Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Context-Aware Pre-Authorization Framework for Enhancing Server and Database Security in Zero Trust Environments

Patricia Ghann

patricia.ghann@ktu.edu.gh

Koforidua Technical University https://orcid.org/0000-0003-3072-2795

Research Article

Keywords: Zero Trust Architecture, Context-Aware Access Control, Pre-Authorization Security, Server and Database Security, Risk-Based Access Management, Credential-Based Attacks, Enterprise Security Architecture

Posted Date: May 19th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9733805/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: The authors declare no competing interests.

Abstract

This study addresses a critical limitation in conventional authentication and authorization mechanisms within Zero Trust environments, where contextual risk evaluation is often performed only after access initiation. This delay creates a vulnerability window that can be exploited through credential-based attacks. To mitigate this risk, this paper proposes a **Context-Aware Pre-Authorization Framework (CAPAF)**that introduces an independent pre-authorization layer between authentication and authorization stages.

The framework evaluates access requests using dynamically weighted contextual attributes, including device trust level, access location, behavioral patterns, and system sensitivity, prior to authorization enforcement. A deterministic risk-scoring model is employed to ensure transparency and auditability of decisions.

The proposed framework was implemented in a simulated environment comprising 10,000 access requests, including both legitimate and malicious scenarios. Experimental results show that CAPAF improves access accuracy from **82.4% to 96.1%** and reduces false negative rates from **14.4% to 1.9%**, with an average latency overhead of **132 ms**, which remains within acceptable operational limits.

The findings demonstrate that integrating a context-aware pre-authorization layer significantly enhances server and database security by enabling early threat detection and reducing reliance on static access control models. CAPAF provides a scalable and practical solution for strengthening Zero Trust architectures in modern enterprise systems.

1. Introduction

The increasing prevalence of credential-based attacks has exposed fundamental weaknesses in traditional authentication and authorization mechanisms used to protect server and database systems[1-3[. Although Zero Trust Architecture (ZTA) promotes continuous verification and strict access control, many implementations still grant access immediately after successful authentication, deferring contextual risk evaluation to later stages of the session lifecycle.

This design introduces a critical security gap: a temporal exposure window during which compromised credentials, trusted devices, or replayed sessions may be exploited before sufficient validation occurs[4-6]. As enterprise systems become more distributed and access patterns more dynamic, relying solely on identity verification is no longer sufficient to ensure secure access control[7-9].

Existing access control mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) primarily evaluate permissions based on static or semi-static attributes.[10-12]. While more advanced models such as Risk-Adaptive Access Control (RAdAC) incorporate contextual risk, they typically embed risk evaluation within authorization logic, resulting in tightly coupled and complex systems[13-15].

To address these limitations, this paper proposes a **Context-Aware Pre-Authorization Framework (CAPAF)** that introduces a dedicated risk evaluation layer positioned between authentication and authorization. This approach enables early detection of anomalous access attempts and eliminates implicit trust following authentication. By decoupling risk assessment from authorization enforcement, CAPAF enhances modularity, scalability, and alignment with Zero Trust principles[16-20].

1.1Problem Statement

The rapid growth of internet-based services has led to increased reliance on web browsers, servers, and databases for information access, storage, and service delivery. To protect these systems, authentication mechanisms such as usernames and passwords are widely used to verify user identity before granting access to servers and backend databases. Despite these measures, unauthorized access and security breaches continue to occur at an alarming rate. Attackers frequently exploit stolen credentials, weak authentication protocols, session hijacking, and server-side vulnerabilities to bypass traditional access control systems.

Current authentication approaches primarily focus on verifying *who* the user claims to be at the point of login, while largely ignoring the *context* and *intent* of the access request after authentication is completed [21-24]. As a result, once valid credentials are compromised, malicious actors are often able to access sensitive systems and resources without triggering additional security checks [16,18,25-27]. This limitation exposes servers and databases to data breaches, privilege escalation, and prolonged unauthorized access.

Moreover, existing systems rarely perform systematic pre-evaluation of critical access attributes such as the intent of the request, the geographical location of access, the duration and frequency of access, the type of system or resource being requested, and the behavioral identity of the requesting entity[28,29]. The absence of such contextual and behavioral assessment mechanisms significantly weakens server-side security, particularly in environments with high volumes of remote and distributed access.

Therefore, there is a critical need for a security framework that extends beyond traditional login-based authentication by introducing a pre-evaluation phase that dynamically analyzes access context, request intent, user behavior, and system sensitivity before granting or sustaining access. Addressing this gap could significantly reduce successful intrusion attempts, limit the impact of compromised credentials, and enhance the overall resilience of servers and databases against modern cyber threats.

1.2 Research Aim and Objectives

To design and evaluate a context-aware pre-authorization framework that enhances server and database security by dynamically enforcing Zero Trust principles after authentication but before access

authorization.

Specific Research Objectives

1. To analyze the security limitations of traditional authentication-based access control mechanisms in server and database environments.

2. To identify and model contextual attributes, including request intent, access location, access duration, system sensitivity, and requester identity, that influence access trustworthiness.

3. To design a context-aware pre-authorization framework that evaluates access requests dynamically before authorization.

4. To align the proposed framework with Zero Trust Architecture principles, including continuous verification and least-privilege enforcement.

5. To implement a rule-based or risk-scoring decision engine for context-driven access control.

6. To experimentally evaluate the effectiveness of the proposed framework in reducing unauthorized access and credential-based attacks.

7. To compare the proposed framework with conventional authentication-only access control approaches.

2. Positioning Against Existing Access Control Models

Traditional access control models such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) rely primarily on static or semi-static authorization decisions made after successful authentication [30,31]. While RBAC assigns permissions based on predefined roles, it lacks contextual adaptability and is vulnerable when credentials are compromised. ABAC improves flexibility by incorporating attributes such as user role, resource type, and environmental conditions; however, authorization decisions are still typically evaluated at a single point in time and do not continuously assess access intent or behavioral anomalies.

Risk-Adaptive Access Control (RAdAC) and Continuous Adaptive Risk and Trust Assessment (CARTA) introduce dynamic risk evaluation into access decisions [32,33]. Nevertheless, many existing implementations integrate risk assessment directly into authorization logic, making them complex to deploy and tightly coupled with application-layer authorization mechanisms.

The proposed Context-Aware Pre-Authorization Framework (CAPAF) differs fundamentally from these approaches by introducing an explicit, standalone pre-authorization phase that operates *between authentication and authorization***.** This architectural separation allows contextual and behavioral risk

evaluation to occur independently of identity verification and authorization enforcement, aligning more closely with Zero Trust principles of continuous verification and assumption of breach.

By decoupling risk-based trust evaluation from traditional authorization mechanisms, CAPAF enhances server and database security without requiring invasive changes to existing authentication or authorization infrastructures. This makes the framework particularly suitable for modern distributed systems and legacy environments transitioning toward Zero Trust Architecture.

