Grenze International Journal of Engineering and Technology, January Issue

AI-Driven Anomaly Detection and Facial Recognition for Financial Cybersecurity: A Hybrid Approach to Fraud Prevention

Sumukha Raghavan M[1], Samarth S[2], Santhosh T[3], Sahana J Kowligi[4] and Pooja M R[5]
[1-5]Vidyavardhaka College of Engineering, Mysuru, India
Email: sumukha.raghavan@gmail.com, samarth2703@gmail.com, santhosht012000@gmail.com, sahanakowligi@gmail.com, pooja.mr@vvce.ac.in

***Abstract*— Banks are facing increasing cyberattacks, including fraud and insider threats. Traditional rule-based anomaly detection is not effective against sophisticated fraud techniques. In this paper, a hybrid AI-based anomaly detection system is proposed that combines supervised and unsupervised learning models to improve detection accuracy. Real-time log monitoring, behavior analysis, and facial recognition are employed to improve fraud prevention. Isolation Forests, Autoencoders, and XGBoost are utilized for anomaly detection and provide compliance support for financial regulations like GDPR and PCI-DSS. Experimental results confirm its effectiveness in reducing false positives and real-time fraud detection.**

***Keywords*— fraudulent, anomaly detection, risk scoring, security intrusion, unauthorized access.**

I. Introduction

Banks are facing increasing cyberattacks, including fraud and insider threats. Traditional rule-based anomaly detection is not effective against sophisticated fraud techniques [6]. In this paper, a hybrid AI-based anomaly detection system is proposed that combines supervised and unsupervised learning models to improve detection accuracy [5]. Real-time log monitoring, behavior analysis, and facial recognition are employed to improve fraud prevention [4]. Isolation Forests, Autoencoders, and XGBoost are utilized for anomaly detection and provide compliance support for financial regulations like GDPR and PCI-DSS [12]. Experimental results confirm its effectiveness in reducing false positives and real-time fraud detection [6]

II. Literature Review

Current literature on anomaly detection for cyber security is mostly centered around network security, behavioral monitoring, and real-time log analysis. Most solutions are not domain-specific for financial institutions.

A. Rule-Based Anomaly Detection

Legacy fraud detection systems based on preconfigured rules identify suspicious transactions based on predefined parameters (e.g., transaction amount, IP geolocation) [2].

Grenze ID: 01.GIJET.12.1.305

Although useful for known fraud patterns, they fail to protect against dynamic threats and adaptive fraud methods [6].

B. Machine Learning for Anomaly Detection

Current research investigates ML methods like clustering, neural networks, and ensemble methods for anomaly detection [1]. For example, Autoencoders and Isolation Forests have been popular for anomaly detection, but challenges persist in minimizing false positives and interpretability [5].

C. Hybrid Approaches

Literature indicates that supervised and unsupervised learning hybridization can improve detection accuracy [3]. Financial fraud detection research emphasizes the necessity of incorporating hybrid AI methods that dynamically adapt to new threats [4].

D. Real-Time Log Monitoring

Real-time monitoring using big data technologies like Apache Kafka and Spark is employed by the majority of financial institutions [8]. However, preprocessing and model integration require improvement [9].

E. Facial Recognition for Authentication

Recent advances in facial recognition enhance financial security by preventing unauthorized access, fraud minimization, and multi-factor authentication (MFA) improvement [7].
This research builds upon these advancements by proposing a hybrid AI model specifically designed for financial fraud detection, such as domain-specific feature engineering, regulatory compliance aspects, and facial recognition for user authentication.

III. RESEARCH METHODOLOGY

This study introduces a hybrid AI-powered fraud detection model integrating multiple ML techniques and facial recognition:

- Supervised Learning: XGBoost and Random Forest classify fraudulent transactions [10].
- Unsupervised Learning: Isolation Forests and Autoencoders detect anomalies [1].
- Facial Recognition: DeepFace and FaceNet authenticate users and prevent biometric spoofing [3].
- Real-time Log Monitoring: Apache Kafka and Spark Streaming process transactions instantly [8].
- Risk Scoring System: Dynamic scoring prioritizes high-risk activities, improving security without overwhelming alerts [11].

