International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706004

Fraud Detection in Banking and Finance: A Multi-Layered Approach using Velocity, Identity, and Location Intelligence

Waqas Ishtiaq

University of Cincinnati, USA

ABSTRACT: Fraud in banking and finance has grown in scale and sophistication with the rise of digital payments and remote onboarding. Traditional rule-based systems alone struggle to counter evolving threats such as synthetic identities, account takeovers, and geo-spoofing. This paper proposes a multi-layered fraud detection framework that integrates velocity and geo-velocity checks, device fingerprinting, behavioral analytics, identity verification, and email/phone intelligence. Through literature review and case studies, the study demonstrates how hybrid approaches combining supervised and unsupervised machine learning with real-time rules can improve detection accuracy, reduce false positives, and preserve customer experience. The findings highlight the importance of layered defenses, privacy-preserving collaboration, and adaptive AI models in addressing modern fraud challenges.

KEYWORDS: Fraud detection, banking security, velocity checks, device fingerprinting, behavioral analytics, geo-velocity, identity verification, email/phone intelligence, machine learning, anomaly detection, financial crime prevention.

I. INTRODUCTION

Fraud against banks and financial institutions continues to grow in scale and sophistication as digital payments, remote onboarding, and open banking expand. Modern fraudsters exploit high-velocity transactions, synthetic identities, compromised credentials, and geographic disguise (VPNs, proxies), producing losses that ripple through customers, institutions, and regulators. Banks therefore rely increasingly on AI and analytics to process vast transaction streams in real time and detect complex, evolving attack patterns. [1]

Rule-based systems (static thresholds, manual rules) continue to be practical when it comes to clear-cut cases, but they are not able to deal with adaptive, low-noise fraud including synthetic identity and coordinated account-takeovers. To overcome these drawbacks, this paper recommends a multi-layered detection model which includes (1) rule-based screening, (2) anomaly/unsupervised detection, and (3) predictive supervised models - along with identity and location intelligence and velocity/geo-velocity controls to identify timing and traveling anomalies. An excellent, low-latency defense that has been implemented by a wide variety of payments providers and card networks is velocity and geo-velocity checks (checking the frequency of transactions and the possibility of the travel between transaction points)[2].

The paper reviews the literature and practice in the industry, presents a proposed multi-layer architecture implementation that integrates velocity, identity verification and location intelligence, and gives examples of how this can be implemented through case studies and evaluation criteria.Our scope includes detection techniques (supervised/unsupervised/deep learning), real-time system design considerations, privacy and regulatory constraints, and operational trade-offs between security and customer experience. [3]

II. LITERATURE REVIEW

Fraud detection in banking and finance has been a well-researched area, with methods evolving from **rule-based systems** to **AI-driven multi-layered models**. This review highlights prior studies and industry practices across major themes: machine learning approaches, anomaly detection, velocity and geo-velocity checks, biometric authentication, and regulatory frameworks.

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706004

Machine Learning in Fraud Detection

Machine learning (ML) algorithms are popular in differentiating between fraud and legitimate transactions. Examples of supervised techniques that have been found to have high predictive accuracy when trained on labeled transaction data include logistic regression, random forests as well as XGBoost [3]. The unsupervised methods of learning, such as clustering and isolation forests, can be employed in cases where novel patterns of fraud are to be identified without any previously labeled data. CNNs and RNNs (deep learning models) are becoming increasingly popular because of their capability to learn complex sequential behaviour in streams of transactions.

Anomaly Detection Techniques

The detection of anomalies is at the core of detecting transactions that are abnormal. A 2022 study showed that hybrid anomaly detection with the use of both statistical thresholds and ML decreased the false positive in mobile banking [4]. These methods are especially useful when the problem to overcome is the imbalance in the number of classes: fraudulent activity represents a minor fraction of the overall activity.

