers because in fraud schemes, disposable numbers are overrepresented.
Number Longevity and History of Activity Recent activated numbers or numbers related to familiar fraudulent accounts make instant alarm bells across the consortium networks [22].

D. SIM Swap Detection:

Keeping an eye on last SIM swaps will allow spotting number-porting attacks to use it and intercept SMS-based authentication codes.

E. Risk Scoring Engines integration.

Instead of being used as hard blocklists, email and phone intelligence signals are applied as weighted inputs to the centralized risk score. For example:

F. Low-Risk Profile:

An old organization email and a fixed mobile phone number and active history of the device.

G. High-Risk Profile:

The new free email account and VoIP number, device fingerprint of high-risk and deviated velocity profiles.
Such a layered identity validation goes a long way in enhancing the Know Your Customer (KYC) and Anti-Money Laundering (AML) alike controls by thwarting fraudulent applications at their inception area, lowering downstream investigation and remediation expenses.

XI. INDUSTRY IMPLEMENTATION AND EFFECTIVENESS

The industry leaders, e.g., Emailage (LexisNexis) and Ekata (a Mastercard company), use consortium-based identity networks over the whole world, which pool anonymized risk indicators of thousands of organisations. One of the European digital banks incorporated Ekata Identity Graph API into its onboarding process and within 28% of application fraud was decreased through detecting and challenging high-risk digital identities before accounts were funded and abused [10].
Synthesis: Designing Unified Intelligence and Decisioning Platform.
The Real-Time Risk Orchestration Engine.
Risk signals cannot be effectively detected in real time without a central system that could correlate, interpret and take action on risk signals. Modern fraud architecture thus orbit around a decisioning engine based on the cloud which is multi-purpose and carries out a number of functions at the same time:

A. API-Driven Data Ingestion:

Gathers systematically and informally organized signals, on all levels: device, behavior, velocity, location, and email/phone on each customer interaction.

B. Correlation and Scoring:

Normalization and weighting of disparate inputs of ensemble machine learning models to produce a single fraud risk score as the likelihood of malicious activity is done.

C. Response Implementation: Policy-based:

The engine responds to risks within milliseconds based on business policies and risk limits. These can consist of smooth approval, step-up authentication, analyst check or automatic rejection of obviously fraudulent activity [19].

D. Overall Data Lake Integration:

Any interaction data is stored to be analyzed in the forensic manner, reported to the regulators, and constantly enhanced.

E. Adapting Learning, Explaining and Compliance:

Fraud detection systems should constantly be improved to be effective. Meanwhile, regulatory supervision requires the accountability and transparency.

F. Adaptive Learning:

Results of manual reviews (False positives and confirmed fraud) are recapitulated back to models as labelled data. With this feedback loop, systems can optimize the accuracy and respond to new trajectories of fraud by undergoing sub-training processes rather than complete retraining.

G. Explainable AI (XAI):

Laws like the EU AI Act (2024) no longer allow automated decisions to be uninterpretable. Auditable accounts of risk scores (e.g., device novelty, abnormal velocity, high-risk geolocation) are available through techniques like LIME and SHAP, which makes them efficient with respect to investigator efficiency, and regulatory compliance [11][10].

XII. THE DIFFICULTIES, ETHICS, AND GOOD IMPLEMENTATION

A. Finding the Way through Data Privacy and Global Compliance.

Vast amounts of data needed to conduct sophisticated fraud prevention procedures create concerns of privacy and governance. The institutions have to make sure that they comply with international regulations, including GDPR, CCPA/CPRA, PSD2, and GLBA and stay efficient in their systems [12].

The mitigation measures consist of data minimization, anonymization and pseudonymization, sensitive behavioral signals processing on-device, and regular Privacy Impact Assessment before deployment.

B. Reducing Algorithmic Bias and Model Drift.

The AI systems mirror the information that they are being trained on and hence, they are susceptible to biases and decreased performance with time [20].

The institutions should address these risks by:

- Carry out frequent fairness audit at both demographic and geographical levels.
- Training datasets Curate diverse, representative training datasets.
- Have a human-in-the-loop (HITL) model to maneuver automated decisions to rectify errors [21].
- The model drift should be mitigated by constant monitoring of the performance and retraining after a certain time with the recent and high-quality data.

C. Fraud Defense in the Next Generation.

Even more detailed data fusion and sophisticated computational methods will characterize future fraud defense.

- Fusion Intelligence:

By incorporating the banking telemetry with IoT data, open-banking indicators, and blockchain analytics, cross-institution anomaly-detection will be possible and enhanced fund-flow monitoring will be improved [4].

- The following features are from Predictive and Prescriptive Analytics:

Fraud will be detected prior to its realization because systems will identify reconnaissance patterns and take proactive steps to counter those [8].

- Federated Learning:

Sharing raw data will not keep privacy or environmental regulations intact and institutions sharing models will reinforce collective defense and provide a stronger defense [5].

- Quantum-Resistant Cryptography:

With the development of quantum computing, financial institutions need to start switching to quantum-safe encryption standards to future-proof security infrastructure [13].