3. Methodology

3.1 Research Design

This study adopts a **quantitative, experimental research design** to evaluate the effectiveness of the proposed Context-Aware Pre-Authorization Framework (CAPAF) in mitigating unauthorized access within Zero Trust environments. The approach combines **system design, formal risk modeling, and simulation-based validation** to assess both security performance and computational overhead.

The evaluation follows a **comparative framework**, where CAPAF is benchmarked against a baseline **authentication-only access control model**, enabling controlled measurement of improvements in detection accuracy, false decision rates, and latency.

3.2 System Model and Architectural Assumptions

The CAPAF framework is modeled as an **intermediate security layer** positioned between authentication and authorization components in a typical enterprise system. The system assumes:

· Users are authenticated through standard identity providers (e.g., token-based or credential-based systems).

· Access requests target protected server and database resources.

· Contextual attributes can be collected in real time without significant delay.

· Security policies and risk thresholds are predefined but configurable.

Let an access request be represented as:

R = {U, A, C, T}

Where:

· U: authenticated user identity

· A: requested action or resource

· C: contextual attributes

· T: timestamp of request

3.3 Contextual Attribute Modeling

CAPAF evaluates access requests using a set of contextual attributes:

C = {A_1, A_2, ..., A_n}

Where each Ai represents a measurable feature influencing access trustworthiness. In this study, the selected attributes include:

- Access Location
- Device Trust Level
- Access Time
- Request Frequency
- System Sensitivity
- Behavioral Patterns

Each attribute is associated with a **risk weight wi** reflecting its relative importance in security decision-making.

3.4 Risk Scoring Model

The CAPAF framework employs a **deterministic weighted risk aggregation model** to quantify the trustworthiness of each access request.

The cumulative risk score is defined as:

$$\text{Risk Score} = \sum_{i=1}^{n} \text{wi}.\,\text{f(Ai)}$$

Where:

· wi ∈ R+: weight assigned to attribute Ai

· f(Ai): deviation function mapping attribute values to risk contributions

· n: total number of contextual attributes

To ensure comparability across requests, the risk score is normalized:

$$\text{Risk Score}_{\text{norm}} = \sum_{i=1}^{n} \text{wi}.\,\text{f(Ai)} / \sum_{i=1}^{n} \text{wi}$$

The deviation function f(Ai)f(A_i)f(Ai) is defined such that:

· f(Ai) = 0 if the attribute complies with policy

· f(Ai) > 0 if deviation or anomaly is detected

Behavioral anomalies are computed using historical access patterns and incorporated as an additive risk component.

3.5 Decision Policy

Access decisions are made using a **threshold-based policy**:

$$\text{Decision}(R)=\{\text{Grant, if Risk Score}_{\text{norm}} \leq \tau, \text{ Deny, if Risk Score}_{\text{norm}} > \tau$$

Where:

· τ: predefined risk threshold

In this study, τ = 0.4 (equivalent to 40%) based on empirical tuning during preliminary simulations.

3.6 CAPAF Workflow

The operational workflow of CAPAF consists of the following stages:

1. **Authentication Stage**
 The user is authenticated using standard mechanisms.

2. **Context Acquisition**
 Real-time contextual attributes are collected.

3. **Risk Evaluation**
 The risk score is computed using the weighted aggregation model.

4. **Pre-Authorization Decision**
 The computed score is compared against the threshold.

5. **Access Enforcement**
 Approved requests proceed to authorization; denied requests are blocked.

6. **Audit Logging**
 All decisions and contextual data are recorded for analysis and compliance.

3.7 Implementation Environment

The framework was implemented using a **modular prototype architecture** with the following technologies:

· **Programming Environment:** Python (core logic and simulation engine)

· **Database Systems:** MySQL / PostgreSQL (logging and policy storage)

· **Security Protocols:** OAuth 2.0, JSON Web Tokens (JWT), TLS/SSL

· **Virtualization Platform:** Docker-based containerized environment

The modular design enables scalability and ease of integration into existing enterprise infrastructures.

3.8 Experimental Setup

A simulation environment was developed to emulate real-world access control scenarios. The dataset consisted of **10,000 access requests**, including both legitimate and malicious cases.

Scenario Categories

· Legitimate user access

· Stolen credential attacks

· Insider threat behavior

· Abnormal access patterns (frequency and timing anomalies)

Malicious scenarios were generated by systematically altering contextual attributes to simulate real-world attack vectors.

3.9 Evaluation Metrics

The framework was evaluated using standard access control performance metrics:

· **Access Accuracy (ACC):** proportion of correct decisions

· **False Positive Rate (FPR):** legitimate requests incorrectly denied

· **False Negative Rate (FNR):** malicious requests incorrectly allowed

· **Decision Latency:** average processing time per request

· **Policy Coverage:** proportion of applicable rules evaluated

These metrics enable a comprehensive assessment of both **security effectiveness and system performance**.

3.10 Baseline Comparison

CAPAF was compared against a **traditional authentication-only model**, where access is granted immediately after successful authentication without contextual evaluation.

This baseline provides a controlled reference to quantify the **security gains introduced by pre-authorization risk assessment**.

4. System Architecture

The proposed Context-Aware Pre-Authorization Framework (CAPAF) is designed as an intermediary security layer positioned between the authentication service and the authorization mechanisms of servers and databases within a Zero Trust environment. The architecture, as illustrated in ***Figure 1***, ensures that successful authentication alone does not imply trust, and all access requests are subject to contextual and behavioral evaluation before authorization.

4.1 Architectural Overview

The architecture consists of six core components:

1. ***Client Interface***
 The client interface represents users accessing servers or databases via web browsers, applications, or APIs. Users authenticate using standard mechanisms such as username/password, multi-factor authentication, or token-based authentication.

2. ***Authentication Service***
 This component verifies user identity using existing authentication protocols (e.g., OAuth 2.0, JWT). Upon successful authentication, no direct access to protected resources is granted. Instead, the authenticated request is forwarded to the pre-authorization layer.

3. ***Context Collector***
 The Context Collector gathers real-time contextual attributes associated with each access request, including:

o User role and identity claims

o Device characteristics

- Network and geographical location
- Time of access
- Request type and access intent

4. ***Risk Evaluation Engine***
The Risk Evaluation Engine analyzes collected contextual data using predefined policy rules and historical behavioral patterns. A cumulative risk score is computed based on policy compliance, anomaly detection, and system sensitivity.

5. ***Pre-Authorization Decision Module***
This module compares the computed risk score against predefined thresholds to determine whether access should be permitted or denied. Only requests that satisfy acceptable risk levels are forwarded to the authorization and resource layers.

6. ***Server and Database Resources***
Protected servers and databases enforce authorization decisions based on least-privilege principles. Access is granted only after successful pre-authorization and standard authorization checks.