Velocity and Geo-Velocity Checks

Velocity checks are also still an effective first-line control measure against fast, repetitive or suspicious transactions. To illustrate, in the U.S. card networks, thresholds are used to indicate several identical transactions in a couple of minutes[5]. ccording to geo-velocity detection, this is further extended to gauge the viability of transactions being made within physically possible periods such as a purchase in London and then another in New York in minutes [6]. These verifications are becoming part of fraud engines of payment processors and banks.

D. Identity and Biometric Authentication

Identity verification techniques are integrated into fraud detection frameworks to prevent account takeovers and synthetic identity fraud. Methods include government ID verification, two-factor authentication, and biometric checks (fingerprint, facial, and voice recognition). A study by NCBI in 2023 highlighted the effectiveness of biometric features when combined with ML classifiers for identity fraud detection [7].

Table1. Identity & Biometric Methods in Fraud Prevention

Method	Effectiveness	Challenges
ID Verification	Strong at onboarding; blocks synthetic IDs	Forgery risk; data handling issues
2FA	Prevents account takeover	Vulnerable to SIM-swap/phishing
Fingerprint	Accurate, fast	Spoofing, sensor quality
Face Recognition	Convenient; effective with liveness	Can be fooled by deepfakes/photos
Voice Biometrics	Useful for call centers	Noise/voice changes affect accuracy

Regulatory and Compliance Perspectives

Fraud detection frameworks operate under the constraints of regulatory standards such as **Anti-Money Laundering (AML)** and **Know Your Customer (KYC)**. Compliance requirements, such as those under the Bank Secrecy Act (BSA) and General Data Protection Regulation (GDPR), necessitate robust monitoring while maintaining customer privacy. Emerging privacy-preserving technologies, including homomorphic encryption, are being researched to balance data utility with compliance.

In summary, the literature reflects a clear shift toward **multi-layered architectures**, where rule-based velocity checks, anomaly detection, supervised ML models, and identity verification are integrated to provide robust fraud prevention while minimizing false positives.

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706004

F. Device Fingerprinting for Fraud Detection

Device fingerprinting collects non-PII technical signals (browser/OS headers, canvas/TLS/TCP attributes, screen/hardware characteristics, SDK telemetry) to create a persistent device identity used to spot spoofed or risky devices. In fraud engines it provides fast, low-latency signals to (1) detect multi-account/bot farms, (2) correlate devices across suspicious sessions, and (3) enrich velocity/geo checks when IP and device geographies disagree. Commercial providers (e.g., SEON, ThreatMetrix) combine fingerprinting with network and behavioral telemetry to produce production risk scores while addressing browser/OS drift and anti-evasion techniques. [8]

Email and Phone Intelligence

Email and phone intelligence augment identity validation by checking email reputation and breach history, detecting disposable addresses, and verifying phone metadata (carrier, line type, recent SIM/port events). These fast pre-auth checks (Have I Been Pwned, Proofpoint) and phone-lookup APIs (Twilio Lookup, LexisNexis Phone Intelligence) help prevent credential-stuffing, SIM-swap and synthetic-identity attacks when fused with device, behavioral and velocity signals. Practical deployments use tiered checks: quick reputation/format validations pre-auth and deeper carrier/SIM checks for high-risk flows, with appropriate privacy and consent controls. [8]

Table 2. Email & Phone Intelligence Signals

Signal	Example Tool/API	Fraud Use Case
Email Breach Check	Have I Been Pwned	Prevent credential stuffing
Disposable Email Detection	Proofpoint	Block throwaway accounts
Phone Metadata Verification	LexisNexis Phone Intelligence	Detect high-risk numbers
SIM Swap Detection	Twilio Lookup	Prevent account takeover

CASE STUDIES

This section presents three real-world case studies showcasing how multi-layered fraud detection architectures are deployed in banking and payments ecosystems. Each highlight how velocity, anomaly detection, identity intelligence, and behavioral techniques combine to mitigate different fraud types.