XIII. CONCLUSION

The situation of a meeting of velocity, identity and location intelligence is the foundation of the contemporary fraud defense. This approach to financial ecosystem protection in combination with explainable AI, adaptive learning, and ethical governance creates a multi-layered design, which helps to maintain the integrity of the financial system ready to serve the needs of the future without breaching customer trust.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] R. Ahmed and S. Khalid, "Cognitive privacy and the architecture of AI-driven surveillance," *SSRN Electronic Journal*, 2025. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5745962

[2] Board of Governors of the Federal Reserve System, *The FedNow Service: Fraud Prevention Considerations for Financial Institutions*, Washington, DC, USA, 2023.

[3] Raza, *Artificial Intelligence, National Security, and Constitutional Governance in the United States: Reinventing the Rule of Law in the Digital Age*. Geh Press, 2025. Available from: https://tinyurl.com/nhk7fyak

[4] L. F. Patel and R. B. Patel, "Cross-channel fraud patterns in modern banking systems," *Journal of Financial Crime*, vol. 30, no. 2, pp. 345–362, 2023.
[5] M. A. Chohan, M. A. Farooqi, A. Raza, M. N. Rasheed, and K. Shahzad, "Artificial intelligence and intellectual property rights: From content creation to ownership," *SSRN Electronic Journal*, 2024. Available from: https://tinyurl.com/yau78cdd
[6] U.S. Federal Trade Commission, *Consumer Sentinel Network Data Book 2022*, Washington, DC, USA, 2023.
[7] Raza, "Navigating the intersection of artificial intelligence and law in healthcare: Complications and corrections," *SSRN Electronic Journal*, 2024. Available from: https://tinyurl.com/49fa2hw7
[8] W. Zhang, M. García-Soriano, and H. Zhang, "Federated learning for privacy-preserving fraud detection in multi-bank environments," *ACM Computing Surveys*, vol. 55, no. 3, pp. 1–35, 2023.
[9] Javelin Strategy & Research, *2023 Identity Fraud Report: The Virtual Fencing of Stolen Identities*, Pleasanton, CA, USA, 2023. Available from: https://tinyurl.com/yr5xd59e
[10] Raza, "Trade secrets as a substitute for AI protection: A critical investigation into different dimensions of trade secrets," *SSRN Electronic Journal*, 2024. Available from: https://tinyurl.com/mvkwswwm
[11] S. R. D. Hwang and P. T. Y. Hwang, "Machine learning for real-time payment fraud detection: A comparative study of ensemble methods," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1245–1253, 2023.
[12] Raza, "Credit, code, and consequence: How AI is reshaping risk assessment and financial equity," *Euro Vantage Journal of Artificial Intelligence*, vol. 2, no. 2, pp. 79–86, 2025. Available from: https://evjai.com/index.php/evjai/article/view/30
[13] Financial Action Task Force (FATF), *Guidance on Digital Identity*, Paris, France, 2021. Available from: https://doi.org/10.3389/fbloc.2021.627641
[14] Raza, M. A. Chauhan, N. Khan, G. Ali, and N. A. Tayyab, "Artificial intelligence and criminal liability: Rethinking criminal liability in the era of automated decision making," *SSRN Electronic Journal*, 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5376011
[15] LexisNexis Risk Solutions, *2024 True Cost of Fraud™ Report: Financial Services and Lending*, Alpharetta, GA, USA, 2024.
[16] B. Munir, A. Raza, S. Khalid, and S. M. Kasuri, "Automation in judicial administration: Evaluating the role of artificial intelligence," *SSRN Electronic Journal*, 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5209960
[17] M. R. Miller and T. G. Miller, "Synthetic identity fraud: The $6 billion threat hiding in plain sight," *IEEE Security & Privacy*, vol. 21, no. 4, pp. 78–86, 2023.
[18] P. J. Moscow and L. C. K. Moscow, "Behavioral biometrics as a robust and transparent authentication factor," *Journal of Cybersecurity*, vol. 8, no. 1, pp. 1–15, 2022.
[19] Raza and B. Munir, "The doctrine of latent copyrights: Protecting generative AI models through representational layers," *SSRN Electronic Journal*, 2025. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5745922
[20] Raza, "The application of artificial intelligence in credit risk evaluation: Obstacles and opportunities in path to financial justice," *Center for Management Science Research*, vol. 3, no. 2, pp. 240–251, 2025. Available from: https://tinyurl.com/5t55347c
[21] Raza and N. Bashir, "Artificial intelligence as a creator and inventor: Legal challenges and protections in copyright, patent, and trademark law," *SSRN Electronic Journal*, 2023. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5376048
[22] Raza, M. A. Farooqi, M. N. Rasheed, K. Shahzad, and A. A. Ansari, "Advancing legal practice: A detailed analysis of integrating AI in legal research, reasoning, and writing," *International Journal of Social Sciences Bulletin*, vol. 2, no. 4, pp. 2525–2535, 2024. Available from: https://socialsciencesbulletin.com/index.php/IJSSB/article/view/646