7. ***Audit and Logging Module***
All access requests, contextual attributes, risk scores, and decisions are logged for security auditing, compliance, and forensic analysis.

4.2 Request Flow Description

1. A user submits an access request through a browser or application.
2. The Authentication Service validates user credentials.
3. The authenticated request is intercepted by the CAPAF layer.
4. Contextual and behavioral data are collected in real time.
5. The Risk Evaluation Engine computes a risk score.
6. The Pre-Authorization Module grants or denies access based on risk thresholds.
7. All decisions are logged for monitoring and analysis.

Figure 2 depicts the sequence of interactions during an access request.

5: Algorithms and Risk Evaluation

5.1 Context-Aware Pre-Authorization Algorithm

The Context-Aware Pre-Authorization Framework (CAPAF) employs a deterministic, rule-based risk evaluation mechanism to assess the trustworthiness of access requests after authentication but before authorization. The algorithm evaluates multiple contextual attributes and assigns a cumulative risk score that determines whether access is granted or denied.

Algorithm 1: CAPAF_PreAuthorization

Input:
Authenticated_User_Request, Context_Data

Output:
Access_Granted or Access_Denied

1. Receive authenticated access request
2. Extract contextual attributes from Context_Data
3. Retrieve applicable security policies and risk weights
4. Compute cumulative Risk_Score
5. Compare Risk_Score against predefined threshold
6. If Risk_Score ≤ Threshold:
   Grant access
   Else:
   Deny access
7. Log decision and contextual attributes
8. Return access decision

5.2 Deterministic Risk Evaluation Model

The risk evaluation engine computes a cumulative risk score based on weighted contextual attributes. Each attribute contributes independently to the overall risk score, enabling transparency and auditability of authorization decisions.

Risk Score = sum(i=1 to n) wi * f(Ai) ….Equ(1)

Where;

wi: weight assigned to attribute Ai

f(Ai): deviation or risk contribution function

n: number of contextual attributes

Algorithm 2: Evaluate_Risk

Input:
Context_Data, User_History

Output:
Risk_Score (0–100)

1. Initialize Risk_Score = 0

2. For each contextual attribute AiA_iAi:
   a. Compare AiA_iAi against policy rules
   b. If deviation detected, add corresponding weight WiW_iWi to Risk_Score

3. Analyze User_History for behavioral anomalies
   a. If anomaly detected, add anomaly weight

4. Normalize Risk_Score to a 0–100 scale

5. Return Risk_Score

Access Threshold:

· Risk_Score ≤ 40 → Access Granted

· Risk_Score > 40 → Access DeniedThe internal risk assessment and decision-making process is illustrated in Figure 3.

5.3 Design Rationale

A rule-based risk engine was selected for this study due to its interpretability, low computational overhead, and suitability for security-critical environments where transparency and auditability are required. While machine learning techniques may enhance anomaly detection accuracy, they introduce complexity and explainability challenges. Therefore, ML-based risk assessment is reserved for future work. The risk weights assigned to contextual attributes were derived using a policy-driven expert judgment approach informed by existing cybersecurity literature and Zero Trust best practices. Attributes with a higher potential impact on confidentiality and system integrity, such as system sensitivity and

access location, were assigned higher weights, while contextual indicators with moderate risk implications, such as access time and request frequency, were assigned lower weights.

This approach reflects common enterprise security policies where access to critical resources and anomalous geographic access are treated as higher-risk events. Although the weights were statically defined for this study to ensure transparency and reproducibility, they can be tuned dynamically based on organizational risk tolerance or historical attack data in real-world deployments. The contextual attributes and their corresponding risk weights used in the CAPAF risk evaluation engine are summarized in Table 1.

Table 1. Contextual Risk Attributes and Assigned Weights

Context Attribute	Description	Weight
Access Location	Unusual or high-risk geographic location	20
Device Trust Level	Unknown or unregistered device	15
Access Time	Abnormal access time	10
Request Frequency	Excessive or burst access attempts	15
System Sensitivity	Critical server or database resource	25
Behavioral Anomaly	Deviation from historical access patterns	15

6. Experimental Setup

The proposed CAPAF framework was evaluated using a simulation-based experimental environment designed to emulate real-world server and database access scenarios. The simulation was implemented using Python and deployed in a virtualized environment using Docker containers.

The test environment consisted of:

· A simulated authentication service

· A CAPAF pre-authorization layer

· A protected server and database backend

A total of **10,000 access requests** were generated, comprising both legitimate and malicious access attempts.

6.1 Attack and Access Scenarios

The evaluation included the following scenarios:

1. **Legitimate Access Requests**

· Normal access behavior

· Known devices and locations

2. **Stolen Credential Attacks**

· Valid credentials used from unfamiliar devices or locations

3. **Insider Threat Simulation**

· Authenticated users attempting access beyond normal usage patterns

4. **Abnormal Access Patterns**

· High-frequency access requests

· Off-hours access to sensitive resources

6.1.1 Malicious Request Simulation

Malicious access requests were generated by systematically modifying contextual attributes of otherwise legitimate authentication events. This included altering access location, device identity, request frequency, and access timing to simulate stolen credential usage, insider misuse, and automated attack behavior. Behavioral anomalies were introduced by deviating from historical access patterns associated with authenticated users. This controlled approach allowed direct comparison between legitimate and malicious access attempts while maintaining reproducibility of the experimental setup.

6.2 Evaluation Metrics

The framework was evaluated using the following metrics:

· **Access Accuracy**: Correct authorization decisions

· **False Positive Rate (FPR)**: Legitimate users denied access

· **False Negative Rate (FNR)**: Malicious users granted access

· **Average Decision Latency**: Pre-authorization processing time

· **Policy Coverage**: Percentage of applied policy rules

The selected evaluation metrics capture both security effectiveness and system performance and are commonly used in access control evaluation studies. These metrics were applied consistently across both the authentication-only baseline and the proposed CAPAF framework.

6.3 Baseline Comparison

CAPAF was compared against a traditional authentication-only access control system, where access was granted immediately after successful authentication without contextual evaluation.

6.4 Results and Discussion

The performance of the proposed Context-Aware Pre-Authorization Framework (CAPAF) was evaluated against a traditional authentication-only access control model using a dataset of 10,000 simulated access requests. The evaluation focused on classification accuracy, false decision rates, and processing latency.

The results demonstrate that CAPAF significantly improves access control effectiveness by incorporating contextual and behavioral risk assessment prior to authorization.

6.4.1 Receiver Operating Characteristic (ROC) Analysis

The ROC curve in **Figure 4** illustrates the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) for both CAPAF and the baseline model.

The CAPAF curve consistently dominates the baseline, indicating superior discriminative capability in distinguishing between legitimate and malicious access requests. The curve approaches the top-left region of the ROC space, reflecting a high detection rate with relatively low false alarms.

