International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 5, Sep-Oct-2026, ISSN (Online): 2395-566X

Adaptive Trust-Based Continuous Authentication Framework Using Risk Aware Zero Trust Architecture

Atharv Sharma
Department of Computer Science Engineering Himachal Pradesh University
University Institute of Technology (UIT)

Abstract- In this paper, we propose Adaptive Trust-Based Continuous Authentication Framework (ATCAF), a lightweight architecture to extend Zero Trust principles with continuous risk aware authentication. The proposed framework does not make a single authentication decision at login but continuously calculates a dynamic trust score by combining multiple contextual security indicators such as device trust, behavioral consistency, location confidence, network reputation and historical user reputation. Access decisions are made in real-time based on the continuously evolving trust score, enabling adaptive responses such as seamless access, step-up multi-factor authentication, privilege reduction or session termination. The paper describes the system architecture, mathematical trust model, continuous evaluation workflow, implementation methodology, public evaluation datasets, security analysis and experimental design to evaluate authentication accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), trust score stability and response latency . The framework we propose aims at improving identity security, while maintaining usability and reducing unnecessary authentication interruptions.

Keywords- Continuous Authentication, Zero Trust Architecture, Risk-Based Authentication, Identity Security, Behavioral Biometrics, Device Fingerprinting, Adaptive Trust, Cybersecurity, Authentication Framework, Access Control.

I. INTRODUCTION

According to the recent cyber security reports, identity-based attacks are one of the fastest growing types of security incidents. Attackers are increasingly targeting authentication systems themselves rather than exploiting vulnerabilities in software. Techniques include credential phishing, password spraying, social engineering, token theft, session hijacking, malicious browser extensions, insider threats and adversary-in-the-middle attacks. Most authentication systems only check authentication during the creation of a session. If the credentials are valid, they usually allow unfettered access to the system.

The fundamental problem of existing authentication system is that they have a binary decision model. Authentication is often depicted as a simple yes-no decision:

This mismatch reveals an important limitation of traditional authentication mechanisms: a successful login does not imply continued trustworthiness throughout an active session.
This is increasingly recognized by modern cyber security frameworks. The Zero Trust Architecture (ZTA) proposed by National Institute of Standards and Technology (NIST) states that no user, device, application or network should be trusted by default, even if located inside an organization's network boundary [1]. Access requests should, however, be continuously verified based on multiple contextual factors. Zero Trust greatly enhances an organization's security posture, but most practical implementations still rely on periodic authentication checks and static policy evaluation, rather than continuous trust adjustment as environmental conditions change.

This research argues that authentication is not a single event, but a continuous decision making process, evolving along the lifetime of a user session. Thus, instead of asking, "Is this user authenticated?", current security systems must be asking, "How much should this session be trusted at this particular moment?"

To address this, this paper proposes the Adaptive Trust-Based Continuous Authentication Framework (ATCAF), a modular and lightweight architecture that computes a dynamic trust score continuously based on various contextual security indicators.

The proposed framework enables improved security without significantly degrading user experience by allowing seamless authentication during trusted sessions and automatically increasing verification requirements as risk levels change.

II. LITERATURE REVIEW

Zero Trust Architecture has significantly influenced modern authentication security. Rose et al. introduced the NIST Zero Trust Architecture framework based on continuous verification and least-privilege access [1]. Freeman et al. proposed a statistical approach to measuring user authenticity using contextual signals for risk-based authentication [2]. Patel et al. reviewed continuous user authentication methods and highlighted behavioral signals for ongoing identity verification [3]. Killourhy and Maxion evaluated anomaly-detection algorithms for keystroke dynamics, demonstrating the potential of behavioral patterns for authentication [4]. Eckersley investigated browser fingerprinting as a method for identifying devices based on browser characteristics [5]. However, existing approaches primarily address individual aspects of authentication, while few works combine behavioral, device, location, network, and historical factors into a unified adaptive trust model for continuous session-level authentication, presenting the research gap that this paper addresses.

