World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

AI-enhanced adaptive two-factor authentication mechanisms for secure and frictionless financial services

Ashmitha Nagraj *

Principal Full Stack Engineer.

World Journal of Advanced Research and Reviews, 2026, 30(01), 370-376

Publication history: Received on 24 February 2026; revised on 04 April 2026; accepted on 06 April 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.30.1.0732

Abstract

Traditional Static Multi-Factor Authentication is no longer sufficient to protect against the growing sophistication of cyber threats such as AI-Generated Deepfakes and Automated Credential Stuffing. Furthermore, the rigid nature of traditional authentication protocols creates significant user friction, which leads to High-Transaction abandonment rates. This paper examines an Artificial Intelligence (AI)-Based Adaptive Two-Factor Authentication (A2FA) or Risk-Based Authentication (RBA) system that uses Machine Learning (ML), behavioral biometrics and Real-Time contextual analysis to dynamically change security friction based upon a calculated risk score. This paper presents a comprehensive architectural framework, review recent empirical advancements such as Dual-Agent Long-Term Memory (LTM) and Short-Term Memory (STM) configurations, and evaluates the tradeoff between Robust Security (Zero Trust) and seamless user experience. Ultimately, the research will demonstrate that AI-based adaptive mechanisms can reduce false rejection rates while maintaining Sub-Millisecond processing latency, thus creating secure and frictionless digital banking environments.

Keywords: Adaptive Authentication; Risk-Based Authentication; Machine Learning; Behavioral Biometrics; Financial Services; Cybersecurity; Multi-Factor Authentication (MFA)

1. Introduction

Rapid technological advancement in the financial industry has led to an increase in cyber-fraud cases. In 2023, financial institutions experienced over $6.8 billion in losses due to fraudulent activity [1]. Security models have traditionally relied on static 2-Factor Authentication (2FA) / Multi-Factor Authentication (MFA). Users are required to enter a Knowledge Factor and a Possession Factor of one-time password or hardware token for each transaction.

Although static MFA greatly enhances the level of security compared to Single Factor Authentication, it creates a rigid obstacle to the user experience. It is reported that as many as 73% of users will abandon their digital transactions if they encounter too much friction from poor implementation of static MFA [1]. Static MFA is also highly susceptible to advanced phishing, SIM-Swap, and Adversary in the Middle (AiTM) attacks [2].

To reconcile the inherent trade-off between strict security and user convenience, the financial industry is transitioning toward Adaptive Authentication or Risk-Based Authentication (RBA) [3]. Enhanced through Artificial Intelligence (AI) and Machine Learning (ML), adaptive systems continuously evaluate the contextual and behavioral risk of a transaction in real time. Consequently, adaptive systems enforce a step-up authentication process e.g., a biometric scan or one-time password (OTP) only if an anomaly is identified in the user's behavior [4]. The research for this article examines the technological frameworks and empirical efficacies of AI enhanced adaptive two-factor authentication (A2FA) in financial services as well as the underlying mechanisms.

* Corresponding author: Ashmitha Nagraj

2. Related Work

Recent academic literature highlights a paradigm shift from traditional rule-based security toward behavior-driven and risk-adaptive models.

2.1. Machine Learning in Adaptive Security

A systematic review of knowledge concerning mobile adaptive authentication found that over 64% of recent peer-reviewed frameworks utilized Machine Learning for continuous authentication and to prevent unauthorized access [2]. Researchers demonstrated that using ensemble at the feature level is more effective than using a single classifier model with multimodal biometrics systems [5].

Machine Learning (ML) plays a foundational role in enabling adaptive security across the four stages illustrated: **Predict, Prevent, Detect, and Respond**, all governed by evolving **policies and compliance requirements**. Unlike static rule-based systems, ML-driven adaptive security continuously learns from user behavior, system activity, network patterns, and payload data to dynamically adjust security posture.