This improvement is primarily attributed to the integration of contextual attributes such as access location, device trust level, and behavioral patterns, which enable early identification of anomalous access attempts that would otherwise bypass authentication-only systems.

The baseline model, by contrast, exhibits limited discriminatory power due to its reliance on identity verification alone, resulting in a higher likelihood of accepting malicious requests with valid credentials.

6.4.2 CAPAF Performance

The confusion matrix in **Figure 5** highlights the classification performance of CAPAF. The framework achieves a high number of true positives and true negatives, indicating effective identification of both malicious and legitimate access requests.

Notably, the false negative rate is significantly reduced to **1.9%**, demonstrating the framework's ability to detect attacks involving compromised credentials. This is critical in Zero Trust environments, where credential-based attacks represent a major threat vector.

However, a slight increase in the false positive rate (**4.7%**) is observed compared to the baseline. This indicates that a small proportion of legitimate users may be incorrectly denied access. While this

introduces minor usability challenges, it is generally acceptable in high-security environments where the cost of unauthorized access outweighs occasional inconvenience.

6.4.3 Baseline Performance

The baseline confusion matrix in **Figure 6** reveals a substantially higher false negative rate (**14.4%**), indicating that a significant number of malicious requests are incorrectly granted access. This confirms the inherent limitation of authentication-only systems, which fail to detect threats once credentials are validated.

Although the baseline exhibits a slightly lower false positive rate (**3.2%**), this marginal usability advantage is outweighed by its inability to prevent unauthorized access effectively.

6.4.4 Latency Analysis

The latency comparison shown in **Figure 7** indicates that CAPAF introduces an average processing delay of **132 ms**, compared to **45 ms** for the baseline model.

This increase is expected due to the additional steps involved in:

· Context data collection

· Risk evaluation

· Pre-authorization decision-making

Despite this overhead, the latency remains within acceptable operational limits (below 200 ms) for most enterprise systems. The trade-off between security and performance is therefore justified, particularly in environments where data sensitivity and system integrity are critical.

6.5 Discussion of Findings

The results confirm that integrating a context-aware pre-authorization layer significantly enhances access control effectiveness in Zero Trust environments.

1. Improved Threat Detection

The substantial reduction in false negatives demonstrates that CAPAF effectively mitigates credential-based attacks by evaluating contextual and behavioral anomalies prior to granting access.

2. Enhanced Decision Accuracy

The increase in overall accuracy from **82.4% to 96.1%** reflects the advantage of combining identity verification with contextual risk assessment. This hybrid approach provides a more comprehensive evaluation of access legitimacy.

3. Security–Usability Trade-off

The slight increase in false positives indicates a trade-off between security and usability. However, this is a common and acceptable compromise in high-security systems, where stricter access control policies are required to prevent breaches.

4. Alignment with Zero Trust Principles

CAPAF reinforces the Zero Trust principle of *"never trust, always verify"* by eliminating implicit trust after authentication and ensuring that every access request is evaluated based on dynamic risk factors.

5. Practical Implications

The modular architecture of CAPAF allows it to be integrated into existing systems without significant modifications to authentication or authorization mechanisms. This makes it a practical solution for organizations transitioning toward Zero Trust security models.

6.6 Limitations of the Evaluation

While the results are promising, several limitations should be acknowledged:

· The evaluation was conducted in a simulated environment, which may not fully capture real-world variability in user behavior and attack patterns.

· The risk scoring model relies on predefined weights and thresholds, which may require tuning for different organizational contexts.

· The absence of real-world datasets limits the generalizability of the findings.

Future work will address these limitations by incorporating real-world deployment scenarios and adaptive machine learning techniques.

7. Conclusion and Future Work

This paper presented a Context-Aware Pre-Authorization Framework (CAPAF) designed to enhance server and database security within Zero Trust environments. By introducing an explicit pre-authorization phase that evaluates contextual and behavioral risk after authentication but before authorization, the framework addresses a critical security gap exploited by credential-based attacks.

Experimental evaluation demonstrated that CAPAF significantly improves access accuracy and reduces unauthorized access compared to traditional authentication-only mechanisms, while maintaining acceptable performance overhead. The findings confirm that context-aware risk assessment is a practical and effective enhancement to existing access control systems and aligns strongly with Zero Trust Architecture principles.

The primary contributions of this work include:

1. The design of a standalone pre-authorization layer that decouples risk evaluation from authentication and authorization.

2. A deterministic, rule-based risk assessment model that supports transparency and auditability.

3. An experimental validation demonstrating improved resilience against credential compromise and insider threat scenarios.

Future work will focus on extending the framework through the integration of machine learning-based anomaly detection to improve adaptability to emerging threats. Additional research will explore continuous re-evaluation of active sessions, large-scale deployment in distributed cloud environments, and real-world validation using operational datasets. Incorporating automated policy adaptation and fine-grained privilege adjustment based on real-time risk levels also represents a promising direction for further enhancement.

References

1. Lee, A. J. (2025). Credential-based access control. In Encyclopedia of Cryptography, Security and Privacy (pp. 463-465). Cham: Springer Nature Switzerland.
2. Ali, H. S., & Sridevi, R. (2022). Credential-based authentication mechanism for IoT devices in fog-cloud computing. In ICT Analysis and Applications (pp. 307-318). Singapore: Springer Nature Singapore.
3. Paya, A., & Gómez, A. (2025). Enhancing software-defined perimeters with integrated identity solutions and threat detection for robust zero trust security: A. Paya et al. International Journal of Information Security, 24(4), 178.
4. Hou, X., Zhao, Y., Wang, S., & Wang, H. (2025). Model context protocol (mcp): Landscape, security threats, and future research directions. ACM Transactions on Software Engineering and Methodology.
5. Alder, F., Scopelliti, G., Van Bulck, J., & Mühlberg, J. T. (2023, May). About time: On the challenges of temporal guarantees in untrusted environments. In Proceedings of the 6th Workshop on System Software for Trusted Execution (pp. 27-33).
6. Ray, P. P. (2025). A survey on model context protocol: Architecture, state-of-the-art, challenges and future directions. Authorea Preprints.
7. Nahar, K., & Gill, A. Q. (2022). Integrated identity and access management metamodel and pattern system for secure enterprise architecture. Data & Knowledge Engineering, 140, 102038.
8. Hamza, M. K., Abubakar, H., & Danlami, Y. M. (2018). Identity and access management system: a web-based approach for an enterprise. Traektoriâ Nauki= Path of Science, 4(11), 2001-2011.