III. RESEARCH CONTRIBUTIONS

The main contributions of this work can be summarized as follows:

1. An Adaptive Trust-based Continuous Authentication Framework (ATCAF) to augment Zero Trust principles by continuous session-level trust evaluation.
2. A unified mathematical trust model which combines device trust, behavioral consistency, location confidence, network reputation and historical user reputation into a dynamic trust score.
3. A lightweight modular architecture for real-time trust recalculation that does not require modifications of the current authentication protocols such as OAuth 2.0 [8], OpenID Connect (OIDC) [9] or SAML [10].
4. A continuous decision engine that can dynamically modify the authentication requirements through seamless access, step-up multi-factor authentication, privilege reduction or session termination based on evolving trust conditions.
5. An implementation-oriented framework for compatibility with modern cloud-native enterprise environments, while preserving explainability, scalability and low computational overhead.

IV. PROPOSED METHODOLOGY

A. System Overview

The goal is not to eliminate authentication, but to dynamically adjust the trust level to the changing security context.

ATCAF combines multiple independent contextual cues into a unified trust model. These indicators are:

- Identity verification
- Device trust
- Behavioral consistency
- Network reputation
- Location confidence
- Historical user reputation

B. Overall System Architecture

The proposed framework is composed of 7 main components that work sequentially during authentication and in a continuous information exchange during active session.

C. System Components

1. Identity Verification Module

Identity verification determines the initial identity of the user prior to the continuous trust evaluation.

The framework supports the following existing enterprise authentication mechanisms:

- Password Authentication
- Multi-Factor Authentication (MFA)

- Passkeys
- OAuth 2.0 [8]
- OpenID Connect (OIDC) [9]
- SAML [10]
- FIDO2 [11]

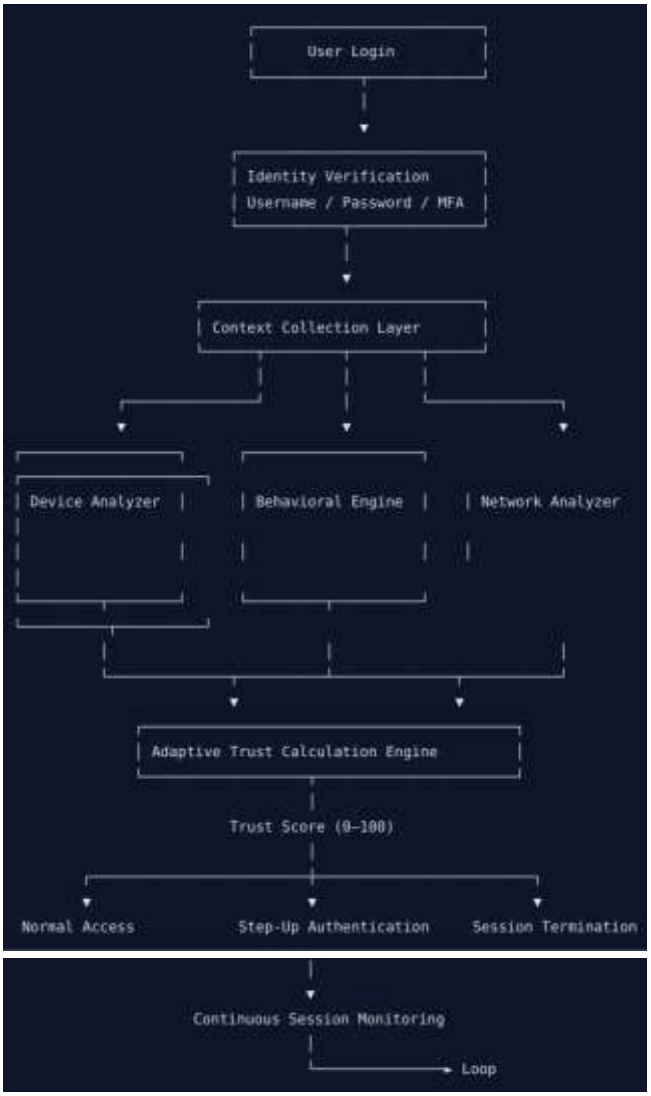

Figure 1. Overall architecture of the proposed Adaptive Trust-Based Continuous Authentication Framework (ATCAF).

Unlike traditional authentication systems, successful identity verification does not imply permanent trust. Instead, it initializes the trust model with a default trust value.

Device Trust Module

The Device Trust Module checks whether the device accessing is a trusted device that has been seen before.