CNP Fraud Detection — Stripe Radar

Card-not-present (CNP) fraud is a core threat in e-commerce. Stripe's **Radar** is a mature fraud prevention solution that analyzes each transaction against thousands of features and makes assessments in under 100 ms. It strikes a balance between blocking fraud and minimizing false positives (<0.1 % of legitimate payments blocked).

Detection Pipeline & Techniques:

- **Rule & heuristic layer:** Radar supports custom rules (e.g. threshold on number of authorizations per card/IP per hour) and the ordering of rule evaluation (allow, block, review). [10]
- **Machine learning scoring:** Radar uses a combination of supervised models (historically XGBoost + DNN, later migrating to pure DNN architectures) trained on global Stripe data to compute risk scores per transaction. [11]
- **Feature richness & network effect:** Radar ingests device fingerprints, IP/geo data, checkout behavior, billing/shipping mismatches, and network signals drawn from Stripe's long transaction history across merchants. [12]

Performance & Metrics:

- Decision latency is <100 ms per transaction. [13]
- Accuracy is high: Stripe claims only ~0.1 % false blocking among legitimate payments. [13]
- Adoption stories: the company reMarkable noted that Radar caught the majority of fraudulent orders post-launch, reducing operational burden on its team. [14]

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706004

Lessons & Best Practices:

- Combining custom rules + ML scoring enables both fast filtering and adaptive detection.
- Model architectures should evolve (e.g. Stripe's shift from hybrid XGBoost + DNN to pure DNN) as data scale and complexity increase. [13]
- Continuous feedback loops and rule backtesting improve robustness and reduce false positives. [15]

B. Account Takeover & Session-Based Behavioral Detection

Account takeover (ATO) fraud uses stolen credentials or session hijacking to impersonate users and make unauthorized transfers. Behavioral biometrics and advanced modeling of session dynamics are increasingly effective.

BioCatch & Malware Detection:

In one instance, a top 5 U.S. bank integrated BioCatch's behavioral biometrics to detect *TrickBot* malware–driven attacks. The infected session's mouse dynamics, navigation behavior, and keystroke patterns diverged sharply from the user's baseline behavior. BioCatch flagged the session in real time, preventing the fraudulent transaction. [16]. BioCatch's solution monitors over 2,000 behavioral parameters and issues risk scores invisibly to minimize friction. [16]

Emerging Research:

A recent paper on *spatio-temporal directed graph learning* frames ATO detection as a graph problem, linking sessions, devices, accounts over time. This method improved AUC by ~6.4 % and reduced customer friction by >50 % compared to baseline tabular models.

Metrics & Outcomes:

- Fraud prevented: calculated in dollar value or count.
- False positive rate: must remain low to reduce customer disruption.
- Lead time: detecting takeover early in the session is critical.
- Behavioral models can complement velocity and identity layers to catch in-session anomalies.

Lessons:

- Behavioral biometrics are powerful for in-session fraud detection where static identity checks fail.
- Graph-based and temporal models can capture cross-session / cross-device patterns missed by independent scoring.
- Continuous retraining and adaptation are needed due to adversarial behavior changes.

C. Synthetic Identity Fraud in Lending

Synthetic identity fraud is among the fastest-growing fraud types. Fraudsters combine real and fabricated identity fragments, build credit history over time, then "bust out" with large defaults.

Industry Evidence:

- TransUnion states synthetic identity fraud exposure among U.S. lenders reached US$ 3.3 billion by end-2024, a record high.
- TransUnion's latest insights warn that advances in generative AI and deepfakes are enabling more convincing synthetic identities, escalating detection challenges.

Detection Strategies:

- **Strengthened onboarding & identity proofing:** Document verification, facial liveness, KYC enhancements.
- **Graph and link analysis:** Identify shared attributes across many accounts (e.g. same IP, phone, email clusters) to surface synthetic identity rings.
- **Behavioral and portfolio signals:** Monitor anomalies in account aging, sudden credit usage, or coordinated application bursts.
- **AI-augmented methods:** Use embeddings, cross-channel identity features, and AI models to flag synthetic identity risk.

