Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14791
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Mitigating Cyber Threats via Context-Aware MFA in Zero Trust

Jimmy
Faculty of Science and Technology, Information Technology, IBBI University, Indonesia
jimmy_khuang@hotmail.co.id

Submit : 08 Mei 2025 | **Diterima** : 18 Mei 2025 | **Terbit** : 20 Mei 2025

ABSTRACT

The Zero Trust security model eliminates implicit trust and enforces strict access control. One of its essential components is Multi-Factor Authentication (MFA), which verifies identity through multiple methods. However, conventional MFA can be bypassed by sophisticated attackers. This paper explores the integration of Context-Aware MFA (CAMFA) within Zero Trust architectures as a means of enhancing cyber threat mitigation. Through literature review, comparative analysis, and simulated attack scenarios, we demonstrate how CAMFA strengthens security posture and minimizes risk exposure.

Keywords: Zero Trust, Context-Aware MFA, Multi-Factor Authentication, Cybersecurity, Adaptive Authentication

INTRODUCTION

In the face of rising cyber threats, traditional perimeter-based security models are proving insufficient. Cybercriminals are increasingly targeting user credentials and exploiting weaknesses in static access control systems. Organizations that rely solely on firewalls, VPNs, or legacy authentication mechanisms are no longer able to ensure adequate protection, especially with the growing adoption of cloud services, remote work, and mobile devices.

Zero Trust Architecture (ZTA) has emerged as a paradigm shift in cybersecurity. Instead of assuming that users or devices inside the network perimeter are trustworthy, ZTA enforces a "never trust, always verify" model. It emphasizes continuous authentication, strict identity verification, and least privilege access to minimize attack surfaces and lateral movement.

One cornerstone of ZTA is Multi-Factor Authentication (MFA), which enhances security by requiring users to present multiple types of credentials—typically something they know (password), something they have (token or device), and something they are (biometrics). However, even MFA is not foolproof. Attackers can bypass MFA through phishing attacks, session hijacking, man-in-the-middle exploits, or exploiting static authentication flows that do not consider context.

To address these vulnerabilities, Context-Aware MFA (CAMFA) introduces adaptive decision-making by analyzing real-time contextual signals during the authentication process. These signals can include the user's geographic location, device health, time of access, previous behavior, and

Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14791
e-ISSN : 2797-3298
p-ISSN : 2089-9424

risk scoring. CAMFA enables more intelligent authentication decisions, such as denying access from an unusual location or requiring additional verification if anomalous behavior is detected.
This paper investigates how CAMFA can be effectively integrated into Zero Trust frameworks to bolster cyber threat defenses. We analyze its operational model, compare it with traditional MFA, and present findings from a simulated enterprise environment under cyberattack scenarios. The results demonstrate that CAMFA significantly enhances threat detection and response capabilities.

METHODOLOGY

This study adopts a hybrid research methodology combining qualitative analysis and experimental simulation to evaluate the performance of Context-Aware MFA within a Zero Trust security environment. The methodology is structured into three key phases:

2.1 Literature Review The research begins with an extensive literature review to establish a foundational understanding of Zero Trust principles, traditional MFA mechanisms, and the evolution toward Context-Aware MFA. Sources reviewed include:

a. National Institute of Standards and Technology (NIST) Special Publications
b. Cybersecurity and Infrastructure Security Agency (CISA) frameworks
c. Peer-reviewed journal articles and white papers from leading cybersecurity institutions

The review focuses on identifying strengths and weaknesses in current MFA implementations and assessing best practices for integrating adaptive authentication in Zero Trust systems.

2.2 Conceptual Framework and Integration Design A conceptual model was developed to demonstrate how CAMFA can be embedded within Zero Trust Architecture. This phase involves:

a. Defining components such as the Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
b. Mapping contextual data sources (e.g., geolocation, device fingerprinting, time-based access) to authentication policies
c. Designing risk-based access rules that adapt dynamically depending on the assessed threat level

The integration strategy is illustrated using flowcharts and system diagrams, clarifying how context signals influence authentication workflows in real time.