During the Prediction phase, Machine Learning (ML) models use historical logs, behavioral biometrics, transaction flows and system telemetry to predict new threat vectors and vulnerabilities. The supervised learning algorithms of Random Forests or Gradient Boosting will be used to categorize "legitimate" versus "suspicious" behavior, whereas unsupervised learning models will be applied to find anomalies in large dimensioned financial data sets. The goal of this phase is to be able to predict where possible abnormal usage may occur so that organizations can transition their defensive posture from reactive to proactive risk mitigation.

During the Prevent phase, predictions made during the Predict phase are turned into an automated control process. Predictive insight is utilized to create an Automated Risk Scoring Engine that will automatically "quarantine" a session that has been deemed suspicious, limit exposure through Adaptive Access Controls and dynamically implement Step-Up Authentication. Through Reinforcement Learning, these predictive controls are continually optimized through the adjustment of thresholds based on evolving Attacker Tactics.

The Detect phase utilizes Real-Time Anomaly Detection through streaming Machine Learning (ML) pipelines. These pipelines continually monitor User Sessions, Transaction Velocity, Device Fingerprint Changes and Behavioral Drift to identify a compromised system or insider threat with Low Latency. Precision, Recall and False-Positive Rate are used to measure detection accuracy for the purpose of ensuring both Security and User Experience.

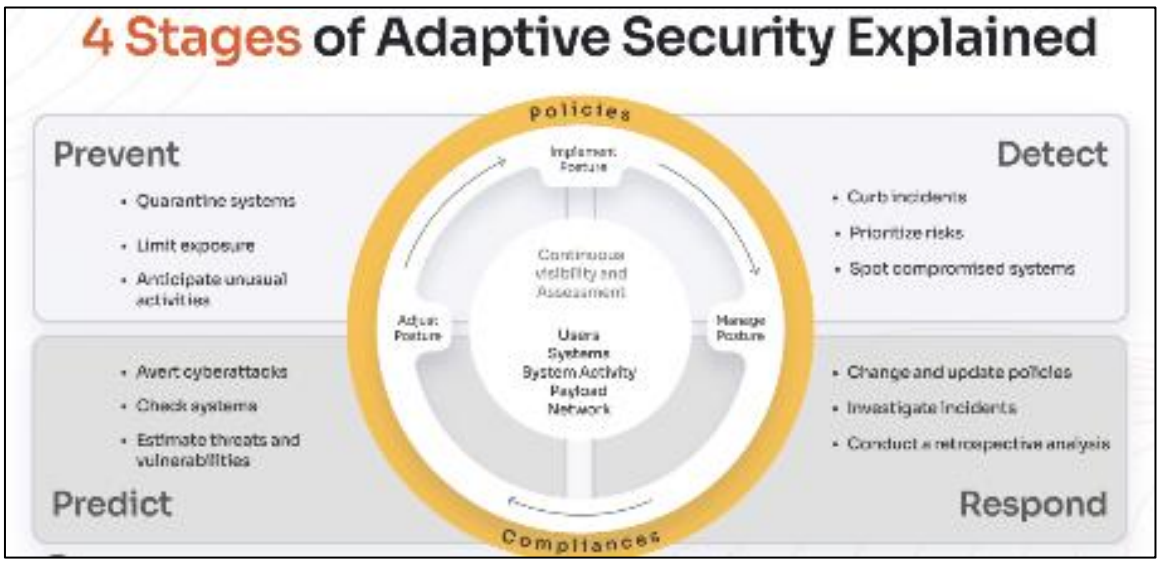

Figure 1 4 Stages of Adaptive Security Explained

Finally, within the Respond phase, machine learning enables automation of incident triage and root cause analysis. Clustering algorithms will enable event correlation; whereas Explainable AI (XAI) techniques will provide transparency

to satisfy regulatory requirements; finally, policy engines will be updated with model feedback to create an adaptive, closed loop system.

Ultimately, what this truly means is that machine learning turns traditional security into an evolving defense mechanism. In addition to employing predictive analytics, anomaly detection, behavior-based profiling and automated responses to attacks, adaptive security systems can become resilient to advanced, AI-powered cyber threats; as well as remain compliant with regulations and efficient with operations in a financial environment.