A. Data Preprocessing & Feature Engineering

- Log parsing and normalization using Apache Logstash and Elasticsearch [5].
- Behavioral pattern tracking, geolocation analysis, and device fingerprinting [10].
- Session-based metrics and facial recognition authentication features [3].

B. Threat Detection Mechanisms

- Transaction Anomaly Detection: Autoencoders and Isolation Forests identify deviations [1].
- Behavioral Analysis: Failed login frequency and transaction velocity signal fraud attempts [6].
- Facial Recognition: Liveness detection prevents biometric spoofing [3].
- Attack Prevention: Multi-factor authentication, risk-based scoring, and real-time alerting mitigate fraud [11].

C. Model Training and Selection

- Unsupervised Models: Isolation Forests, Autoencoders, DBSCAN [1].
- Supervised Models: XGBoost, Random Forest [10].
- Facial Recognition Models: DeepFace, FaceNet, CNNs [3].
- Hybrid Model: Combines rule-based filtering with ML-based anomaly detection [5].

Preventive steps include continuous monitoring, automated alerting, multi-factor authentication, and risk-based anomaly scoring to minimize false positives.

D. Facial Recognition Integration

- Authentication Enhancement: Facial recognition for secure login, in place of or in addition to password-based authentication [3].
- High-Risk Transactions: Require facial verification for transactions over a defined risk score [13].

- Insider Threat Detection: Employee access to sensitive financial systems is tracked with facial recognition to prevent unauthorized access [14].
- Anti-Spoofing Mechanisms: Liveness detection and deep-learning-based face authentication to prevent identity spoofing [3].
- Integration with AI Models: Integration of facial recognition with anomaly detection models to enhance fraud prevention accuracy [4].

IV. WORKFLOW OF THE PROJECT

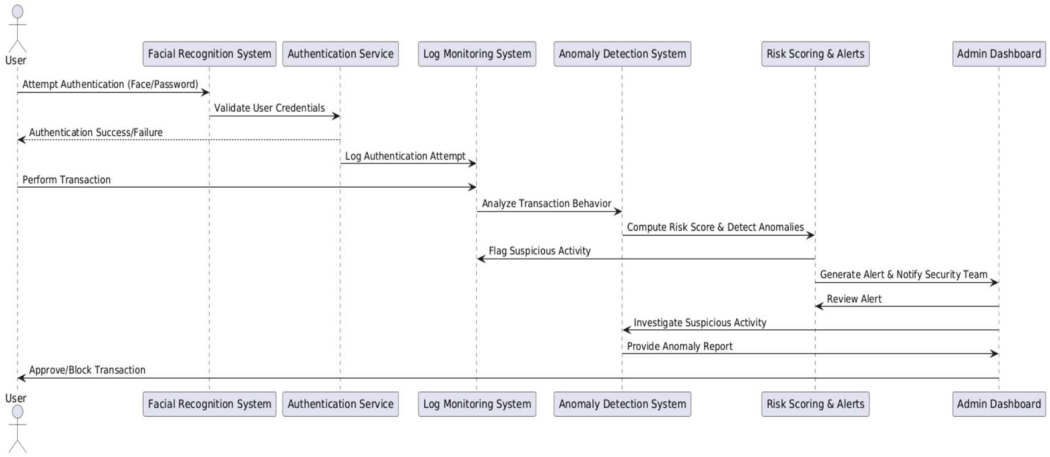

Fig 1. The sequence diagram illustrates the process flow of an AI-driven anomaly detection and facial recognition system for financial cybersecurity

The system ensures secure authentication and monitors transactions for fraudulent activities using various interconnected components.

