AI-DRIVEN ADAPTIVE FRAMEWORK FOR BEHAVIORAL IDENTITY MAPPING AND SECURE FINANCIAL TRANSACTION

Ms. A. SUNITHA M.E,
Assistant Professor, Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – asunitha2022@gmail.com

Ms. JEANE MAXY P,
Student, Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – jeanemaxy2004@gmail.com

Ms. SANYA JOSHY I V,
Student, Computer Science and Engineering,
St. Joseph College of Engineering, Chennai-602117, Tamil Nadu,
Email Id – joshysanya@gmail.com

Abstract -- Digital financial ecosystems are increasingly vulnerable to identity fraud, account takeovers, transaction manipulation, and synthetic identity attacks. Traditional authentication mechanisms such as passwords and static verification systems are insufficient against evolving behavioral fraud strategies. This research proposes an AI-Driven Adaptive Framework for Behavioral Identity Mapping and Secure Financial Transactions that integrates behavioral biometrics, deep learning–based identity modeling, anomaly detection, and adaptive risk scoring mechanisms.

The framework continuously learns user behavioral patterns such as typing rhythm, transaction frequency, geolocation patterns, device fingerprints, and interaction dynamics. Using contextual embeddings and adaptive neural anomaly detection, the system detects deviations in behavioral identity signatures before approving financial transactions. Unlike static rule-based fraud detection systems, the proposed architecture enables real-time adaptive authentication, zero-day fraud detection, and dynamic risk-based authorization.

The modular architecture ensures scalability, regulatory compliance support, and integration with API-based financial infrastructures. This work contributes toward building intelligent, self-adaptive, and secure digital financial ecosystems.

I.INTRODUCTION

The rapid expansion of digital banking, mobile payments, and online financial services has significantly improved transaction convenience and accessibility. However, this digital transformation has also increased exposure to cyber threats such as identity theft, account takeover, and financial fraud. Traditional authentication methods, including passwords and one-time passwords (OTPs), are increasingly vulnerable to sophisticated attacks and social engineering techniques. To address these challenges, Artificial Intelligence (AI) has become a key enabler in modern fraud detection systems. AI-based approaches analyze transaction behavior, contextual parameters, and historical patterns to identify anomalies in real time. Behavioral identity mapping, in particular, enhances security by continuously monitoring user-specific patterns such as spending habits, device usage, transaction timing, and activity frequency. Despite these advancements, many existing fraud detection models lack adaptability and generate high false-positive rates, leading to inconvenience for legitimate users. Therefore, there is a need for an intelligent and adaptive framework that continuously learns from user behavior while dynamically evaluating transaction risk .This paper proposes an AI-Driven Adaptive Framework for Behavioral Identity Mapping and Secure Financial Transactions. The framework integrates multi-factor contextual risk scoring, real-time behavioral monitoring, and adaptive learning mechanisms to enhance fraud detection accuracy. By combining automated AI-based risk evaluation with additional verification for high-risk transactions, the proposed system ensures a balance between security, usability, and scalability in modern digital financial ecosystems.

II.BACKGROUND AND MOTIVATION

GROWTH OF DIGITAL FINANCIAL SYSTEM

The adoption of online banking, digital wallets, and fintech platforms has expanded financial accessibility. However, increased digital exposure has amplified fraud vectors.

With the rapid growth of digital banking, UPI systems, online payments, and e-commerce platforms, financial transactions have become increasingly convenient and accessible. However, this digital transformation has also led to a significant rise in cyber fraud, identity theft, and unauthorized financial activities. Traditional security mechanisms such as passwords, PINs, and OTP-based authentication are often insufficient against modern fraud techniques. Attackers exploit stolen credentials, phishing attacks, and social engineering to bypass static authentication systems.

To address these challenges, behavioral identity mapping has emerged as a promising solution. Instead of relying solely on static credentials, behavioral systems analyze user transaction patterns such as spending habits, device usage, time patterns, and activity velocity to detect anomalies.

Artificial Intelligence enables adaptive fraud detection by continuously learning and updating user behavioral profiles. This makes security systems more intelligent, dynamic, and capable of detecting suspicious activities in real time.

The motivation behind this work is to develop an AI-driven adaptive framework capable of continuously learning user behavior, dynamically assessing transaction risk, and strengthening fraud prevention while maintaining usability. The proposed solution aims to bridge the gap between intelligent fraud detection and practical financial system implementation, ensuring secure and reliable digital transactions in modern financial ecosystems.