Example features include:

- Device Identifier
- Operating System
- Browser Version
- Screen Resolution
- Trusted Hardware
- TPM Availability
- Secure Boot Status
- Browser Fingerprint
- Device Certificate

The module computes a normalized device trust value: $0 \leq D \leq 1$

where

$D = 1$ represents a fully trusted device.

$D = 0$ represents an unknown or suspicious device.

Behavioral Analysis Engine

Behavioral Consistency measures the similarity between current user interaction and past behavioral patterns.

Observed features include:

- Typing speed
- Typing rhythm
- Mouse movement trajectory
- Scroll behavior
- Window switching frequency
- Interaction timing
- Session navigation patterns Behavioral similarity is represented as: $0 \leq B \leq 1$

where higher values indicate greater similarity to the legitimate user's historical behavior.

Behavioral evaluation, compared to biometric authentication, is passive and does not interrupt the user.

Network Reputation Module

The Network Reputation Module assesses the security characteristics of the network to which the user is connecting.

Indicators include:

- IP reputation
- ASN reputation
- VPN usage
- TOR exit node detection
- Proxy detection
- Historical abuse reports

- Country risk level Network trust is defined as $0 \leq N \leq 1$

A high network reputation increases overall trust, while suspicious infrastructure decreases trust.

Location Confidence Module

The framework does not weight all locations equally, but estimates the likelihood that the current login location is legitimate.

Factors include:

- Historical login locations
- Travel velocity
- Time difference
- GPS consistency
- Device location agreement For example,

	Scenario 1	Scenario 2
Location	Shimla	Russia
Device	Same laptop	Unknown virtual machine
Time	9:00 AM	3:12 AM
Confidence	High Confidence	Very Low Confidence

Location confidence is normalized as $0 \leq L \leq 1$

Historical Reputation Module

Historical reputation summarizes long-term user reliability.

Subject to

$$wD + wB + wL + wN + wH = 1 \; 0 \leq wi \leq 1$$

It includes factors such as:

- Previous successful authentications
- Security incidents
- Password reset frequency
- Account recovery history
- Previous trust scores

Historical reputation evolves gradually over time. $0 \leq H \leq 1$

Unlike short-term contextual indicators, historical reputation change is slow and provides long-term stability to the trust model.

Adaptive Trust Model

The proposed framework treats trust as a continuously evolving numerical quantity rather than a binary authentication decision.

The overall trust score is a weighted amalgamation of contextual indicators:

$$T = wDD + w B + w L + w N + w H$$
$$B \quad L \quad N \quad H$$

Where

T=Overall Trust Score

D=Device Trust

B=Behavioral Consistency

L=Location Confidence

N=Network Reputation

H=Historical Reputation

The weighting factors can be configured according to organizational security requirements. Example Suppose the contextual trust indicators have the following values:

Parameter	Value
Device Trust	0.95
Behavioral Consistency	0.88
Location Confidence	0.91
Network Reputation	0.76
Historical Reputation	0.93

Using the weighting factors : wD = 0.25, wB = 0.25, wL = 0.15, wN = 0.15, wH = 0.20

the resulting trust score is : $T = 0.25(0.95) + 0.25(0.88) + 0.15(0.91) + 0.15(0.76) + 0.20(0.93)$

$= 0.895$

or

$T = 89.5\%$

This indicates a high-trust authentication context, suggesting that the user satisfies the organization's trust requirements.

Adaptive Decision Engine

Instead of binary authentication, access decisions depend on trust intervals.

Trust Score	Decision
90–100	Normal access
70–89	Continue monitoring
40–69	Step-up MFA
Below 40	Terminate session

This enables gradual adaptation instead of abrupt denial.

Continuous Trust Update

As opposed to traditional authentication systems, trust is continuously recalculated during the user session to reflect changes in contextual and behavioral indicators.

At every observation interval, the trust score is updated as

$$T_{t+1} = \alpha T_t + (1 - \alpha) T_{new}$$

where

T_t = Previous trust score

T_{new} = Newly calculated trust score

α = Smoothing coefficient, where $0 < \alpha < 1$

The smoothing coefficient determines how much influence the previous trust score has on the updated value. A higher value of α provides greater stability by reducing the impact of short-term fluctuations, whereas a lower value enables the system to respond more rapidly to significant changes in user behavior.

