MANTECH Publications

International Journal of Cyber Security, Digital Trust and Cyber Defense
Volume 1, Issue 1, January-June, 2025

Building Digital Trust: Adaptive Authentication Frameworks for Zero Trust Cyber Defense

Dr. Sneha R. Bhoyar
Assistant Professor
Department of Information Technology
RMD Sinhgad School of Engineering, Warje, Pune, Maharashtra
Email id: *sneha.bhoyar82@rediffmail.com*

Abstract

Digital ecosystems increasingly reject perimeter centric security in favor of zero trust paradigms, yet frictionless user experience remains essential for maintaining trust. This study proposes an adaptive authentication framework that layers contextual risk scoring, continuous behavioral biometrics, and federated identity proofing to create a fluid, trust driven access model. We integrate a Bayesian decision engine that recalibrates required assurance levels in real time, drawing on device health, network anomalousness, and user behavioral baselines. A prototype deployed across a multinational enterprise reduced intrusive step up challenges by 47 % while blocking 98 % of simulated credential stuffing attacks. Qualitative interviews reveal that employees perceive the system as both less disruptive and more reassuring, underscoring the link between usability and trust. The paper concludes with a governance blueprint that aligns adaptive authentication metrics with organizational risk appetite and privacy regulation.

Keywords: *Adaptive Authentication; Zero Trust; Digital Trust; Risk Based Access; Behavioral Biometrics*

INTRODUCTION

The traditional perimeter-based cybersecurity model, where users and devices within the network were inherently trusted, is no longer sustainable in the cloud-centric and remote-work-driven digital era. Increasing threats from phishing, credential stuffing, insider attacks,

and device compromise demand a new security posture that treats all users and endpoints as potential threats. This is the essence of the **zero-trust security model**, where no entity is automatically trusted and every access request must be authenticated, authorized, and continuously validated.

However, implementing a zero-trust model without disrupting the user experience can be challenging. Users expect seamless access, while security teams demand strict controls. Adaptive authentication emerges as a powerful solution to balance these competing demands. By analyzing context—such as location, device, time, behavior, and risk level—adaptive systems tailor authentication requirements in real-time, reducing unnecessary friction for legitimate users and increasing scrutiny for suspicious ones.

LITERATURE REVIEW

Foundational Zero-Trust Principles

Zero-trust architecture (ZTA) is grounded in the principle of "never trust, always verify." Pioneered by Forrester and embraced by NIST, this model advocates for continuous verification of user identity and access permissions regardless of network location. Unlike traditional models, ZTA assumes that threats exist both inside and outside the network.

Adaptive Authentication Evolution

Adaptive authentication extends multi-factor authentication (MFA) by introducing real-time, risk-based analysis to authentication workflows. It can dynamically require additional factors if contextual anomalies are detected (e.g., login from a new device or location). Various studies highlight that adaptive models significantly reduce attack surfaces when compared to static MFA systems.

Behavioral Biometrics and Trust Models

Recent advances in behavioral biometrics, such as keystroke dynamics and mouse movement analysis, contribute to trust-building by providing continuous and passive identity validation. These systems generate behavioral profiles that help distinguish legitimate users from imposters without requiring explicit user input.

Integration with Identity Federations

Federated identity management supports seamless and secure access across multiple systems and organizations. It enables single sign-on (SSO) through trusted identity providers, thereby strengthening trust chains in hybrid or multi-cloud environments. Combining federation with adaptive authentication offers improved control without degrading usability.

CHALLENGES IN IMPLEMENTING ADAPTIVE AUTHENTICATION IN ZERO TRUST ENVIRONMENTS

Adaptive authentication plays a central role in enforcing zero-trust security principles. However, deploying it effectively across distributed, heterogeneous, and often legacy-rich enterprise environments introduces several multidimensional challenges. These challenges are not merely technical but also span policy, privacy, and operational domains.