9. Omotunde, H., & Ahmed, M. (2023). A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. Mesopotamian Journal of CyberSecurity, 2023, 115-133.
10. Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., ... & Scarfone, K. (2013). Guide to attribute based access control (abac) definition and considerations (draft). NIST special publication, 800(162), 1-54.
11. Lee, U., Joy, J., & Noh, Y. (2015). Secure personal content networking over untrusted devices. Wireless Personal Communications, 80(4), 1449-1473.
12. Farhadighalati, N., Estrada-Jimenez, L. A., Nikghadam-Hojjati, S., & Barata, J. (2025). A systematic review of access control models: Background, existing research, and challenges. IEEE Access, 13, 17777-17806.
13. Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. H. (2022). A unified framework for risk-based access control and identity management in compliance-critical environments. Journal of Frontiers in Multidisciplinary Research, 3(1), 23-34.
14. Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). SoK: Context and risk aware access control for zero trust systems. Security and Communication Networks, 2022(1), 7026779.
15. Xiao, S. (2023). A policy language for context-aware access control in zero-trust network.
16. Fang, W., Zhang, W., Chen, W., Pan, T., Ni, Y., & Yang, Y. (2020). Trust-based attack and defense in wireless sensor networks: a survey. Wireless Communications and Mobile Computing, 2020(1), 2643546.
17. Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews, 19(3), 105-116.
18. Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News, 190(1), 1-69.
19. Mayeke, N. R., Arigbabu, A. T., Olaniyi, O. O., Okunleye, O. J., & Adigwe, C. S. (2024). Evolving access control paradigms: A comprehensive multi-dimensional analysis of security risks and system assurance in cyber engineering. Asian Journal of Research in Computer Science, 17(5), 108-124.
20. Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309.
21. Shah, S. W., & Kanhere, S. S. (2019). Recent trends in user authentication–a survey. IEEE access, 7, 112505-112519.
22. Boonkrong, S. (2021). Authentication and Access Control. Berkeley, CA: Apress, 133-162.
23. Baig, A. F., & Eskeland, S. (2021). Security, privacy, and usability in continuous authentication: A survey. Sensors, 21(17), 5967.
24. Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., & Park, Y. (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. Ieee Access, 8, 54314-54344.

25. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.
26. Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. IEEE Communications Surveys & Tutorials, 21(4), 3723-3768.
27. Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8), 4060.
28. Liu, Y., Yu, F. R., Li, X., Ji, H., & Leung, V. C. (2020). Blockchain and machine learning for communications and networking systems. IEEE communications surveys & tutorials, 22(2), 1392-1431.
29. Pan, S., Tao, Z., Hoang, T., Zhang, D., Li, T., Xing, Z., ... & Lo, D. (2024). A {NEW}{HOPE}: Contextual Privacy Policies for Mobile Applications and An Approach Toward Automated Generation. In 33rd USENIX Security Symposium (USENIX Security 24) (pp. 5699-5716).
30. Alnaim, A. K. (2025). Adaptive Zero Trust Policy Management Framework in 5G Networks. Mathematics, 13(9), 1501.
31. Fu, C., Shen, G., Huang, Z., Xie, J., & Fu, J. (2025). Automatic IoT permission assignment with transformer models under spatiotemporal constraints. Journal of Information Security and Applications, 93, 104099.
32. Kumar, P. (2025). Next-generation secure authentication and access control architectures: advanced techniques for securing distributed systems in modern enterprises. International Journal of Computational and Experimental Science and Engineering, 11(3), 4966-4995.
33. Rehan, H. Zero-Trust Architecture for Securing Multi-Cloud Environments.

Figures

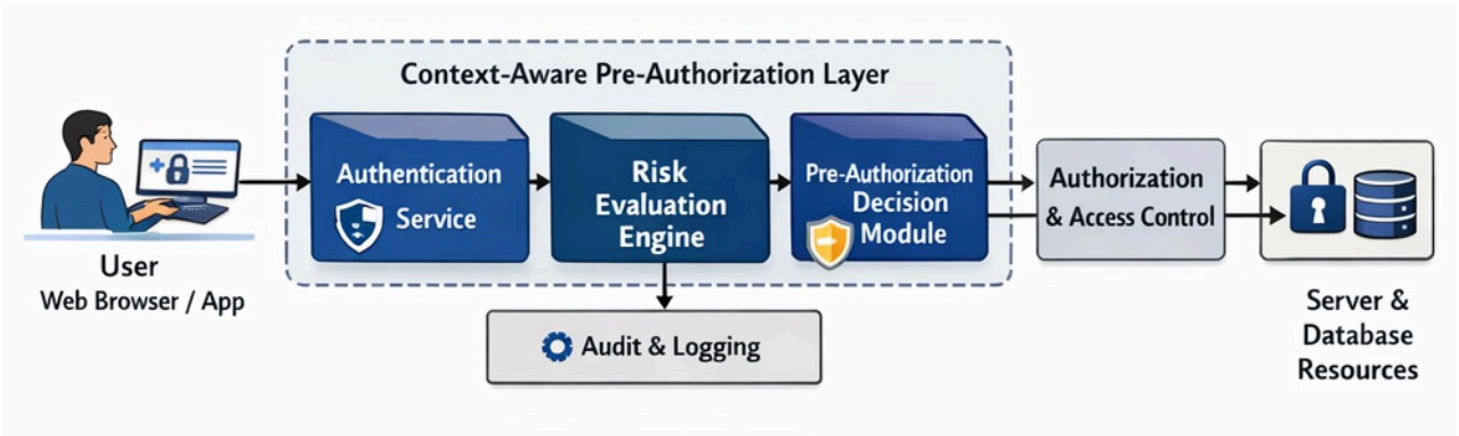


Figure 1

System Architecture of the Context-Aware Pre-Authorization Framework (CAPAF)