This exponential smoothing approach prevents sudden trust variations caused by temporary anomalies while allowing the system to adapt to persistent behavioral or contextual changes.

The workflow consists of the following steps:

Risk Score Estimation

While trust represents confidence in user legitimacy, risk estimates the likelihood that the current session has been compromised.

The proposed framework models the overall session risk as

$R = 1 - T$

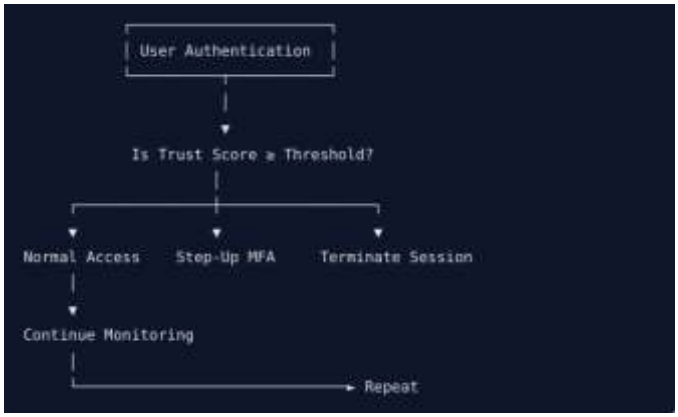

Figure 2. Continuous authentication workflow of the proposed ATCAF framework.

where

R = Session Risk

T = Normalized Trust Score

Since trust and risk are complementary, $0 \leq R \leq 1$

A high trust score naturally produces a low estimated security risk.

STRIDE Threat Model

Threat	Example	ATCAF Mitigation
Spoofing	Credential Theft	Continuous Trust
Tampering	Session Modification	Integrity Verification
Repudiation	Denying Actions	Audit Logs
Information Disclosure	Token Leakage	Dynamic Re-authentication
Denial of Service	Session Flooding	Risk-Based Rate Limiting
Elevation of Privilege	Privilege Escalation	Adaptive Authorization

V. SECURITY ANALYSIS

The proposed framework is designed to strengthen authentication against several common attack vectors by continuously evaluating contextual security information.

A. Credential Theft

In conventional authentication systems, possession of valid credentials often grants unfettered access.

Phishing attacks and password reuse can therefore directly result in account compromise.

In the proposed framework, valid credentials only establish the initial identity. Additional authorizations rely on continuously assessed contextual evidence including familiarity with the device, behavioral consistency and network reputation. So stolen credentials alone are not enough to maintain a highly trusted session.

B. Session Hijacking

Session hijacking is when an attacker hijacks an authenticated session by stealing cookies, access tokens or browser session identifiers.

Traditional authentication mechanisms seldom reevaluate trust once logged in.

ATCAF keeps track of the session's characteristics. If the behavior deviates significantly from the context, the trust score is lowered, and additional authentication may be required or the session may be terminated.

C. Insider Threats

Legitimate privileges can be abused by authorized users, whether maliciously or inadvertently.

The framework can detect the anomalous access pattern which is different from the user's historical behavior based on the behavioral consistency and historical reputation.

Authorization is not assumed to be permanently trusted, but it is ever-adapting to observed activity

D. Device Compromise

Compromising devices typically have valid authentication credentials and anomalous system characteristics.

The framework uses device fingerprinting to identify unexpected changes including:

- Browser modifications
- Operating system changes
- Hardware replacement
- Secure Boot status changes
- Trusted Platform Module (TPM) availability

Reduced device trust directly influences the overall trust score.

E. Network-Based Attacks

Network reputation contributes additional contextual evidence by evaluating:

- VPN usage
- Anonymous proxy services
- TOR exit nodes
- IP reputation
- Geographic anomalies

This information complements behavioral and device analysis without relying on any one security indicator alone.

VI. LIMITATIONS

While the suggested framework overcomes some of the limitations of conventional authentication systems, it has some limitations.

1. The importance of proper adjustment of the relevant weighting factors in various organizational settings.
2. Behavioral characteristics change naturally over time, so models need to be updated periodically.
3. Reducing the uniqueness of fingerprints in browser privacy protections by design might impact device fingerprinting.
4. Continuous surveillance has increased the complexity of the infrastructure in comparison to traditional authentication systems.
5. The framework currently relies on trusted collection of contextual data from client devices and enterprise infrastructure.