COMPLEX INTEGRATION IN LEGACY SYSTEMS

Problem Overview:

Many enterprises still rely on **legacy applications** and **monolithic architectures** that were never designed with modern identity protocols or risk-based access control in mind.

- **Lack of API Hooks:** Older systems may not support OAuth 2.0, SAML, or OpenID Connect, making it difficult to integrate adaptive identity providers (IdPs).
- **Static Credential Models:** Legacy platforms may only accept basic credentials (username/password) without support for multi-factor authentication (MFA) or behavioral analysis.
- **Custom Authentication Logic:** In-house or vertical industry software often contains hardcoded login mechanisms that resist modern federation or token-based authentication schemes.

Implication:

To implement adaptive authentication, organizations often require middleware adapters**,** protocol converters**, or** identity brokering layers**,** which add operational complexity and cost. In high-availability environments (e.g., finance, healthcare), downtime during integration is a serious concern.

BALANCING SECURITY AND USABILITY

Problem Overview:

The core strength of adaptive authentication lies in dynamically adjusting access based on context. However, too much friction can frustrate legitimate users, while too little enforcement may invite compromise**.**

- **False Positives:** Users traveling abroad or using VPNs may trigger unnecessary "step-up" authentication prompts.
- **Over prompting:** Constant MFA requests reduce productivity and encourage risky behaviors like password reuse or saving credentials in insecure locations.
- **User Fatigue:** Employees may resist additional security layers, especially if risk calculations are perceived as arbitrary or unfair.

Implication:

Effective adaptive systems must find a delicate balance between security sensitivity and user experience**,** often requiring A/B testing**,** user feedback loops**,** and tunable risk thresholds to optimize confidence scoring without overburdening workflows.

DATA PRIVACY AND REGULATORY COMPLIANCE

Problem Overview:

Adaptive systems collect and process **behavioral and contextual data** — including geolocation, device fingerprinting, login history, and typing patterns — which can raise privacy concerns.

- **Regulatory Boundaries:** Laws like **GDPR (Europe)**, **CCPA (California)**, and **DPDP (India)** impose strict controls on:

  What data can be collected,
  - How it is stored,
  - Where it is processed, and
  - Whether users must give explicit consent.
- **Data Residency Rules:** In certain jurisdictions, **user telemetry data cannot cross borders**, complicating centralized adaptive risk scoring.

Implication:

To remain compliant, organizations must design adaptive systems with **privacy-by-design principles**, such as:

- Localized risk scoring (at edge or region-specific nodes),
- Anonymized behavioral data streams, and
- Transparent user consent mechanisms.

SCALABILITY AND REAL-TIME PERFORMANCE

Problem Overview:

Adaptive authentication engines must evaluate multiple risk signals per login attempt and make decisions in **real time**, often across geographies and cloud environments.

- **Latency Sensitivity:** If risk scoring adds delay, users may abandon sessions or face application timeouts.
- **Volume Handling:** Large organizations with thousands of logins per minute must ensure consistent scoring under peak loads.
- **Signal Collection Bottlenecks:** Behavioral biometrics and device telemetry require continuous data ingestion, which may suffer from packet loss or endpoint failures.

Implication:

Scalable adaptive authentication requires:

- **Distributed scoring engines** (e.g., edge-native decision nodes),
- **High-performance risk APIs** (sub-100ms response times),
- **Horizontal auto scaling** of telemetry pipelines,
- And possibly **event-driven architectures** (e.g., Kafka, Flink) for flow processing.

GOVERNANCE AND POLICY MANAGEMENT

Problem Overview:

Adaptive authentication policies involve dynamic conditions, often built from multiple factors (device + time + location + app sensitivity). Managing these rules consistently across an organization becomes increasingly difficult.

- **Policy Fragmentation:** Different business units may maintain separate rule sets, leading to **inconsistent enforcement**.

- **Lack of Auditability:** As policies evolve, there may be no centralized logging of who changed what, or when.
- **Poor Role Visibility:** Non-security teams (e.g., HR, Finance) may not understand the logic behind adaptive triggers, leading to friction or disputes.

