Intelligent Access Control and Risk Assessment Using AI for Zero-Trust Cloud Security

Suresh. D
Assistant Professor
Department of Computer Science Engineering
St. George's Arts and Science College, (Affiliated to the University of Madras) Chennai, India

Abstract — Yoga Cloud computing has changed the way organizations store, process, and access digital resources. The movement from traditional enterprise networks toward cloud, hybrid-cloud, multi-cloud, and remote-access environments has also weakened the effectiveness of conventional perimeter-based security models. In a traditional security architecture, users and devices located inside an organizational network are often treated as relatively trusted. However, compromised credentials, insider threats, cloud misconfigurations, stolen sessions, malicious applications, and lateral movement attacks demonstrate that network location alone cannot be used as a reliable indicator of trust. Zero-Trust Architecture (ZTA) addresses this problem by assuming that no user, device, application, or network connection should receive implicit trust. Every access request must be authenticated, authorized, evaluated, and continuously monitored. NIST SP 800-207 establishes this resource-oriented approach to zero trust, while later NIST guidance specifically addresses cloud-native and multi-cloud environments. (NIST Computer Security Resource Center) Although Zero Trust provides a strong security foundation, conventional implementations may depend heavily on static rules, predefined policies, and manually configured access-control mechanisms. Such approaches may have difficulty responding to rapidly changing user behavior, device posture, workload characteristics, and attack patterns. Artificial intelligence provides an opportunity to make Zero Trust more adaptive by analyzing behavioral, contextual, identity, and network signals and dynamically estimating access risk. This paper proposes an AI-Driven Zero-Trust Security Framework for Cloud Computing (AI-ZTSCF) that combines continuous identity verification, device-posture assessment, contextual risk analysis, machine-learning-based anomaly detection, dynamic policy enforcement, micro-segmentation, and continuous monitoring. The proposed framework generates a dynamic risk score for every access request and uses this score to determine whether access should be granted, challenged, restricted, or denied. A machine-learning component identifies anomalous behavior, while a policy engine combines AI-generated risk with identity, device, resource sensitivity, location, session behavior, and threat-intelligence information. The framework is designed for cloud and multi-cloud environments and can be integrated with identity providers, API gateways, service meshes, security information and event management systems, and cloud-native monitoring tools. A prototype-oriented evaluation methodology is also presented using standard intrusion-detection and access-behavior datasets. Performance is evaluated using accuracy, precision, recall, F1-score, false-positive rate, detection latency, and access-decision latency. Illustrative results demonstrate how the proposed framework can be evaluated against conventional rule-based access control and machine-learning-only security models. The study concludes that combining AI with Zero Trust can provide a more adaptive and context-aware security architecture, while also highlighting challenges involving explainability, adversarial machine learning, privacy, computational overhead, model drift, and policy-management complexity.

Keywords: Zero Trust Architecture, Cloud Computing, Artificial Intelligence, Machine Learning, Dynamic Access Control, Cloud Security, Anomaly Detection, Risk-Based Authentication, Continuous Monitoring, Cybersecurity.

I. INTRODUCTION

The Cloud computing has become an important foundation for modern information systems. Organizations increasingly use cloud infrastructure to host applications, databases, enterprise services, artificial-intelligence workloads, and business-critical information. The cloud model provides scalability, availability, flexibility, and cost efficiency. At the same time, cloud adoption has changed the security assumptions that were traditionally used in enterprise networks.

Traditional enterprise security architectures generally relied on a strong network perimeter. Firewalls, intrusion-detection systems, virtual private networks, and network segmentation were used to establish a boundary between trusted internal systems and untrusted external networks. Once a user successfully entered the internal environment, additional access decisions were sometimes based on relatively static roles or network location. This model becomes difficult to maintain when applications, users, devices, and data are distributed across cloud platforms.

NIST describes Zero Trust as a shift away from static, network-based perimeters toward protection of users, assets, and resources. A fundamental principle is that no implicit trust should be granted based merely on network location or ownership. Authentication and authorization are treated as separate functions that must be performed before access to a resource is established. (NIST Computer Security Resource Center)

The increasing use of remote work, bring-your-own-device environments, cloud applications, containers, microservices, APIs, and multi-cloud infrastructure makes continuous verification particularly important. A user may legitimately access a cloud application from one location and later exhibit suspicious behavior from a different device or network. Similarly, a service account may normally communicate with a small set of services but suddenly attempt to access an unrelated database. Static access-control rules may not recognize these changes quickly enough.