These limitations offer opportunities for further investigation.

VII. ETHICAL CONSIDERATIONS

Continuous authentication is based on the acquisition and processing of contextual user information Thus, privacy preservation should be a major design goal.

The proposed framework recommends following the following principles:

- Collect only information necessary for authentication.
- Avoid unnecessary long-term storage of behavioral information.
- Encrypt all authentication-related data both at rest and in transit.
- Provide transparency regarding collected contextual information.
- Comply with applicable privacy regulations including GDPR [13], HIPAA [14], and regional data protection legislation where applicable.

Behavioral information should only be used for authentication purposes, not for employee monitoring or any other unrelated surveillance purposes.

Future Work

Several research directions may extend the proposed framework.

Federated trust learning across multiple organizations.

- Privacy-preserving behavioral authentication using federated learning.
- Integration with passkeys and passwordless authentication.
- Edge-based trust computation for mobile devices.

- Machine learning–based adaptive weighting of contextual indicators.
- Integration with Security Information and Event

Management (SIEM) platforms.

- Formal verification of trust update algorithms.
- Large-scale empirical evaluation using enterprise authentication datasets.

These directions may further improve scalability, privacy, and resilience against emerging cyber threats.

VIII. CONCLUSION

In this paper we presented the Adaptive Trust-Based Continuous Authentication Framework (ATCAF), a lightweight architecture that extends Zero Trust principles with continuous risk-aware authentication.

The proposed framework differs from traditional authentication approaches that authenticate users at login by continuously evaluating trust through the combination of different context based security indicators such as device trust, behavior consistency, network reputation, location confidence and past user reputation.

A unified mathematical trust model was proposed to quantify the user trust as a continuously changing value rather than a binary authentication decision. This enables dynamic authorization responses, from seamless access to step-up multi-factor authentication or session termination based on changing security conditions.

REFERENCES

1. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
2. D. Freeman, S. Jain, M. Dürmuth, B. Biggio, and G. Giacinto, "Who Are You? A Statistical Approach to Measuring User Authenticity," in Proc. 23rd Network and Distributed System Security Symp. (NDSS), San Diego, CA, USA, 2016. doi: 10.14722/ndss.2016.23240.
3. V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent Progress and Remaining Challenges," IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49–61, Jul. 2016. doi: 10.1109/MSP.2016.2555335.
4. K. S. Killourhy and R. A. Maxion, "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics," in Proc. IEEE/IFIP Int. Conf. Dependable Systems and Networks (DSN), Lisbon, Portugal, 2009, pp. 125–134. doi: 10.1109/DSN.2009.5270346.
5. P. Eckersley, "How Unique Is Your Web Browser?," in Privacy Enhancing Technologies (PETS 2010), Lecture Notes in Computer Science, vol. 6205, Berlin, Germany: Springer, 2010, pp. 1–18. doi: 10.1007/978-3-642-14527-8_1.
6. J. Glasser and B. Lindauer, "Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data," in Proc. 2013 IEEE Security and Privacy Workshops, San Francisco, CA, USA, 2013, pp. 98–104. doi: 10.1109/SPW.2013.37.
7. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in Proc. 4th Int. Conf. Information Systems Security and Privacy (ICISSP), Funchal, Portugal, 2018, pp. 108–116.
8. D. Hardt, Ed., "The OAuth 2.0 Authorization Framework," IETF RFC 6749, Oct. 2012.
9. N. Sakimura, J. Bradley, M. B. Jones, B. de Medeiros, and C. Mortimore, "OpenID Connect Core Incorporating Errata Set 1," OpenID Foundation, Nov. 2014.
10. S. Cantor, J. Kemp, R. Philpott, and E. Maler, Eds., "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS Standard, Mar. 2005.
11. J. Hodges, J. C. Jones, M. B. Jones, A. Kumar, and E. Lundberg, Eds., "Web Authentication: An API for Accessing Public Key Credentials Level 2," W3C Recommendation, Apr. 2021.
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Official Journal of the European Union, L119, 2016.