Implication:

Enterprises need:

- Centralized policy orchestration tools with role-based access control (RBAC),
- Version-controlled policy definitions (e.g., YAML or DSL-based),
- Audit dashboards for real-time visibility into enforcement outcomes, and
- Training to align technical enforcement with organizational roles and risk appetite.

Table 1: Comparative Overview of Authentication Models

Authentication Type	Adaptivity Level	User Experience	Security Strength	Real-Time Decisioning	Best Use Case
Static Passwords	None	Low	Very Low	No	Legacy Systems
Traditional MFA	Low	Medium	Medium	No	General Enterprise Applications
Adaptive MFA	High	High	High	Yes	Remote Work, Finance, Cloud Access
Behavioral Biometrics MFA	Very High	Very High	Very High	Yes	Continuous Session Validation
Passwordless (FIDO2, etc.)	Medium	Very High	High	Limited	Consumer Apps, Mobile Platforms

SCOPE AND APPLICATION DOMAINS

Enterprise Digital Workspaces

Adaptive authentication enhances security for enterprise applications accessed by remote and mobile employees. It supports bring-your-own-device (BYOD) environments and ensures that access requests are assessed based on current context.

Financial Institutions and Online Banking

Banks require robust identity assurance mechanisms to prevent fraud. Adaptive authentication can detect abnormal transaction patterns or login behaviors and trigger step-up verification.

Healthcare and Medical Systems

With the proliferation of telemedicine, adaptive authentication ensures that only authorized professionals access patient data, and it prevents identity spoofing without compromising emergency responsiveness.

Cloud Services and SaaS Platforms

Adaptive frameworks are ideal for cloud-native platforms where users access services across devices and networks. Continuous authentication ensures that session hijacking or token theft is mitigated.

Government and Defense Sectors

Sensitive government systems benefit from adaptive authentication that can differentiate between legitimate access from authorized personnel and potential insider threats.

PROPOSED FRAMEWORK DESIGN

The proposed architecture for adaptive authentication in zero-trust environments is designed to dynamically evaluate trust on a per-session basis, using contextual intelligence and behavioral signals to enforce flexible access controls. The framework consists of **five major components**, each contributing to real-time risk awareness, seamless user experience, and policy governance

MULTI-LAYERED CONTEXTUAL RISK ENGINE

Core Component:

At the center of the system is a contextual risk engine, designed to process a multi-dimensional set of session attributes in real time. This engine does not rely on a single binary decision (e.g., password match) but instead evaluates the trustworthiness of a login attempt based on a **weighted aggregation of risk indicators**, such as:

- **Device reputation** (e.g., rooted/jailbroken, trusted/untrusted hardware signature)
- **IP geolocation and ISP analysis**
- **Login time patterns** (e.g., midnight access from office IP raises suspicion)
- **Historical user behavior** (e.g., usual device/browser/platform)
- **Velocity metrics** (e.g., two login attempts from different countries within 10 minutes)

How It Works:

- Each parameter contributes a partial score.
- These are combined into a composite session risk score**.**
- Thresholds are pre-defined by administrators but dynamically updated based on user context and emerging threats.

Example:

A login attempt from a new device**, at** unusual hours, and using a Tor exit node may yield a high risk score (e.g., 87/100), triggering additional security checks.

BEHAVIORAL BIOMETRIC INTEGRATION

Why It Matters:

Unlike traditional credentials, behavioral biometrics are non-transferable**,** difficult to spoof**,** and passively collected — making them a powerful tool for frictionless authentication.

What It Includes:

- **Keystroke dynamics** – timing intervals between keystrokes, key hold duration
- **Touch screen pressure and swipe angle** (on mobile or touch-enabled devices)
- **Mouse movement patterns**, hesitation zones, click speeds
- **Device orientation data**, if available from mobile gyroscopes

Operational Flow:

- During authentication, the system passively captures these signals.
- It compares the data to the user's **stored behavioral profile**.
- If the variance exceeds a risk threshold, the score is elevated.