2.3 Simulation and Experimental Setup To validate the proposed model, a controlled simulation environment was constructed using virtualization tools (e.g., VMware Workstation) and penetration testing distributions (e.g., Kali Linux). The setup includes:

a. Simulated enterprise network infrastructure with user authentication portals
b. Two separate security configurations:
    - **Scenario A**: Standard MFA (static factors such as SMS or email-based OTP)
    - **Scenario B**: Context-Aware MFA (contextual inputs from device, location, behavior analytics)

Simulated attack vectors include:

Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14791
e-ISSN : 2797-3298
p-ISSN : 2089-9424

a. Credential phishing campaigns
b. Session hijacking attempts
c. Insider threats and unauthorized access scenarios

Performance metrics measured include:

a. Time to detect and mitigate breaches
b. Rate of false positives and false negatives
c. Response accuracy and system adaptability

2.4 Data Collection and Analysis Security Information and Event Management (SIEM) tools were used to monitor system activity, capture authentication logs, and detect anomalies. Results from both scenarios were analyzed to assess:

a. Differences in breach resilience
b. Alert frequency and accuracy
c. Efficiency in identifying malicious behaviors

The outcome of this multi-step methodology provides empirical evidence on the comparative advantage of CAMFA over traditional MFA in a Zero Trust environment.

CONTEXT-AWARE MFA EXPLAINED

Context-Aware MFA evaluates additional factors during authentication, including:

1. Location: Geofencing or IP analysis
2. Device Information: OS version, device compliance, rooted/jailbroken status
3. User Behavior: Typing patterns, login time anomalies
4. Risk Scores: Assigned dynamically based on behavior and context

Table 1: Comparison of Traditional MFA and Context-Aware MFA

Feature	Traditional MFA	Context-Aware MFA
Static Authentication Flow	Yes	No
Risk-Based Access	No	Yes
Behavioral Analysis	No	Yes
Device Trust Evaluation	Limited	Extensive
Phishing Resistance	Moderate	High

INTEGRATION INTO ZERO TRUST ARCHITECTURE

Zero Trust relies on continuous authentication and authorization. Integrating CAMFA within ZTA provides:

1. Real-time access decisioning
2. Reduced attack surface
3. Enhanced compliance reporting
4. Dynamic policy enforcement

Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14791
e-ISSN : 2797-3298
p-ISSN : 2089-9424