2.2. Dual-Agent Frameworks

Recent developments have included the development of two different types of Artificial Intelligence (AI) agents that can be used to process different types of temporal data. The first is a dual-agent authentication framework which includes a Long-Term Memory (LTM) agent for tracking past behavior and an STM (Short Term Memory) agent for real-time contextual processing [1]. In testing this architecture, it was found that there were .4955 fraud detections in the initial assessment phase, while the false positives were limited to .0943 [1] and decision processing times averaged less than one millisecond (.000012s) [1].

2.3. Behavioral Biometrics

Continuous, passive authentication through behavioral biometrics has been gaining popularity in recent years. Studies have shown that by monitoring micro-patterns (keystroke dynamics, touchscreen swipe speed, gyroscope/accelerometer data) systems can continuously authenticate the user without any user action [6] [7].

3. Proposed AI-Driven Adaptive Authentication Architecture

For us to create a seamless financial experience, while maintaining the highest level of security, the paper proposes an A2FA multi-layered model based upon the concept of Zero Trust ("never trust, always verify") [8].

The architecture comprises three primary tiers:

3.1. Signal Ingestion and Data Collection Layer

This layer passively collects data points during the user's session without interrupting the user journey. The signals are categorized into:

- **Contextual Signals:** IP address, geolocation, network type (VPN, public Wi-Fi), and time of access.
- **Device Telemetry:** Device fingerprinting (OS, browser version, hardware IDs), jailbreak/rooting status, and malware detection.
- **Behavioral Biometrics:** Typing cadence, mouse fluidity, swipe trajectory, and device angle [7].

3.2. AI/ML Risk Scoring Engine

Data from transactions are used to feed an AI-based risk engine. Based on the use of historical data baselines and in real-time, anomaly-detection capabilities, the machine learning algorithms produce a probabilistic risk score based on the likelihood that a transaction will result in a loss.

Define the risk score R for a given transaction X as follows:

$$R(X) = \sum_{i=1}^{N} W_i F_i(X) + \alpha \cdot P(A|X)$$

The dynamic weight W_i of each of the features $F_i(X)$ is represented with respect to the transaction; α is an industry-specific risk tolerance factor that is applied to the probability of an anomaly being detected by a deep neural network; and P(A|X), or the probability that an anomaly exists in the transaction, is determined by a deep neural network [9].

3.3. Dynamic Orchestration and Decision Layer

Adaptive Authentication's dynamic orchestration & decisions layer is the core enforcement of the framework. After the AI-based Risk Scoring Engine generates a Probabilistic Risk Score for an individual transaction or session, the Dynamic Orchestration & Decisions Layer will generate a context-aware security action based on the generated risk score.

Unlike traditional authentication methods where all users must go through the same authentication process, the Access Control Server (ACS), by using Real-Time logic, determines the proper security posture for each user. As a result, the security controls applied to protect the users will always be proportional to the threat level Assessed at the time of transaction/session while allowing the legitimate users to use their systems without unnecessary complexity.

Typically, the orchestration logic uses pre-defined risk thresholds which are aligned to the organization's risk appetite, regulatory mandates, and fraud tolerance levels. These thresholds are not fixed; they can be continuously adjusted via feedback loops generated from fraud outcomes, false positive rates, and continuous updates to the threat intelligence feeds.

Prior to making the final Policy Decision, the ACS reviews various contextual signals including, but not limited to: device fingerprint consistency, geolocation velocity, behavioral biometric stability, and transaction value sensitivity [10].