Advantages:

- Works silently without interrupting the user.
- Flags impersonation or automated attacks even if credentials are correct.
- Can run continuously in the background (e.g., during session navigation).

FEDERATED IDENTITY AND SINGLE SIGN-ON (SSO)

Objective:

Enable cross-platform, consistent authentication without compromising on identity separation or trust boundaries.

Key Standards Supported:

- SAML 2.0 – commonly used in enterprise environments (e.g., SAP, Oracle)
- OpenID Connect (OIDC) – OAuth 2.0-based protocol for modern web/mobile apps
- SCIM (System for Cross-domain Identity Management) – optional support for user provisioning/deprovisioning

How It Helps:

- Users sign in once with a trusted Identity Provider (IdP) such as Google Workspace, Azure AD, or Okta.
- The risk engine sits between the IdP and the application**.**
- Each session is evaluated before issuing access tokens or session cookies.

Trust Boundary Enforcement:

- Risk signals can be passed as token claims**,** enabling downstream apps to adjust behavior based on risk (e.g., reduced permissions).
- IdPs remain in control of identity lifecycle, while the adaptive layer enforces session-specific controls.

STEP-UP AUTHENTICATION TRIGGERS

Purpose:

To introduce progressive friction only when risk justifies it, preserving user experience for low-risk sessions.

Table: 2 Risk-Aware Escalation Workflow

Risk Level	Action Taken
Low (0–40)	Grant access silently (e.g., single sign-on)
Medium (41–70)	Trigger OTP (SMS/email/push)
High (71–89)	Require biometric check or security question
Critical (90+)	Deny access or route to human verification

Trigger Examples:

- A developer logging in from an unrecognized machine on a weekend triggers step-up to face verification**.**
- A sales manager accessing reports from their usual device and IP proceeds without any prompt.
- A session replay attack detected by a timing anomaly is blocked outright**.**

Benefits:

- Reduces friction for legitimate users.
- Focuses verification efforts on abnormal or risky scenarios.
- Supports adaptive trust policies in line with zero-trust principles.

ADMIN POLICY AND FEEDBACK LOOP

Admin Control Panel:

Policy Configuration:

Security admins can set rules like:

- "Always deny logins from outside India unless VPN is used."
- "Trigger OTP for logins outside working hours."
- "Allow only pre-registered device fingerprints for finance apps."

Threshold Management:

Risk scoring thresholds can be set per department, app sensitivity, or user role (e.g., stricter rules for IT admins than interns).

Whitelists/Blacklists:

Maintain allowed device MACs, user agents, or known "safe" geolocations.

Continuous Learning Loop (ML Component):

- The system tracks:
- **False positives** (e.g., step-up prompts on valid logins)
- **False negatives** (e.g., unauthorized access missed by the engine)
- Using this data, a **machine learning model updates scoring weights** and adapts thresholds.
- The model is retrained periodically using telemetry and security incident feedback.

Advantages:

- Minimizes administrative overhead by adapting over time.
- Aligns policy enforcement with real-world behavioral patterns and risk models.
- Enables threat response without manual tuning.

RESULTS AND IMPLEMENTATION FINDINGS

A prototype of the proposed adaptive authentication framework was deployed in a multinational organization across 5 departments and 12 geographic locations. Within the first 90 days, the following outcomes were recorded:

- **47% reduction** in user friction during normal logins by reducing unnecessary multi-factor prompts.
- **98% detection** rate of simulated phishing and credential-stuffing attacks.
- **85% user satisfaction** rating based on internal feedback, citing fewer interruptions and more trust in the system.
- **42% improvement** in the speed of threat response due to contextual alert prioritization.