III.NOVEL APPLICATIONS OF THE PROJECT

The proposed AI-Driven Adaptive Framework introduces a novel behavioral-centric security architecture for digital financial transactions. Unlike traditional authentication systems that rely primarily on static credentials such as passwords, PINs, or one-time passwords, the proposed system leverages dynamic behavioral identity mapping combined with adaptive multi-factor risk evaluation.

The novelty of this work lies in the integration of real-time behavioral profiling with contextual risk fusion mechanisms. The system continuously analyzes transaction attributes including spending deviation, device trust level, temporal access patterns, and transaction velocity to generate a normalized adaptive risk score. This behavioral intelligence model enables continuous authentication rather than single-point verification.

Furthermore, the framework incorporates an adaptive learning mechanism that updates the user's behavioral baseline after each verified transaction. This self-updating profile enhances detection accuracy over time and reduces false positives compared to static rule-based systems.

Another novel contribution is the implementation of a multi-parameter weighted risk fusion model that dynamically adjusts decision thresholds based on transaction magnitude and contextual deviation. This allows the system to distinguish between legitimate behavioral shifts and potential fraud attempts.

The inclusion of bilingual voice-based feedback enhances accessibility and user inclusiveness, extending secure financial services to digitally semi-literate populations — a feature rarely addressed in existing fraud detection frameworks.

The proposed framework introduces a behavior-based authentication approach for securing

financial transactions. It dynamically analyzes user spending patterns, device usage, time behavior, and transaction velocity to generate an adaptive risk score. The system continuously updates the user's behavioral profile, enabling real-time fraud detection and intelligent verification. This approach enhances security, reduces false positives, and provides a more adaptive alternative to traditional static authentication methods.

IV. ROLE AND POTENTIAL

ROLE:

A. The proposed framework introduces a dynamic behavioral profiling mechanism that continuously evaluates user transaction patterns instead of relying solely on static credentials such as passwords or OTPs. This enhances identity verification reliability and reflects real-time behavioral shifts.

B. The framework combines automated AI-based risk scoring with secondary human verification (PIN-based confirmation). This hybrid approach ensures both security robustness and usability balance.

C. Traditional fraud systems often generate high false alarms. The proposed adaptive baseline updating mechanism reduces false positives by learning normal user behavior over time, thereby improving trust and system efficiency.

D. The architecture is modular, allowing integration with banking APIs, fintech systems, or enterprise-level transaction platforms. This scalability increases industrial applicability and research relevance.

E. The framework bridges the gap between Artificial Intelligence, Behavioral Biometrics, and Financial Transaction Security, contributing interdisciplinary value to research.

F. The inclusion of real-time analytics dashboards provides transparency, risk visualization, and audit logs, supporting forensic analysis and regulatory compliance

POTENTIAL:

A. The topic aligns with current research trends in AI-driven fraud detection, behavioral biometrics, adaptive authentication, and financial cybersecurity, making it suitable for IEEE, Springer, and Scopus-indexed journals.

B. The framework can be extended with real-world datasets, accuracy evaluation metrics (Precision, Recall, F1-Score, ROC-AUC), and comparative performance analysis to strengthen empirical research contribution.

C. The risk-scoring engine can be enhanced with supervised or unsupervised learning models such as Random Forest, LSTM, or Autoencoders, increasing the research novelty.

D. The system can incorporate explainability modules to interpret risk decisions, which is a highly demanded research area in trustworthy AI systems.

E. The framework is adaptable for digital wallets, UPI systems, cross-border payments, and mobile banking applications, enhancing real-world impact.

F. The framework is adaptable for digital wallets, UPI systems, cross-border payments, and mobile banking applications, enhancing real-world impact.

G. Potential research extensions include blockchain-based transaction validation, federated learning for privacy preservation, and multi-modal biometric fusion.

V.METHODOLOGY

The proposed AI-Driven Adaptive Framework follows a structured methodology consisting of behavioral data collection, contextual risk analysis, adaptive learning, and secure decision-making. Initially, the system captures transaction-related parameters such as user identity, transaction amount, device information, transaction time, and transaction frequency. These parameters form the behavioral profile of each user. A baseline model is created using historical transaction data to represent normal behavioral patterns. Next, the framework performs contextual risk evaluation. The transaction amount deviation from the user's average spending, device trust level, time-based activity patterns, and transaction velocity are analyzed. Each factor is assigned a weighted risk score. These scores are combined to generate a final adaptive risk value between 0 and 1.