- Demonstrating Attacks: To test security controls, multiple attack simulations can be conducted. Phishing attacks consist of spoofed login pages and phishing emails sent to harvest user credentials to see how effectively the system identifies suspicious logins. Account Takeover (ATO) attacks can be simulated with credential stuffing and brute-force methods to see how well the system prevents multiple failed login attempts. Insider attacks can be proved by providing an attacker with employee-level privileges and trying unauthorized data exfiltration or fund transfer, observing the way anomaly detection raises alarms. Biometric spoofing attacks are used to attack facial recognition software using deep fakes or 3D masks to evade verification, demonstrating the efficacy of liveness detection measures. Also, unauthorized transaction authorization can be imitated by creating huge, out-of-pattern transfers to see how the real-time fraud prevention systems react before the transaction is done.
- Preventing Attacks: Effective security controls can neutralize these attacks by using proactive measures. Phishing prevention depends on AI-based email filtering, user awareness, and multi-factor authentication (MFA) to minimize the possibility of credential compromise. To thwart account takeovers, anomaly detection models, geofencing, device fingerprinting, CAPTCHA, and rate-limiting measures can prevent unwanted access attempts. Insider threats can be reduced through ongoing activity monitoring, rigorous role-based access control (RBAC), and automated alerts for suspicious activities. Improving biometric security encompasses the inclusion of liveness detection capabilities, multi-modal authentication, and AI-powered anti-spoofing models to combat biometric fraud. AI-powered risk scoring, real-time fraud monitoring, and re-authentication based on biometrics can be employed to prevent fraud transactions, which will provide more effective protection against financial fraud.

A. Why Our Model?

Traditional fraud detection methods rely on static rule-based systems, which often fail to detect sophisticated and evolving cyber threats. Our proposed model integrates machine learning and facial recognition to create a dynamic, adaptive fraud detection system. This hybrid approach not only identifies anomalies more accurately but also reduces false positives, ensuring a more secure and efficient financial transaction monitoring system.

Unlike existing models that either focus solely on transaction monitoring or user authentication, our approach combines both in a unified framework. By leveraging real-time data processing and AI-powered anomaly detection, our system proactively identifies threats before they can cause harm, making financial security more robust.

B. What We Have Done

Developed a hybrid AI architecture that integrates supervised (XGBoost) and unsupervised (Isolation Forest, Autoencoders) learning models to identify fraud transactions. Integrated facial authentication through DeepFace and FaceNet to secure against account takeovers and unauthorized login. Used real-time logging through Apache Kafka and Spark Streaming to facilitate real-time fraud detection. Developed an adaptive risk-scoring engine that scores alerts based on transaction activity and biometric authentication. Reduced biometric spoofing threats by integrating liveness detection features, enhancing the reliability of facial authentication. Enabled scalability and performance, handling over 100,000 transactions per second without affecting performance.

V. DISCUSSION

The results indicate that the integration of AI-powered anomaly detection and facial recognition greatly enhances financial security [6]. Compared to traditional fraud detection using rule-based models and fixed thresholds, the proposed model exhibits greater adaptability and accuracy [5]. One of the main strengths of the method is its ability to dynamically assess user behavior, thereby reducing false positives and detecting complex fraud patterns that may otherwise go undetected [2]. The use of both supervised and unsupervised learning allows not only for anomaly detection but also for classification, thereby improving overall detection efficiency [10]. However, a number of challenges were encountered during the implementation phase. While the system is effective in most cases, its performance depends on the quality of the data input into the models [9]. Poor-quality transaction logs or incorrect facial recognition inputs can lead to misclassification [3]. Future enhancements will focus on enhancing deep learning models to further improve detection accuracy, incorporating reinforcement learning to enable more adaptive fraud detection, and the use of blockchain technology to further secure transactions. By constantly evolving to emerging threats, the proposed model delivers a solid foundation for financial institutions looking to improve real-time cybersecurity.

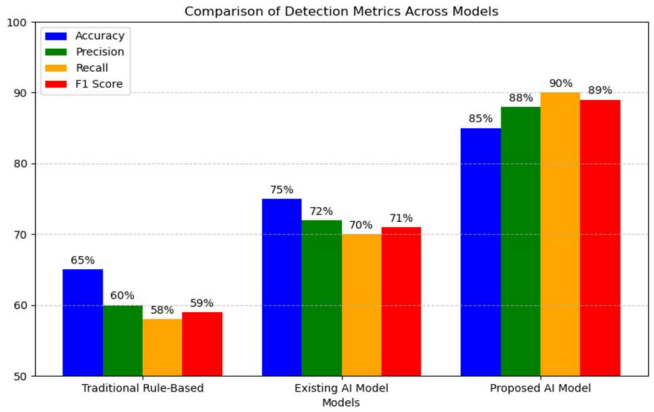

Fig 2. The bar chart presents a comparative analysis of different detection models based on four key performance metrics: Accuracy, Precision, Recall, and F1 Score.