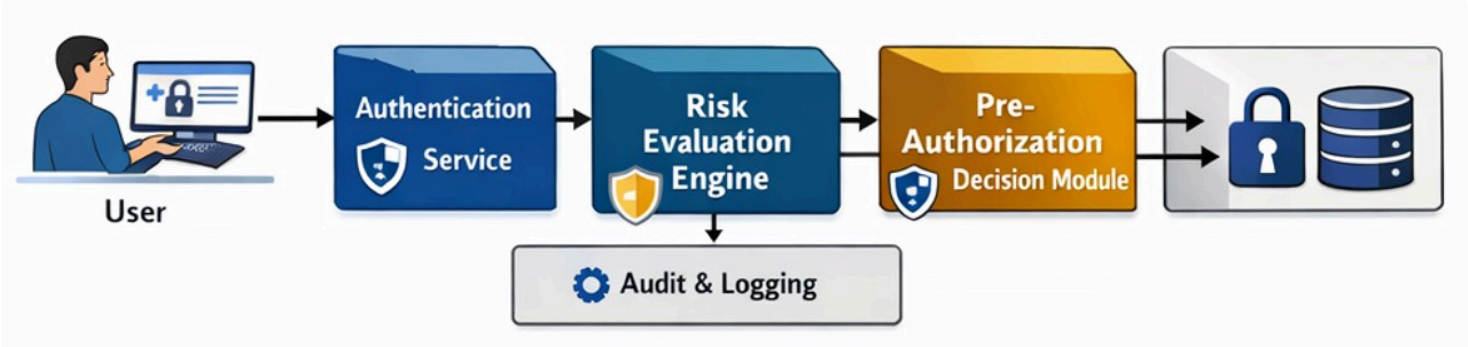


Figure 2

Access Request Flow in the CAPAF Framework

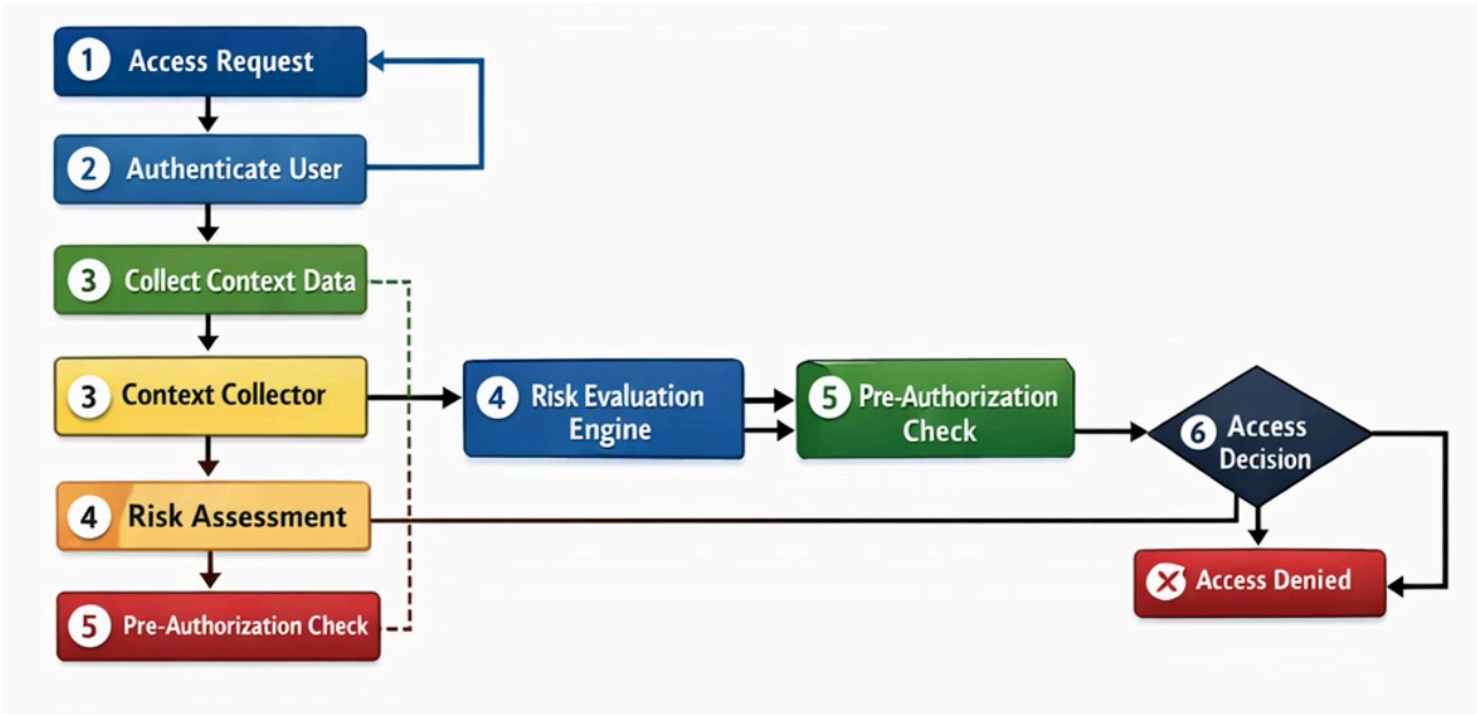


Figure 3

Risk Evaluation and Pre-Authorization Decision Flow in CAPAF

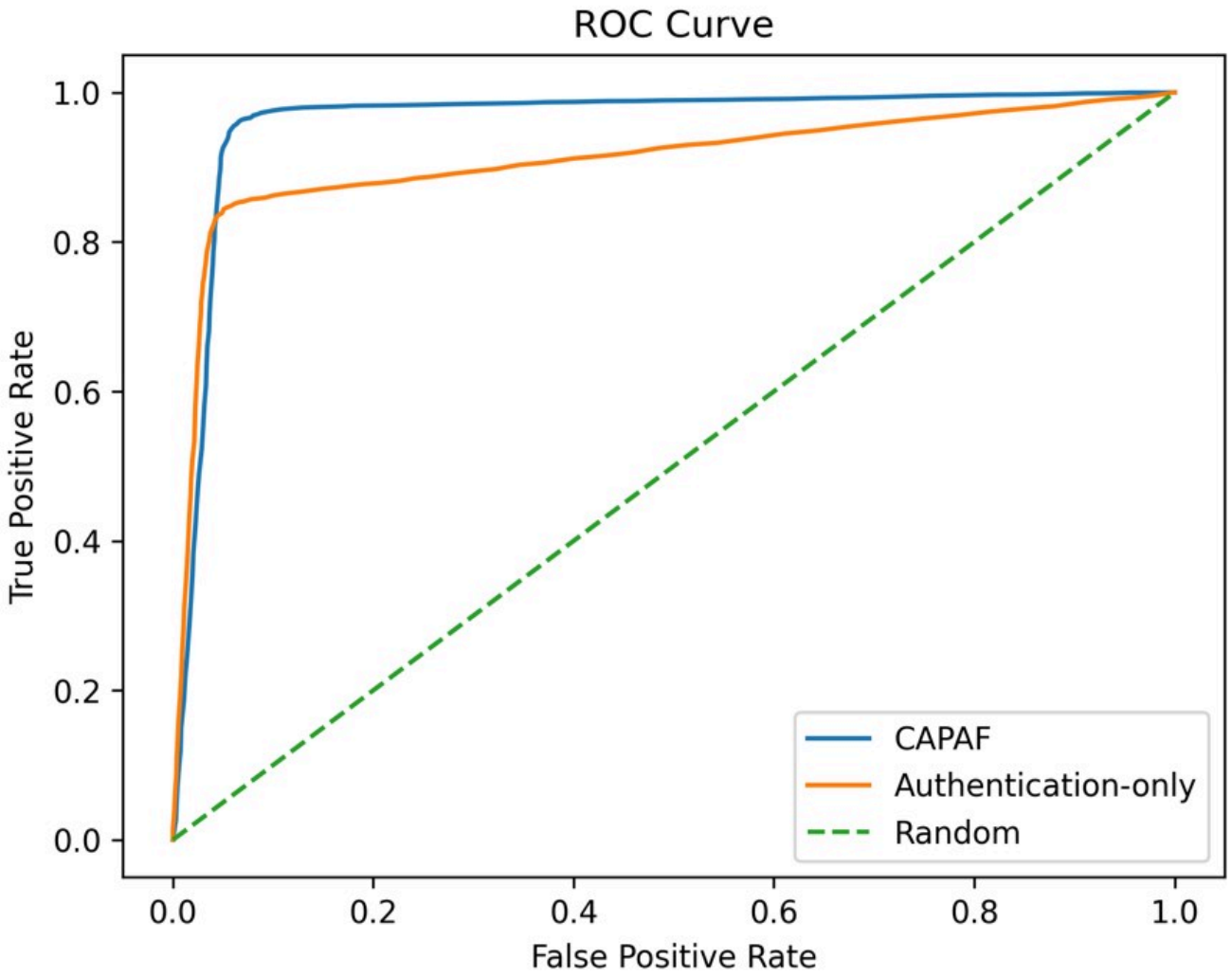


Figure 4

Receiver Operating Characteristic (ROC) curve comparing the performance of the proposed Context-Aware Pre-Authorization Framework (CAPAF) with a traditional authentication-only access control model. The CAPAF model demonstrates superior discriminative