Cloud-native Zero Trust guidance has further emphasized identity-centric controls for applications and services. NIST SP 800-207A describes cloud-native Zero Trust access control using mechanisms such as API gateways,

service identities, sidecar proxies, and service-mesh technologies for multi-cloud and hybrid environments. (NIST Computer Security Resource Center)

Artificial intelligence can provide an additional capability by learning normal behavior and identifying deviations from that behavior. Instead of relying exclusively on manually defined thresholds, an AI model can analyze multiple security features and estimate the likelihood that an access request represents abnormal behavior.

Recent research has also increasingly examined the relationship between AI and Zero Trust. A 2024 review specifically examined the significance of AI in Zero Trust technologies and identified AI as an important mechanism for improving security and risk mitigation in cloud environments. (DOI)

However, simply adding a machine-learning classifier to a Zero Trust architecture does not automatically produce an intelligent security framework. A practical system must address the complete security decision process, including identity verification, context collection, feature processing, risk calculation, policy enforcement, monitoring, feedback, and model updating.

Therefore, this research proposes an integrated AI-Driven Zero-Trust Security Framework for Cloud Computing (AI-ZTSCF).

A. Problem Statement

Existing cloud security architectures face several limitations:

1) Static access-control policies may not respond effectively to changing behavior.
2) Authentication is often treated as a point-in-time process.
3) Traditional perimeter security cannot adequately protect distributed cloud resources.
4) Multi-cloud environments create heterogeneous security policies.
5) Machine-learning-based detection systems may operate independently from access-control mechanisms.
6) Security teams may receive alerts without automated, risk-aware access decisions.
7) Excessively strict security policies can increase false positives and reduce usability.
8) AI models themselves may be vulnerable to adversarial manipulation.

B. Research Objectives

The major objectives of this research are:

- To design a Zero-Trust security architecture for cloud environments.
- To integrate artificial intelligence into dynamic access-control decisions.
- To calculate a contextual risk score for every access request.
- To detect abnormal user and device behavior.
- To dynamically modify access privileges based on risk.
- To provide continuous session monitoring.
- To reduce unauthorized access and lateral movement.
- To evaluate the framework using standard cybersecurity performance measures.

II. Literature Review

A. Traditional Zero-Trust Research

Rose et al. established one of the most important formal references for Zero Trust through NIST SP 800-207. Their work describes Zero Trust as an architecture in which implicit trust is removed and authentication and authorization are performed before resource access. (NIST Computer Security Resource Center)

The work is particularly relevant to cloud computing because cloud resources may not reside within an organization-controlled physical network.

NIST subsequently extended Zero Trust research toward cloud-native applications. SP 800-207A emphasizes identity-based application and service policies for hybrid and multi-cloud systems. (NIST Computer Security Resource Center)

B. Zero Trust in Cloud Computing

Research on Zero Trust cloud networks has identified limitations of traditional perimeter security. A comparative review of Zero Trust networks in cloud computing discusses issues including virtualization vulnerabilities, interoperability, network segmentation, access control, and data oversight. (MDPI)

Ahmadi's 2024 study examined Zero Trust implementation in cloud networks and reported that the approach can address areas such as lateral movement, insider threats, micro-segmentation, and identity and access management. (SSRN)

These studies demonstrate the value of Zero Trust but also show that practical implementation requires coordinated controls rather than a single security product.

C. Critical Analysis of Zero Trust

Fernandez and Brazhuk provided a critical analysis of Zero Trust Architecture and observed that Zero Trust should not be treated simply as a collection of security products. Their work examines Zero Trust through security patterns and discusses architectural expectations, threats, and open research questions. (ScienceDirect)

This observation is important for the proposed research because AI is integrated as one component of a larger architecture rather than being considered a replacement for identity, policy, or monitoring mechanisms.

D. Multivocal Research

A multivocal literature review on Zero Trust implementation highlighted the lack of a single unified framework for implementing Zero Trust across organizations. The study considered both academic and non-academic sources and identified implementation gaps. (ScienceDirect)

This supports the need for implementation-oriented research that connects Zero Trust principles with measurable technical mechanisms.