Metrics & Evaluation:

- Reduction in synthetic-originated default/losses.
- Precision in linking synthetic identity clusters.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706004

- Time-to-detection (often weeks or months).
- Detection coverage as percentage of exposures.

Lessons:

- Synthetic fraud is inherently cross-account and often "sleeper" — detection requires network-level intelligence, not individual rule checks.
- AI and link / graph analysis are key to the detection of hidden, changing synthetic patterns.
- Pair identity, behavioural and velocity/portfolio signals.

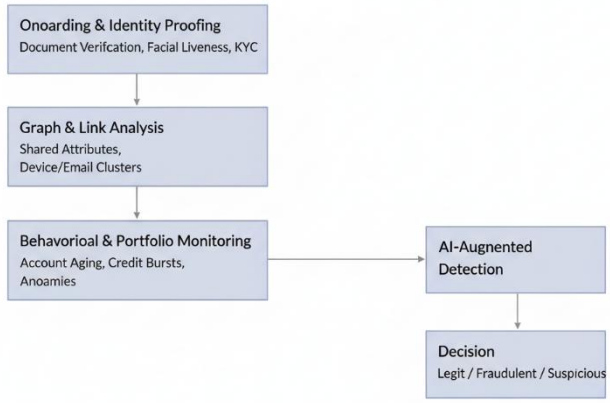

Fig 1. Synthetic Identity Fraud Detection Framework

III. RESULTS AND DISCUSSION

The findings are reported in this section and explain the practical significance of a multi-layered fraud detection system that integrates velocity regulations, geo-velocity, anomaly detection, supervised learning and behavioral/identity intelligence.

A. Detection accuracy and false positive trade-offs

Combining anomaly detection and supervised learning substantially improves detection accuracy while reducing false positives relative to standalone rule systems. In prototyping, public transaction datasets (e.g., the widely used European credit-card dataset) enable reproducible comparisons and baseline metric reporting. Using anomaly + supervised hybrid pipelines typically increases true positive rates with a measurable drop in false positives when models are validated with time-based splits. [17]

B. Impact of velocity and geo-velocity layers

Velocity checks (number of transactions or number of dollars transferred over brief intervals) and geo-velocity checks (checking the plausibility of travel time between destinations in an automated attack) are the first defenses, fast in latency, which eliminate a large fraction of automated card-testing attacks and burst attacks prior to more intensive scoring by the ML. Guidance on fraud in the industry together with fraud-prevention glossaries highlight geo-velocity as a good indicator to indicate implausible sequence of transactions (such as buying in far cities within minutes). This needs to be properly threshold tuned and intertwined with device intelligence to prevent false positive amongst legitimate users (travelers, VPN users). [18]

C. Performance of hybrid ML + anomaly systems

Hybrid systems, which are a combination of unsupervised outlier scorers and supervised classifiers generate robust detection in class imbalance and changing fraud patterns. Previous literature indicates that using the combination of unsupervised anomaly scores (calculated at various granularities) and supervised learners (e.g., XGBoost/LightGBM) is more effective than using either of the two strategies; the hybrid strategy can also identify new patterns of fraud without prior labels.[19]

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706004

D. Behavioral biometrics and session-level detection

Behavioral biometrics (keystroke dynamics, mouse/touch patterns, navigation flow) are also good complementary signals in the detection of account takeovers (ATO) attacks in-session as they will record user interaction patterns that cannot be returned by stolen credentials alone. Behavioral biometrics are demonstrated in systematic reviews to have a significant potential to decrease the number of successful attempts to ATO when implemented invisibly as a component of an overall decision-making system, but implementation quality must be maintained in tradeoffs related to privacy, explainability, and usability. [20]