3.3.1. Frictionless - Lower Risk:

The transaction will be identified as low risk when the calculated risk score drops below a previously defined, lower risk threshold. This classification removes the need for users to receive explicit, secondary authentication prompts. Device Continuity, Historical Behavioral Alignment and Trusted Network Attributes are examples of passive signals that indicate legitimacy and are considered sufficient for legitimate users. The Frictionless method enhances the user's overall experience with respect to authentication, by reducing the number of interruptions during the normal course of activity. An operational benefit of the frictionless method is reduced OTP delivery costs, reduced authentication latency and fewer help desk escalation calls resulting from failed logins. Background, continuous monitoring is always active, even while the application is operating in a frictionless mode, so that sudden changes in behavior may prompt a mid-session re-assessment if necessary.

3.3.2. Step-Up 2FA - Moderate Risk:

A step-up authentication challenge will be initiated by the ACS when a risk score is greater than the low-risk threshold; however, it is not high enough to meet the definition for critical risk. Secondary verification may consist of: SMS-based One-Time Passwords (OTPs). Secure mobile app-based approvals with push notifications. Hardware tokens, Biometric authentication such as facial recognition or fingerprint scanning

The selection of the factor(s) used for secondary verification may also be adaptive, i.e., may depend upon the perceived reliability of the context in which the request was made. For instance, if there are indicators that SIM-swapping is occurring; then the use of SMS OTP will likely be bypassed and an app-based, cryptographically authenticated, push notification will be required instead. Step-up 2FA methods provide a balance between providing assurance of security while at the same time minimizing the inconvenience to users; thereby validating anomalous yet potential legitimate behavior before denying access.

3.3.3. Block/Review - High Risk:

Dynamic Orchestration and Decision Layer is where zero trust is put into practice by continually assessing the validity of identities and contexts and enforcing them based on the level of risk, the level of risk being determined by the previous layers. The risk layer dynamically scores and validates each potential threat to an account through its continuous monitoring of behavior in conjunction with the static information gathered from the data layer. If the risk exceeds a predefined threshold, then it triggers a "High Risk" classification for that activity. Upon receipt of this signal, the ACS immediately takes corrective measures i.e. blocks access to requested resources, terminates the user's session, or routes the transaction to a fraud operations team for review. A "High Risk" trigger is generally an indication of a potentially fraudulent or malicious transaction; however, some examples of high-risk triggers may include an "impossible travel scenario," significant changes in a user’s behavior, indicators of a compromised device, and/or a large value transaction that does not follow the user's historical patterns. When a high-risk trigger is identified, automated case creation, event logging and audit trail generation occur to ensure that there is a complete record for both compliance purposes and for use in forensic analysis.

4. Core AI Technologies Enabling A2FA

The efficacy of adaptive authentication is contingent upon the accuracy and speed of its underlying AI technologies.

4.1. Behavioral Biometrics

Behavioral biometric traits unlike physical biometric traits that measure what a user is, behavioral biometric traits measure how a user behaves given that these traits are governed by subconscious cognitive and neuromuscular functions, malicious actors would find it extremely difficult to replicate them.

- K**eystroke Dynamics:** Measures flight time (time between key presses) and dwell time (duration a key is pressed).
- K**inesthetic Attributes:** Measures the dominant hand used in performing actions on devices, the pressure applied to a touch screen of a device, and the angle at which a mobile device is held.
- C**ognitive Pauses:** Measures hesitation or automated "copy-paste" actions indicative of a bot or fraudster consulting stolen credentials.

4.2. Contextual and Spatio-Temporal Analysis

AI Models can easily find the anomalies that represent impossible travel and contextual deviations by using machine learning algorithms. If a customer logs into their online bank account from New York, and then a few minutes later initiates a transaction from an IP address in Tokyo, the AI Model instantly identifies the physical impossibility of this speed [8].

4.3. Continuous Authentication

Conventional 2-Factor authentication (2FA), only assesses the risk at the time of login. AI-based authentication systems allow continuous authentication throughout the session to continually update the risk profile. If an attacker were to hijack a session after login with a remote access trojan (RAT), or if they were to steal the session cookie, the drastic change in the behavioral biometrics would cause a real time session lock [11].

5. Empirical Evaluation and Performance Metrics

Evaluating the effectiveness of A2FA mechanisms requires analyzing both security efficacy and user experience improvements.