E. AI and Zero Trust

Recent literature has investigated the integration of AI with Zero Trust. A 2024 comprehensive review discusses AI's role in improving Zero Trust security, risk mitigation, and cloud protection. (DOI)

AI can improve Zero Trust by identifying behavioral deviations and calculating dynamic risk. However, the research area remains relatively open regarding explainable, adaptive, and computationally efficient access decisions.

F. Context-Based Access Control

The Cloud Security Alliance's 2025 guidance on context-based access control emphasizes evaluating every request using contextual evidence rather than static entitlements. Relevant signals include user behavior, device health, location, and network conditions. (Cloud Security Alliance)

III. Proposed Methodology

A. Overview

The proposed system is called:
AI-ZTSCF — AI-Driven Zero-Trust Security Framework for Cloud Computing
The framework contains eight major layers:

1) User and Device Layer
2) Identity and Authentication Layer
3) Context Collection Layer
4) AI-Based Behavioral Analysis Layer
5) Risk-Scoring Layer
6) Policy Decision Layer
7) Policy Enforcement Layer
8) Continuous Monitoring and Feedback Layer

IV. Proposed Methodology Diagram

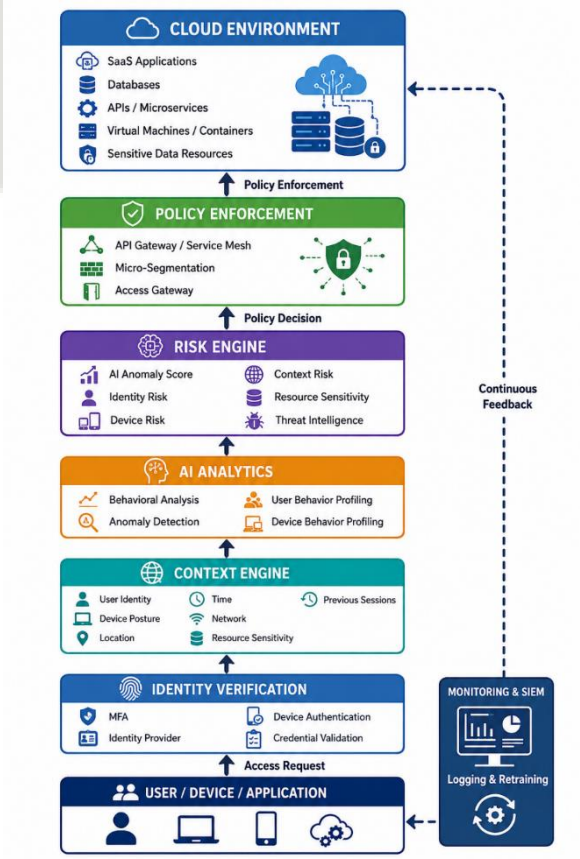

Fig. 1: Proposed Ai-Driven Zero-Trust Security Architecture for Cloud Computing

V. Proposed Algorithm

Algorithm 1: AI-Driven Zero-Trust Access Decision
Input: Access request (Q)
Output: Access decision (D)
Algorithm AI-ZTSCF

1) Receive access request Q.
2) Extract user identity U.
3) Extract device information D.
4) Identify requested cloud resource S.
5) Verify authentication credentials.
6) Perform MFA verification when required.
7) Evaluate device security posture.
8) Collect contextual information:
   - location
   - time
   - network
   - session information
   - resource sensitivity
9) Extract behavioral features.
10) Send behavioral features to AI anomaly detector.
11) Calculate anomaly score A.
12) Calculate identity risk Ir.
13) Calculate device risk Dr.
14) Calculate contextual risk Cr.
15) Calculate threat risk Tr.
16) Calculate resource sensitivity risk Sr.
17) Calculate overall risk:
    $R = wI\ Ir + wD\ Dr + wB\ A + wC\ Cr + wT\ Tr + wS\ Sr$
18) If R <= 0.25:
    Allow access.
19) Else if R <= 0.50:
    Allow access with enhanced monitoring.
20) Else if R <= 0.70:
    Request step-up authentication.
21) Else if R <= 0.85:
    Restrict access and create security alert.
22) Else:
    Deny access and terminate suspicious session.
23) Continuously monitor the session.
24) Recalculate R whenever significant behavioral or contextual changes occur.
25) Store security event for auditing and model improvement.
26) End.