capability, achieving a higher true positive rate across varying false positive rates, indicating improved detection of malicious access attempts.

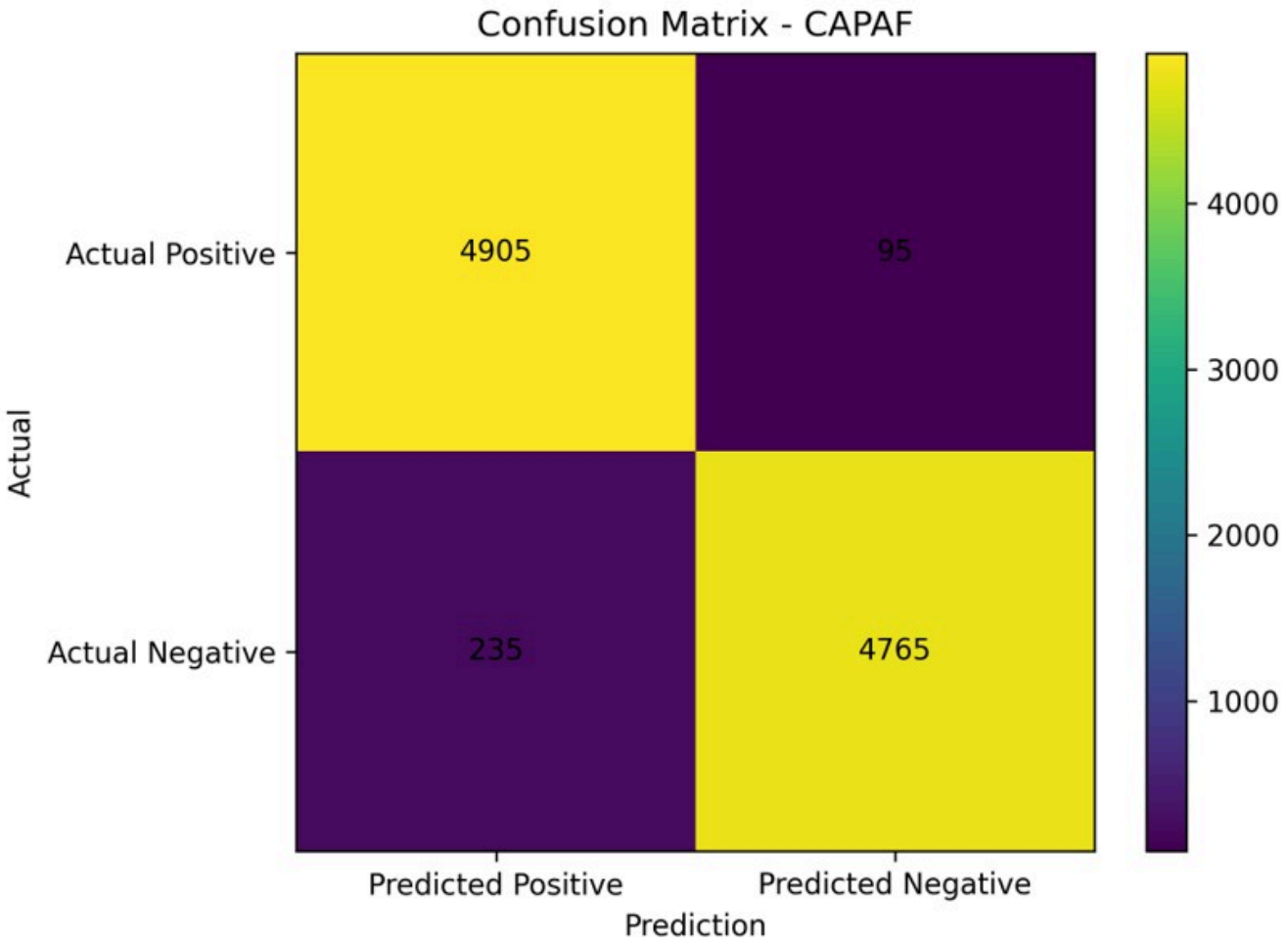


Figure 5

Confusion matrix of the CAPAF framework showing classification outcomes for access requests. The model achieves a high number of true positives and true negatives, with a significantly reduced false negative rate, demonstrating effective detection of unauthorized access attempts while maintaining acceptable false positive levels.