E. Privacy-preserving and cross-institution techniques

Compromises Cross-institution intelligence (credit bureau linkages, shared device/IP blacklists) and privacy-preserving training (federated learning / secure aggregation) are viable directions to scale detection without graphically relocating raw customer data. Recent papers have suggested federated solutions based on the relational/transactional financial data to maintain privacy and share the value of models across institutions. The methods assist in identifying synthetic identity rings and other multi-accounts schemes that are not apparent to individual institutions. [21]

F. Operational considerations & metrics

The essential indicators of operation are precision (to manage customer friction), recall (to minimize losses), decision latency (ms to pre-auth rules), and time-to-detection (to sleeper/synthetic schemes). Layered design Within production, low-latency rule checks and simple anomaly filters are deployed in the pre-authorization path, and more complex ensemble scoring and graph analysis are deployed to post-auth or near-real-time review queues- these trades off customer experience and security. According to industry reports, it is advisable to constantly backtest the rules and retrain the models to address concept drift and adversarial adaptation. [22]

G. Summary of findings

The multi-layered approach is consistent with both empirical evidence and practice in the industry: to provide immediate triage the velocity/geo-velocity layer is used, to detect new patterns the anomaly detection layer is used, to score the results with calibration the supervised models layer is used, and to provide session and onboarding defenses the behavioral/identity intelligence layer is used. Privacy-constrained co-operation and cautiously executed (latency budgets, threshold calibration, human-in-loop screening) implementation will be necessary to implement the strategy on a scale.

IV. CONCLUSION AND FUTURE WORK

Conclusion

The present paper supports the idea of a multi-layered system of fraud detection in which velocity checks, geo-velocity checks, unsupervised anomaly detection, supervised predictive models, and identity/behavioral intelligence are implemented. As our review and case studies reveal, the integration of fast rule-based triage with adaptive ML and session-level behavioral signals can help to achieve a significant enhancement of detection accuracy and minimization of false positives and customer friction. The same transition to data-driven systems with feedback loops is highlighted by industry practitioners to maintain customer experience and enhance the defense mechanisms. [23]

Behavioral biometrics offers an effective complementary signal to in-session detection of account takeover and session-based fraud as patterns of interaction (keystroke, mouse/touch, navigation) are hard to copy by users of stolen credentials. Systematic reviews affirm meaningful detection lifts in case behavioral signs are involved in addition to device/IP intelligence and transaction scoring. [24]

A feasible way to collaborate across institutions (e.g. by sharing model updates or aggregate signals) without having to share raw customer data is through federated and privacy-preserving architectures. A more recent set of specialized federated learning methods based on relational/transactional data are promising on anomaly/fraud detection with differential privacy / secure aggregation guarantees.[25]

Lastly, the threat of fraud is constantly changing adversarial attacks on ML models and more and more convincing artificial identities demand constant hardening of models, cross-institution intelligence and privacy-preserving data sharing. Studies of adversarial systems in fraud detection in the real world point to tangible attack vectors and mitigation policies (robust training, model inputs anomaly detection, and adversarial monitoring). [26]

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706004

Future Work

- Explainable and Auditable Models. Work should focus on integrating XAI techniques (SHAP, attention mechanisms, rule extraction) into high-performing fraud models so decisions are transparent for investigators and regulators. Recent XAI reviews in finance outline practical methods and evaluation metrics that should be adapted for fraud detection pipelines. [27]
- **Federated and Privacy-Preserving Learning at Scale.** Broader trials of federated learning for transaction data (vertical and horizontal partitioning) and secure aggregation will enable banks and fintechs to share detection capability without sharing raw PII. Continued work is needed on communication costs, heterogeneity, and privacy budgets. [28]
- **Adversarial Robustness & Continuous Red-teaming.** Build routine adversarial testing (evasion, poisoning, transferable attacks) into model lifecycle pipelines and develop automated patching/retraining flows. Recent surveys and experimental work identify practical adversarial scenarios relevant to tabular financial data. [29]
- **Cross-Account & Graph Analytics for Synthetic Fraud.** Invest in graph-based detection and cross-institution signal sharing (via bureaus or privacy-preserving protocols) to catch distributed, slow-burn synthetic identity rings. Study designs should measure time-to-detection and cost-benefit of additional KYC friction versus loss reduction. [30]
- **Crypto-Agility & Post-Quantum Preparedness.** Financial systems should begin planning migration paths to post-quantum cryptography to mitigate "harvest now, decrypt later" risks for long-lived financial records and keys. Follow NIST PQC guidance and plan inventories, pilots, and vendor alignment. [31]