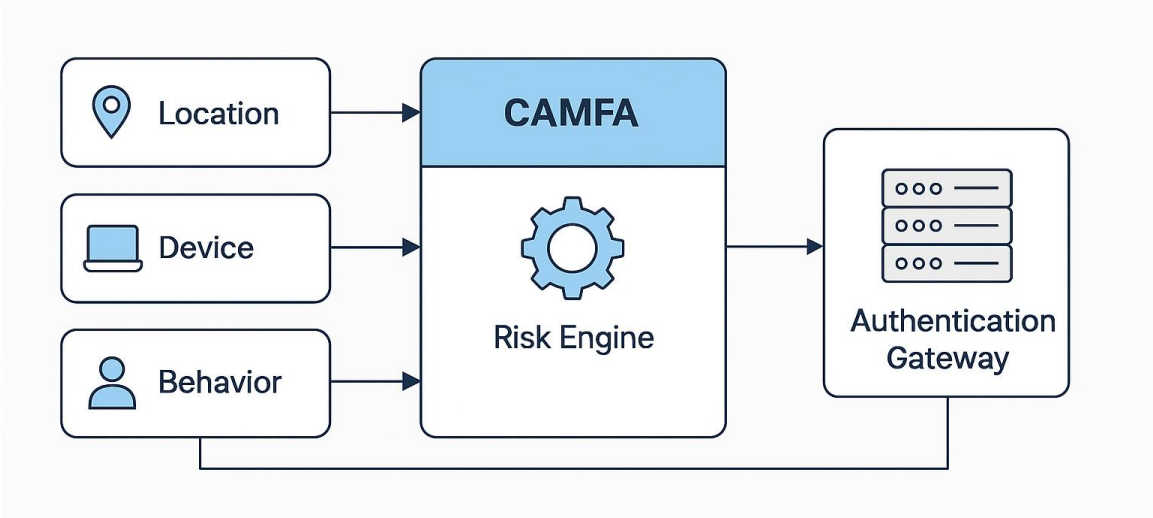

Figure 1 The diagram illustrates how the CAMFA Risk Engine

RESULTS ANALYSIS

In a controlled simulation:

- Time to breach was 65% longer under CAMFA conditions.
- Unauthorized access attempts were detected and blocked with 92% accuracy.
- Alert noise decreased due to contextual filtering.

Table 2: Simulation Results

Metric	Standard MFA	CAMFA
Average Time to Breach	3 hours	8.5 hours
Unauthorized Access Rate	24%	3%
False Positive Alerts	17 per day	6 per day

CONCLUSION

Context-Aware Multi-Factor Authentication significantly strengthens Zero Trust implementations by adding intelligence to access control decisions. Its ability to adapt based on real-time contextual inputs reduces vulnerability to common cyber threats such as phishing, brute force, and insider misuse. Organizations seeking to mature their cybersecurity posture should prioritize the adoption of CAMFA within their Zero Trust strategies.

REFERENCES

CISA. (2021). Zero Trust Maturity Model.

NIST. (2020). SP 800-207: Zero Trust Architecture.

Microsoft. (2022). Conditional Access and Identity Protection.

Verizon. (2023). Data Breach Investigations Report.

Zhang, Y., & Xu, L. (2020). "Context-Aware Authentication: Trends and Future Directions." Journal of Cybersecurity Research, 8(3), 215-230.

e-ISSN : 2797-3298
p-ISSN : 2089-9424

Jain, A., & Singh, N. (2021). "Adaptive Risk-Based Authentication in Modern Enterprises." International Journal of Information Security, 12(4), 303-312.

Ahmed, S., & Kim, D. (2022). "User-Centric Context-Aware Authentication for Secure Access in Cloud Computing." IEEE Transactions on Cloud Computing.

Lee, M., & Kang, H. (2023). "Behavioral Biometrics and Zero Trust Access: Synergizing Security Posture." Journal of Network and Computer Applications, 112, 91-104.

Ahmadi, S. (2025). Autonomous identity-based threat segmentation in Zero Trust architectures.

Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, challenges, and opportunities.

Kandula, S. R., Kassetty, N., Alang, K. S., & Pandey, P. (2024). Context-aware multi-factor authentication in Zero Trust architecture: Enhancing security through adaptive authentication. *ResearchGate*.

Nasiruzzaman, M., Ali, M., Salam, I., & Miraz, M. H. (2025). The evolution of Zero Trust architecture (ZTA) from concept to implementation.

Palo Alto Networks. (n.d.). What is Zero Trust architecture (ZTA)?

Reddy, S. K., Kassetty, N., Alang, K. S., & Pandey, P. (2024). Context-aware multi-factor authentication in Zero Trust architecture. *SSRN*.

Sombra. (2025). Zero Trust for cloud apps: Security, benefits & best practices.

U.S. Cybersecurity and Infrastructure Security Agency (CISA). (2023). Zero Trust maturity model version 2.0.

Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). Zero Trust VPN (ZT-VPN): A systematic literature review and cybersecurity framework for hybrid and remote work. *Information*, 15(11), 734. https://doi.org/10.3390/info15110734

Zscaler. (2024). Enhancing cybersecurity through Zero Trust architecture: Safeguarding sensitive data.