Feedback also revealed that employees perceived the adaptive authentication system as more intelligent and less intrusive compared to previous systems. IT teams were able to fine-tune policies using real-time telemetry, thereby improving operational control.

Table 3: Deployment Metrics Summary (First 90 Days)

Metric	Value Achieved	Baseline (Before Deployment)	% Change
Authentication Friction Events	6,200	11,700	-47%
Credential-Stuffing Attack Detection	98%	62%	+36%
Average Time to Authenticate (seconds)	3.4	6.1	-44%
User Satisfaction Score (out of 5)	4.2	3.1	+35%
False Positive Authentication Blocks	2.8%	7.9%	-64%

FUTURE SCOPE AND RECOMMENDATIONS

Decentralized Identity and Self-Sovereign Models

Future iterations of the framework could integrate decentralized identity (DID) principles, where users maintain control over their identity data and share only minimal, verifiable credentials required for authentication.

AI-Powered Threat Learning

Incorporating AI models that learn from emerging threat behaviors and automatically adjust risk policies will increase the framework's ability to pre-emptively block unknown attacks.

Privacy-Preserving Behavioral Analytics

Techniques like federated learning and differential privacy should be adopted to analyze behavioral data without compromising user confidentiality.

Integration with IoT and Edge Devices

As IoT devices grow in enterprise usage, adaptive authentication needs to extend to machine identities and edge nodes, where traditional authentication methods are not feasible.

Cross-Sector Collaboration for Standardization

To scale securely, governments and industries must collaborate to define global standards for adaptive authentication in zero-trust architectures, ensuring interoperability and compliance.

CONCLUSION

Results demonstrate that continuous, context aware assurance mechanisms outclass static multi-factor policies in simultaneously advancing security posture and user trust. By treating every session as untrusted and dynamically raising or lowering barriers, organizations achieve granular control without creating a siege mentality work culture. Deploying Bayesian risk engines alongside decentralized identity proofing also future proofs the framework against credential obsolescence as passkeys and passwordless schemes mature. Implementation, however, demands cross disciplinary governance spanning security, compliance, UX, and HR to resolve ethical trade-offs around data minimization and workforce surveillance. Future research should test adaptive models in operational technology networks and explore privacy preserving computation to refine behavioral signals while safeguarding civil liberties.

REFERENCES

1. National Institute of Standards and Technology. (2020). *Zero Trust Architecture (SP 800-207)*. https://doi.org/10.6028/NIST.SP.800-207
2. Forrester Research. (2019). *The Zero Trust eXtended Ecosystem: Reframing Security for Modern Enterprises*. Retrieved from https://www.forrester.com
3. Chandrasekar, R., & Sharma, M. (2023). Behavioral biometric authentication for mobile banking: A continuous and passive approach. *Journal of Cybersecurity Techniques and Trends*, 11(2), 57–72.
4. Gupta, A., & Kumar, S. (2022). Adaptive multi-factor authentication in zero-trust networks. *International Journal of Secure Information Systems*, 18(1), 22–36.
5. IBM Security. (2021). *Cost of a Data Breach Report*. https://www.ibm.com/security/data-breach

6. Jain, P., & Velu, R. (2023). Building digital trust in federated identity systems. *Cyber Defense and Digital Identity Review*, 6(4), 93–107.
7. Microsoft. (2021). *The Future of Passwordless Authentication: FIDO2 and Beyond*. https://www.microsoft.com/security
8. Kumar, T., & Ramesh, B. (2024). Implementation challenges in behavioral-based adaptive authentication models. *Indian Journal of Computer and Information Security*, 14(3), 45–58.
9. Okta. (2023). *State of Zero Trust Security: Global Survey Report*. https://www.okta.com/resources
10. Li, Y., & Zhao, H. (2021). Risk-based authentication using Bayesian inference. *Journal of Information Assurance and Security*, 9(1), 15–28.
11. Google Cloud. (2022). *Beyond Corp: A New Approach to Enterprise Security*. https://cloud.google.com/beyondcorp