5.1. Security Metrics

The primary metrics for assessing biometric and AI authentication models are the False Acceptance Rate (FAR) and False Rejection Rate (FRR).

$$FAR = \frac{FP}{FP + TN}$$

$$FRR = \frac{FN}{FN + TP}$$

The amount of false positives (FP) and true negatives (TN), false negatives (FN) and true positives (TP) [12]. The most recent applications of adaptive machine learning (ML) have shown that they can reduce false accept rates (FAR) by up to 27 percent and false reject rates (FRR) by up to 35 percent when compared with non-adaptive (static) systems [5]. Therefore it is clear that this system is able to successfully block malicious individuals from accessing the system while correctly identifying legitimate users as their habits change over time.

5.2. User Experience and Operational Efficiency

By reserving high-friction challenges exclusively for anomalous transactions, financial institutions can authorize approximately 90% of logins seamlessly [3].

Table 1 Static MFA vs. AI-Enhanced Adaptive MFA

Feature	Static MFA	AI-Enhanced Adaptive MFA
Authentication Trigger	Every login/transaction	Based on real-time risk score
User Friction	High (constant interruptions)	Low (frictionless for trusted profiles)
Authentication Type	Point-of-entry only	Continuous / Session-long
Context Awareness	None	High (Device, IP, Velocity, Behavior)
Response to Deepfakes/Bots	Vulnerable (if OTP is intercepted)	Highly resilient (detects non-human patterns)

Furthermore, A2FA dramatically lowers operational costs. By minimizing unnecessary SMS OTP transmissions and reducing the burden on IT helpdesks for password resets or locked accounts, institutions achieve significant cost savings alongside heightened security [13].

Table 2 Performance Impacts of A2FA Implementation [1], [5]

Metric	Industry Average (Static)	AI-Adaptive Architecture (Observed)
Fraud Detection Rate	~35.0%	50.95% (at initial assessment)
False Positive Rate	>15.0%	9.43%
Processing Latency	>1.0s	0.000012s (Sub-millisecond)
Transaction Abandonment	~73%	Reduced by 47.36%

6. Challenges and Future Directions

Despite the profound benefits, deploying AI-driven A2FA in financial services introduces several critical challenges that warrant future research.

6.1. Regulatory Compliance and Data Privacy

Granular behavioral and biometric data ingestion is intersecting with strict global data privacy regulations such as the European Union's GDPR and the California CCPA [14] in order for financial institutions to develop privacy preserving AI models. The raw, identifiable telemetry from which behavior data was derived could be converted into a mathematical cryptographic hash instead of being stored directly [15].

6.2. Adversarial AI and Evasion Tactics

As defensive artificial intelligence capabilities increase in sophistication, so will threat actor offensive cyber capabilities. With the use of Generative Artificial Intelligence and automated scripting, threat actors are using more sophisticated methods for simulating the behavior of a "human" [5]. Therefore, future adaptive systems must utilize adversarial machine learning to train their models against sophisticated AI generated behaviors.

6.3. Algorithmic Bias

Biases exist in machine learning models due to the nature of their training datasets. A model that is limited to a single demographic when being developed will likely be biased against users with different physical attributes or who interact with devices in a manner that is different from most users. Therefore, an ongoing process of auditing algorithms will need to occur to ensure equitable financial opportunities are available to all.

7. Conclusion

The inclusion of artificial intelligence (AI) with adaptive two-factor authentication represents an important improvement in the way financial organizations protect their customers' information using cybersecurity. In contrast to traditional fixed, "one size fits all" security systems that do not take individual differences into account when providing security, A2FA uses machine learning (ML), context-based data collection, and behavioral-based biometric identifiers to provide a continuously changing zero-trust based digital environment around users [16]. The proposed

two-agents and continuous authentication models clearly show how A2FA can both improve fraud detection and lower both the friction to use the service and the number of abandoned transactions. As financial organizations move forward through increasingly complex regulatory environments and more sophisticated adversary attacks, AI-enabled adaptive authentication will be the foundation upon which the next generation of secure digital banking will be built.