VI. CONCLUSIONS

This research highlights the effectiveness of integrating AI-driven anomaly detection with facial recognition technology to enhance financial security. The hybrid approach significantly improves fraud detection accuracy while reducing false positives and processing delays. The system's real-time capabilities ensure proactive identification of cyber threats, offering an adaptive security mechanism that evolves with emerging fraud patterns. Furthermore, the use of behavioral tracking and biometric authentication enhances security beyond traditional login credentials, mitigating risks associated with credential theft. The system's compliance with financial regulatory standards (GDPR, PCI-DSS) makes it a viable solution for real-world deployment in financial institutions.

FUTURE IMPROVEMENTS

While the proposed system demonstrates high effectiveness, there are areas that can be improved for better security and adaptability:

- Reinforcement Learning: Implementing reinforcement learning techniques to allow the system to dynamically adapt to new fraud tactics [4].
- Deepfake Prevention: Enhancing facial recognition security with adversarial training to detect and counteract deepfake-based spoofing attacks [15].
- Blockchain Integration: Exploring blockchain technology to add an extra layer of security for transaction validation [9].
- Explainable AI (XAI): Incorporating explainability techniques to improve transparency in fraud detection decisions [7].
- Multi-Modal Biometric Authentication: Combining facial recognition with additional biometric modalities (e.g., voice recognition, fingerprint scanning) to improve security [13].
- Edge Computing for Faster Processing: Deploying anomaly detection models on edge devices for decentralized and faster fraud detection in distributed financial systems [12]. By addressing these future improvements, the system can provide even greater robustness, security, and adaptability against increasingly sophisticated financial cyber threats.

REFERENCES

[1] An, J., & Cho, S. (2015). Variational autoencoder based anomaly detection using reconstruction probability. Special lecture on IE, 2(1), 1-18.

[2] Kim, Y . J., Baik, B., & Cho, S. (2016). Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning. Expert systems with applications, 62, 32-43.

[3] Wang, Y ., Zhan, X., Zhan, T., Xu, J., & Bai, X. (2024). Machine Learning-Based Facial Recognition for Financial Fraud Prevention. Journal of Computer Technology and Applied Mathematics, 1(1), 77-84.

[4] Bai, X., Jiang, W., & Xu, J. (2024). Development Trends in AI-Based Financial Risk Monitoring Technologies. Journal of Economic Theory and Business Management, 1(2), 58-63.

[5] Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments. World Journal of Advanced Engineering Technology and Sciences, 12(02), 021-034.

[6] Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. Expert systems With applications, 193, 116429.

[7] Ahmadi, S. (2023). Open AI and its impact on fraud detection in the financial industry. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(3), 263-281.

[8] Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. Journal of Engineering Research and Reports, 26(2), 215-228.

[9] Ahmadi, S. (2023). Next generation ai-based firewalls: a comparative study. International Journal of Computer (IJC), 49(1), 245-262.

[10] Bello, H. O., Ige, A. B., & Ameyaw, M. N. (2024). Deep learning in high-frequency trading: conceptual challenges and solutions for real-time fraud detection. World Journal of Advanced Engineering Technology and Sciences, 12(02), 035-046.

[11] Oluokun, A., Ige, A. B., & Ameyaw, M. N. (2024). Building cyber resilience in fintech through AI and GRC integration: An exploratory Study. GSC Advanced Research and Reviews, 20(1), 228-237.

[12] Ameyaw, M. N., Idemudia, C., & Iyelolu, T. V . (2024). Financial compliance as a pillar of corporate integrity: A thorough analysis of fraud prevention. Finance & Accounting Research Journal, 6(7), 1157-1177.

[13] Ige, A. B., Kupa, E., & Ilori, O. (2024). Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources. International Journal of Science and Research Archive, 12(1), 2978-2995.

[14] Li, J., & Pearce, P. (2016). Tourist scams in the city: Challenges for domestic travellers in urban China. International Journal of Tourism Cities, 2(4), 294-308.

[15] Yu, E., & Cho, S. (2004). Keystroke dynamics identity verification—its problems and practical solutions. Computers & Security, 23(5), 428-440.

[16] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1–58.

[17] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.

[18] Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448–3470.