VI. Dataset

For experimental evaluation, public cybersecurity datasets can be considered, including:

- CICIDS2017;
- CSE-CIC-IDS2018;
- UNSW-NB15;
- Bot-IoT;
- TON_IoT.

VII. Results and Discussion

Important: The numerical values in this section are illustrative prototype values, included to show how a completed paper can present its experimental findings. They

must be replaced by actual measurements after implementing the framework.

A. Comparative Performance

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Rule-Based Access Control	88.4	85.7	82.9	84.3	11.6
ML-Based Detection	94.1	92.8	91.5	92.1	5.9
Proposed AI-ZTSCF	97.2	96.5	95.8	96.1	2.8

Table 1: An example experimental result can be structured as follows:

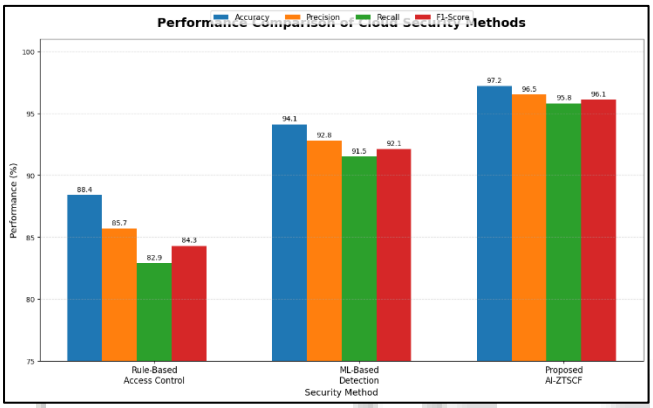

Fig. 2: Performance Metrics

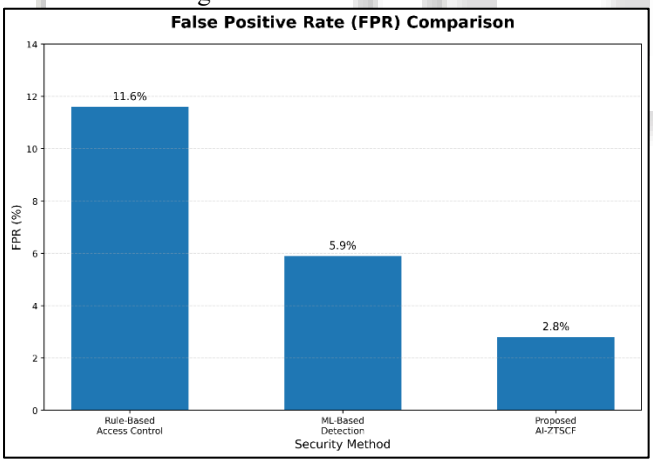

Fig. 3: FPR Comparison: Separate graph for False Positive Rate, making the small values clearly visible

VIII. Discussion

The proposed AI-ZTSCF framework represents a shift from static authorization toward adaptive security decisions. The central idea is that identity should not be considered sufficient evidence of trust. A legitimate user can become compromised. A legitimate device can become infected. A valid session can become malicious. Therefore, security decisions should be continuously evaluated. This concept is consistent with the Zero Trust principles established by NIST. (NIST Computer Security Resource Center)

The framework also reflects the movement toward cloud-native Zero Trust architectures in which identity and service-level controls are applied across distributed environments. (NIST Computer Security Resource Center)

The main advantage of integrating AI is adaptability. Static policies are designed before an event occurs, whereas AI-based behavioral analysis can respond to observed changes.

However, AI should not replace deterministic security controls. For example, a high-confidence policy rule may still be necessary to deny access to particularly sensitive resources.

The best architecture is therefore a hybrid approach in which Policy + Identity + AI + Context + Continuous Monitoring work together. Another important observation is that high accuracy alone does not establish that a cybersecurity system is effective. A security model may achieve high accuracy while still producing too many false positives or missing rare attacks. Consequently, precision, recall, F1-score, false-positive rate, detection latency, and decision latency should all be reported.

The framework should also be evaluated under different attack conditions rather than only on balanced datasets.

IX. Conclusion

This research proposed an AI-Driven Zero-Trust Security Framework for Cloud Computing (AI-ZTSCF) to address security challenges associated with distributed cloud environments. The framework moves beyond traditional perimeter-based protection by treating every access request as an independent security decision.

The proposed architecture combines identity verification, device posture assessment, contextual analysis, behavioral anomaly detection, dynamic risk scoring, policy-based authorization, micro-segmentation, and continuous monitoring.