The system continuously updates the user's behavioral baseline after each successful transaction. This adaptive learning mechanism ensures that the model evolves with

changing user patterns, reducing false positives over time.

Finally, all transaction records are stored in a structured database, and analytical dashboards are generated for monitoring, visualization, and audit purposes. This methodology ensures real-time fraud detection, scalability, and practical deployment in digital financial systems.

VI.FUTURE ENHANCEMENTS

The proposed AI-Driven Adaptive Framework can be further enhanced by integrating advanced deep learning models such as LSTM, Autoencoders, or Transformer-based architectures to improve anomaly detection accuracy and predictive capability. These models can help in identifying complex behavioral patterns that traditional scoring mechanisms may not capture.

Future improvements may also include the incorporation of Explainable AI (XAI) techniques to provide transparent reasoning for risk decisions. This will increase user trust and ensure regulatory compliance in financial systems. Additionally, integrating blockchain technology can enhance transaction integrity and provide tamper-proof validation mechanisms.

Finally, deploying the system in cloud-native and large-scale banking environments will improve scalability, real-time responsiveness, and industry adoption, making it suitable for next-generation secure digital financial ecosystems.

VII. CONCLUSION

The proposed AI-Driven Adaptive Framework for Behavioral Identity Mapping and Secure Financial Transactions presents an intelligent and scalable solution to modern financial fraud challenges. Unlike traditional authentication systems that rely on static verification methods, this framework introduces continuous behavioral monitoring combined with adaptive risk assessment to ensure secure and reliable transaction processing.

By integrating contextual risk parameters such as transaction amount deviation, device trust level, time-based behavioral patterns, and transaction velocity, the system enhances real-time fraud detection accuracy. The adaptive learning mechanism enables the framework to evolve with user behavior, thereby reducing

false positives while maintaining high security standards.

Overall, the proposed framework contributes to the advancement of AI-based financial cybersecurity by offering a dynamic, modular, and extensible security model. It demonstrates strong potential for academic research, industrial deployment, and future expansion into advanced domains such as explainable AI, federated learning, and blockchain-integrated secure transaction systems.

VIII. REFERENCE

1. **M. Hassan, Y. Chen, and D. Park, "Real-Time Fraud Detection in Digital Payment Systems Using Adaptive Machine Learning Models," IEEE Access, vol. 12, pp. 84521–84534, 2024.**
2. **S. Banerjee and A. Mukherjee, "Context-Aware Behavioral Analytics for Secure Financial Transactions," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 4120–4132, 2024.**
3. **K. Reddy and H. Al-Mutairi, "Adaptive Risk-Based Authentication Framework for Online Banking Systems," IEEE Internet of Things Journal, vol. 11, no. 7, pp. 6234–6246, 2024.**
4. **S. Chen and J. Wang, "Real-Time Risk-Based Authentication Using Adaptive Machine Learning Frameworks," Journal of Cybersecurity and Privacy, vol. 4, no. 2, 2024.**
5. **A. Sharma and R. Malhotra, "Behavioral Biometrics for Fraud Detection in Digital Banking: An AI-Driven Approach," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 450–462, 2024.**
6. **H. Alqahtani and M. Lee, "Deep Learning-Based Transaction Risk Scoring for Online Payment Systems," IEEE Access, vol. 12, pp. 93211–93225, 2024.**
7. **T. Nguyen and H. Lee, "Anomaly Detection in Financial Velocity Patterns using Deep Learning," Sensors, vol. 25, no. 1, 2025.**
8. **L. Zhang and P. Sharma, "Explainable AI Models for Financial Fraud Detection Using Behavioral Patterns," IEEE Transactions on Artificial Intelligence, vol. 6, no. 1, pp. 102–114, 2025.**
9. **V. Narayanan and S. Kumar, "Anomaly Detection in Real-Time Financial Transactions Using Hybrid Learning Models," IEEE Access, vol. 13, pp. 11567–11580, 2025.**
10. **M. Rahman and K. Lee, "Deep Learning Approaches for Behavioral Anomaly Detection in FinTech Systems," Future Generation Computer Systems, vol. 156, 2025.**

11. P. Roy and S. Banerjee, "Blockchain-Integrated Secure Transaction Models for Smart Banking," Journal of Information Security and Applications, vol. 82, 2024.

.