References

[1] Mittal, Akshay & Govindaraj, Sabarinathan. (2025). Adaptive Dual-Agent Authentication Framework: Balancing Security and user Experience in Digital Banking. 1-6. 10.1109/ICCST63435.2025.11293952.

[2] Podapati, Vyoma Harshitha & Nigam, Divyansh. (2025). SoK: A Systematic Review of Context-and Behavior-Aware Adaptive Authentication in Mobile Environments. 10.2139/ssrn.5333334.

[3] F. Alaca and P. van Oorschot, "Device fingerprinting for augmenting web authentication: Classification and analysis of methods," in ACSAC'16. ACM, 2016. *(PDF) Exploring Device Fingerprinting for Password-Less Authentication Systems*.

[4] Mondal, Soumik & Bours, Patrick. (2016). A study on Continuous Authentication using a combination of Keystroke and Mouse Biometrics. Neurocomputing. 230. 10.1016/j.neucom.2016.11.031.

[5] Wiefling, Stephan & Lo Iacono, Luigi & Dürmuth, Markus. (2019). Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. 10.1007/978-3-030-22312-0_10.

[6] Sommer, Robin & Paxson, Vern. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. Proceedings - IEEE Symposium on Security and Privacy. 305-316. 10.1109/SP.2010.25.

[7] Frank, Mario & Biedert, Ralf & Ma, Eugene & Martinovic, Ivan & Song, Dawn. (2012). Touchalytics: On the Applicability of Touchscreen Input as a Behavioral

[8] Biometric for Continuous Authentication. IEEE Transactions on Information Forensics and Security. 8. 10.1109/TIFS.2012.2225048.

[9] Feng, Tao & Liu, Ziyi & Kwon, Kyeongan & Shi, Weidong & Carbunar, Bogdan & Jiang, Yifei & Nguyen, Nhung. (2012). Continuous mobile authentication using touchscreen gestures. 2012 IEEE International Conference on Technologies for Homeland Security, HST 2012. 451-456. 10.1109/THS.2012.6459891.

[10] E.W.T. Ngai, Yong Hu, Y.H. Wong, Yijun Chen, Xin Sun, The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature, Decision Support Systems, Volume 50, Issue 3, 2011, Pages 559-569, ISSN 0167-9236, *https://doi.org/10.1016/j.dss.2010.08.006*. (*https://www.sciencedirect.com/science/article/pii/S0167923610001302*)

[11] Rose, S. , Borchert, O. , Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-207, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420 (Accessed March 13, 2026)

[12] Mihajlov, Martin & Jerman, Borka. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. Interacting with Computers. 23. 582-593. 10.1016/j.intcom.2011.09.001.

[13] Teh, Pin Shen & Teoh, Andrew & Yue, Shigang. (2013). A Survey of Keystroke Dynamics Biometrics. TheScientificWorldJournal. 2013. 408280. 10.1155/2013/408280.

[14] Hazratifard M, Gebali F, Mamun M. Using Machine Learning for Dynamic Authentication in Telehealth: A Tutorial. Sensors (Basel). 2022 Oct 9;22(19):7655. doi: 10.3390/s22197655. PMID: 36236752; PMCID: PMC9572725.

[15] Egelman, Serge & Jain, Sakshi & Portnoff, Rebecca & Liao, Kerwell & Consolvo, Sunny & Wagner, David. (2014). Are you ready to lock? Understanding user motivations for smartphone locking behaviors. Proceedings of the ACM Conference on Computer and Communications Security. 750-761. 10.1145/2660267.2660273.

[16] Frank Stajano and Paul Wilson. 2011. Understanding scam victims: seven principles for systems security. Commun. ACM 54, 3 (March 2011), 70–75. *https://doi.org/10.1145/1897852.1897872*

[17] Bonneau, J., Herley, C., Oorschot, P.C., & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *2012 IEEE Symposium on Security and Privacy*, 553-567.