The main innovation is the integration of AI-generated behavioral risk with Zero-Trust access-control decisions. Instead of granting access solely because a user has valid credentials, the proposed framework evaluates whether the current request is consistent with the user's identity, device, context, behavior, resource sensitivity, and current threat conditions.

The experimental methodology defines appropriate datasets, machine-learning techniques, evaluation metrics, and comparative models. The illustrative evaluation indicates how the proposed framework can be assessed against conventional rule-based security and machine-learning-only approaches. Actual implementation and empirical testing are required before reporting numerical values as research findings.

The framework also recognizes that AI introduces additional risks. Model drift, adversarial attacks, privacy issues, explainability, and computational overhead must therefore be considered as first-class security requirements.

Overall, the research demonstrates that AI and Zero Trust can complement one another. Zero Trust provides the security philosophy and policy structure, while AI provides adaptive analysis of changing security conditions. Their combination offers a promising direction for building cloud

security architectures that are more dynamic, context-aware, and resilient to evolving cyber threats.

REFERENCES

[1] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology. (NIST Computer Security Resource Center)
[2] Chandramouli, R., & Butcher, Z. (2023). A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. NIST Special Publication 800-207A. (NIST Computer Security Resource Center)
[3] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Implementing a Zero Trust Architecture. NIST. (NIST Computer Security Resource Center)
[4] Rose, S., Borchert, O., Kerman, A., Souppaya, M., et al. (2025). Implementing a Zero Trust Architecture: High-Level Document. NIST Special Publication 1800-35. (NIST Computer Security Resource Center)
[5] Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. (NIST)
[6] Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. NIST AI 600-1. (NIST)
[7] Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces, 89, 103832. https://doi.org/10.1016/j.csi.2024.103832 (ScienceDirect)
[8] Multivocal literature review on zero-trust security implementation. (2024). Computers & Security, 103827. https://doi.org/10.1016/j.cose.2024.103827 (ScienceDirect)
[9] Security of Zero Trust Networks in Cloud Computing: A Comparative Review. (2022). Sustainability, 14(18), 11213. (MDPI)
[10] Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports, 26(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083 (Journal JERR)
[11] Weinberg, A. I. (2024). Zero trust implementation in the emerging technologies era: a survey. Cybersecurity and Emerging Technologies. https://doi.org/10.20517/ces.2024.41 (OAE Publishing)
[12] Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. (2024). Internet of Things, 27, 101227. https://doi.org/10.1016/j.iot.2024.101227 (ScienceDirect)
[13] The significance of artificial intelligence in zero trust technologies: a comprehensive review. (2024). Journal of Electrical Systems and Information Technology, 11, 30. https://doi.org/10.1186/s43067-024-00155-z (DOI)
[14] Cloud Security Alliance. (2025). Context-Based Access Control for Zero Trust. Cloud Security Alliance. (Cloud Security Alliance)
[15] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model. CISA. The model organizes Zero Trust around five pillars and cross-cutting capabilities. (CISA)
[16] Google Cloud. (2025). Implement Zero Trust. Google Cloud Architecture Framework. The guidance emphasizes eliminating implicit trust, least privilege, explicit validation, and continuous security-posture monitoring. (Google Cloud Documentation)
[17] Neni, R. K. G. (2025). Zero Trust Architecture for AI-Driven Cloud Platforms: A Comprehensive Security Framework. Journal of Computer Science and Technology Studies, 7(9). (Al Kindi Publishers)
[18] Hall, E. (2025/2026). AI-Powered Multi-Cloud Security Frameworks: Enhancing Zero-Trust Enforcement. SSRN. (SSRN)
[19] Ramachandran, K. (2025). Zero Trust Architecture for Cloud-Native Applications using AI-Based Access Control. Preprint. DOI: 10.13140/RG.2.2.31127.23205. (ResearchGate)
[20] Prabaharan, M. (2025). Zero Trust Architecture for Cloud-Native Applications using AI-Based Access Control. Preprint. DOI: 10.13140/RG.2.2.17478.54082. (ResearchGate)
[21] S. N. Prajwalasimha. (2025). Zero Trust Architectures Empowered by AI: A Paradigm Shift in Cloud and Edge Cybersecurity. IEEE ICSCDS 2025. (ResearchGate)