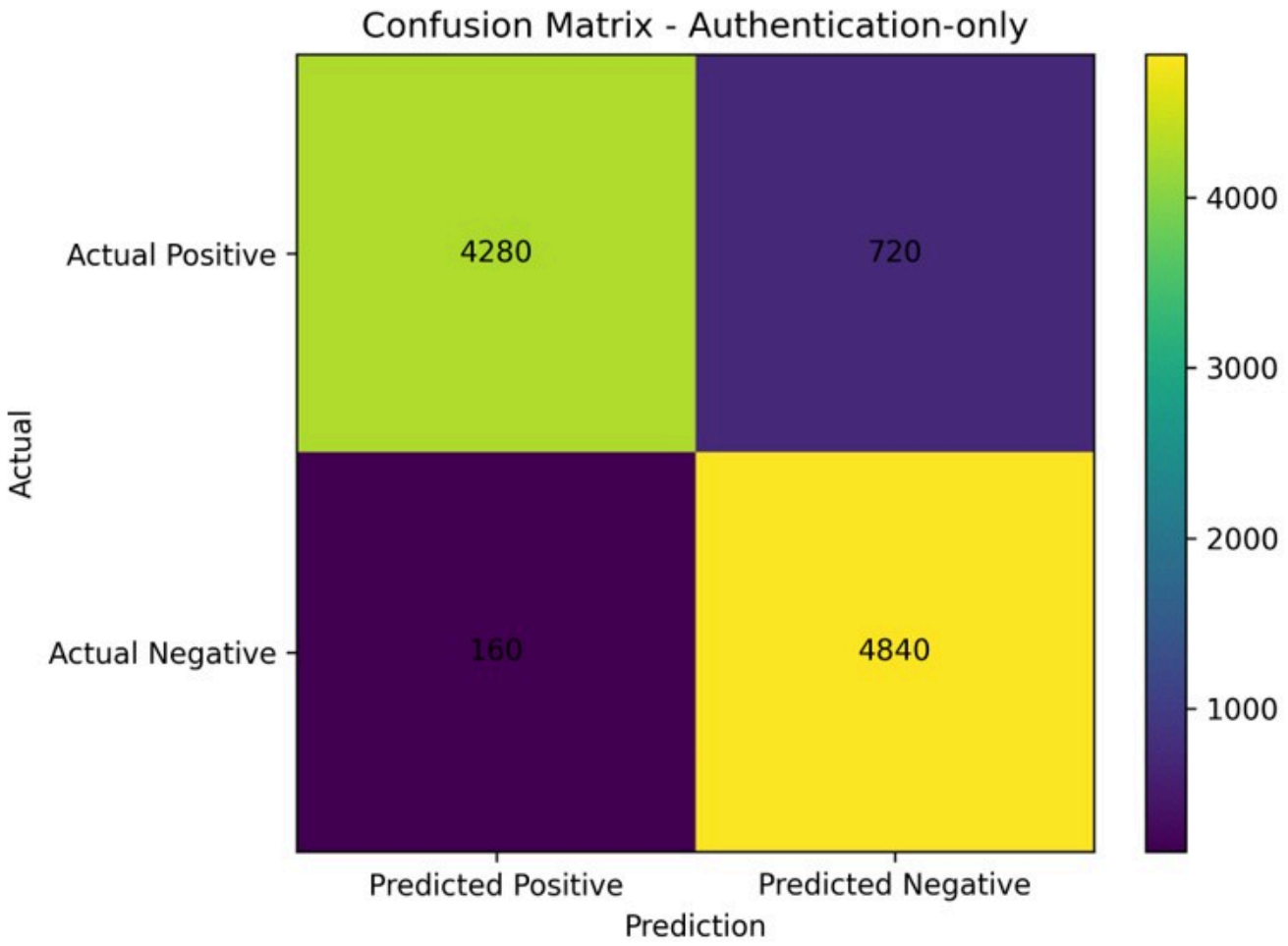


Figure 6

Confusion matrix of the authentication-only baseline model. The results indicate a higher false negative rate compared to CAPAF, highlighting the inability of traditional authentication mechanisms to detect malicious access attempts when valid credentials are used.

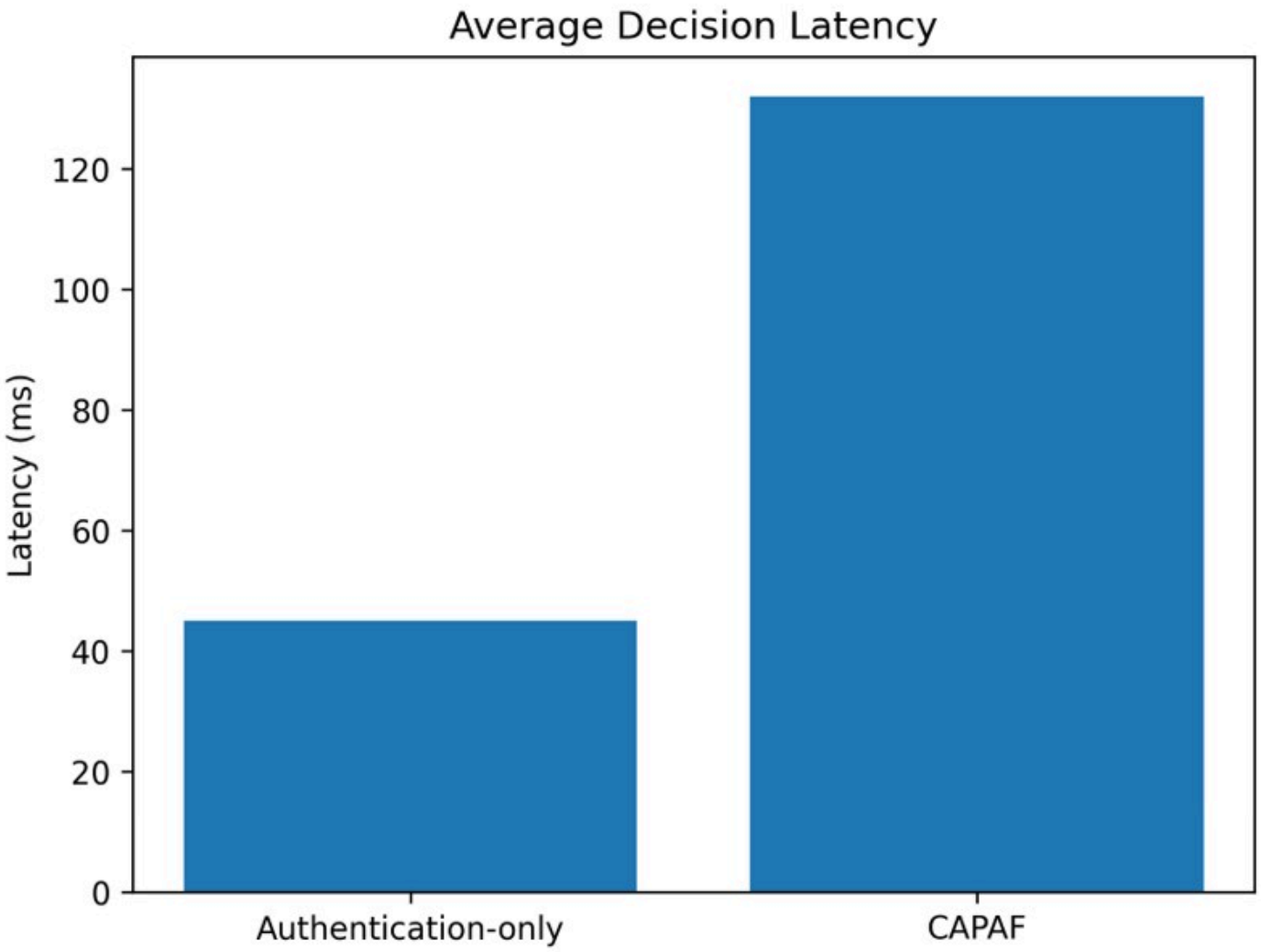


Figure 7

Average decision latency comparison between the authentication-only model and the CAPAF framework. The CAPAF model introduces additional processing time due to contextual risk evaluation; however, the latency remains within acceptable operational thresholds for enterprise systems.