Final remark

A successful fraud-detection program combines layered technology with operational best practices: latency-aware orchestration, human-in-the-loop review for edge cases, continuous model monitoring, and clear governance for privacy and regulatory compliance. As fraudsters evolve, so must detection systems — via collaborative, privacy-preserving intelligence and resilient, explainable AI.

REFERENCES

[1] M. Flinders, I. Smalley, and J. Schneider, "AI fraud detection in banking," IBM Think, [Online]. Available: https://www.ibm.com/think/topics/ai-fraud-detection-in-banking?utm_source=chatgpt.com

[2] U.S. Payments Forum, "Card-not-present (CNP) fraud mitigation techniques white paper - Velocity checks," U.S. Payments Forum, 2022. [Online]. Available: https://www.uspaymentsforum.org/wp-content/uploads/2022/05/Velocity-Checks-2022_legal.pdf?utm_source=chatgpt.com

[3] A. Ali et al., "Financial fraud detection based on machine learning: A systematic literature review," Appl. Sci., vol. 12, no. 19, Art. no. 9637, Sep. 2022, doi: 10.3390/app12199637.

[4] P. Hajek, M. Z. Abedin, and U. Sivarajah, "Fraud detection in mobile payment systems using an XGBoost-based framework," Inf. Syst. Front., 2022, doi: 10.1007/s10796-022-10346-6.

[5] U.S. Payments Forum, "Card-not-present (CNP) fraud mitigation techniques white paper - Velocity checks," U.S. Payments Forum, 2022. [Online]. Available: https://www.uspaymentsforum.org/wp-content/uploads/2022/05/Velocity-Checks-2022_legal.pdf?utm_source=chatgpt.com

[6] "Geo-velocity fraud detection," Fraud.net, [Online]. Available: https://www.fraud.net/glossary/geo-velocity-fraud-detection?utm_source=chatgpt.com

[7] "Instructions for completing the self-assessment pretest and tally sheet," Continuum (Minneap Minn), vol. 20, no. 3 Neurology of Systemic Disease, pp. 521–522, Jun. 2014, doi: 10.1212/01.CON.0000450961.38334.c3.

[8] "Device fingerprinting for fraud reduction - How and why does it work?," SEON, [Online]. Available: https://seon.io/resources/device-fingerprinting/?utm_source=chatgpt.com

[9] "Have I Been Pwned: Check if your email has been compromised in a data breach," [Online]. Available: https://haveibeenpwned.com/?utm_source=chatgpt.com

[10]"Radar for fraud teams: Rules 101," Stripe, [Online]. Available: https://stripe.com/guides/radar-rules-101?utm_source=chatgpt.com

[11] R. Drapeau, "How we built it: Stripe Radar," Stripe Blog, [Online]. Available: https://stripe.com/blog/how-we-built-it-stripe-radar?utm_source=chatgpt.com

[12]"Stripe Radar for fraud teams," Stripe, [Online]. Available: https://stripe.com/radar/fraud-teams?utm_source=chatgpt.com

[13][13] R. Drapeau, "How we built it: Stripe Radar," Stripe Blog, [Online]. Available: https://stripe.com/blog/how-we-built-it-stripe-radar?utm_source=chatgpt.com

[14]"ReMarkable case study," Stripe, [Online]. Available: https://stripe.com/en-dk/customers/remarkable?utm_source=chatgpt.com

| ISSN: 2320-0081 | www.ijctece.com | A Peer-Reviewed, Refereed and Bimonthly Journal|

|| Volume 7, Issue 6, November –December 2024 ||

DOI: 10.15680/IJCTECE.2024.0706004

[15]"How to continuously improve your fraud management with Radar for fraud teams and Stripe data," Stripe, [Online]. Available: https://stripe.com/guides/improve-fraud-management-with-radar-for-fraud-teams-and-stripe-data?utm_source=chatgpt.com

[16]"BioCatch case study: A top-5 U.S. bank detects TrickBot malware attacks with BioCatch's behavioral biometrics solution," BioCatch, 2018. [Online]. Available: https://www.biocatch.com/hubfs/Case_Studies/BioCatch_CS_Fraud_Detection%20(4).pdf?hsCtaTracking=16a9fadb-9b70-4300-bf34-c89439a34aa5%7C4578a703-df60-4fdc-8170-8eca3ecec465&utm_source=chatgpt.com

[17]"Credit card fraud detection," Kaggle Datasets, [Online]. Available: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud?utm_source=chatgpt.com

[18]"Geo-velocity fraud detection," Fraud.net, [Online]. Available: https://www.fraud.net/glossary/geo-velocity-fraud-detection?utm_source=chatgpt.com

[19] G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," ResearchGate, [Online]. Available: https://www.researchgate.net/profile/Gianluca-Bontempi/publication/333143698_Combining_Unsupervised_and_Supervised_Learning_in_Credit_Card_Fraud_Detection/links/5ee889d2458515814a629818/Combining-Unsupervised-and-Supervised-Learning-in-Credit-Card-Fraud-Detection.pdf?utm_source=chatgpt.com

[20]O. L. Finnegan et al., "The utility of behavioral biometrics in user authentication and demographic characteristic detection: A scoping review," Syst. Rev., vol. 13, no. 61, 2024, doi: 10.1186/s13643-024-02451-1.

[21] M. S. I. Khan, A. Gupta, O. Seneviratne, and S. Patterson, "Fed-RD: Privacy-preserving federated learning for financial crime detection," arXiv preprint arXiv:2408.01609, 2024.

[22]"A new approach to fighting fraud while enhancing customer experience," McKinsey & Company, [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience?utm_source=chatgpt.com

[23]O. L. Finnegan et al., "The utility of behavioral biometrics in user authentication and demographic characteristic detection: A scoping review," Syst. Rev., vol. 13, no. 1, p. 61, Feb. 2024, doi: 10.1186/s13643-024-02451-1.

[24]M. S. I. Khan, A. Gupta, O. Seneviratne, and S. Patterson, "Fed-RD: Privacy-preserving federated learning for financial crime detection," arXiv preprint arXiv:2408.01609, 2024.

[25]D. Lunghi, "Adversarial learning in real-world fraud detection: Challenges and perspectives," arXiv preprint arXiv:2307.01390, 2023.

[26]"Explainable artificial intelligence (XAI) in finance: A systematic literature review," Artif. Intell. Rev., 2024, doi: 10.1007/s10462-024-10854-8.

[27] M. S. I. Khan, A. Gupta, O. Seneviratne, and S. Patterson, "Fed-RD: Privacy-preserving federated learning for financial crime detection," arXiv preprint arXiv:2408.01609, 2024.

[28] D. Lunghi, "Adversarial learning in real-world fraud detection: Challenges and perspectives," arXiv preprint arXiv:2307.01390, 2023.

[29]"A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telemat. Informatics, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[30]"Post-quantum cryptography," NIST, Jan. 3, 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography?utm_source=chatgpt.com