International Journal of Research in Engineering, Science and Management
Volume 9, Issue 4, April 2026
www.ijresm.com | E-ISSN: 2581-5792 | RESAIM Publishing | www.resaim.com

ZTNA – Zero Trust Network Access

Raj Ganesh Patil[1*], Sairaj Dattu Unde[1], Sakshi Prashant Sanas[1], Riya Rakesh Sanap[1], Mridul Saxena[1]
[1]*Department of Artificial Intelligence and Data Science, University of Mumbai, Navi Mumbai, India*

***Abstract*: Zero Trust Network Access (ZTNA) is a modern cybersecurity approach that addresses the weaknesses of traditional perimeter-based security models that rely on implicit trust. This project proposes an AI-driven ZTNA framework that enhances security through strict identity verification and continuous monitoring. The system uses artificial intelligence and machine learning to analyze user behavior, device health, and contextual data in real time to make risk-based access decisions. It integrates multi-factor authentication, policy-based access control, and anomaly detection to prevent unauthorized access. The framework also enables secure remote access and improves overall network security and access management.**

***Keywords*: Zero Trust Network Access, Cybersecurity, Artificial Intelligence, Machine Learning, Identity-Based Access Control, Continuous Authentication, Cloud Security, Anomaly Detection, Real-Time Monitoring, Network Protection.**

1. Introduction

In today's digital environment, securing access to or- ganizational resources has become challenging due to increasing cyber threats such as insider attacks and cre- dential theft. Traditional perimeter-based security mod- els rely on implicit trust, which often creates serious security vulnerabilities, especially with the rise of cloud computing and remote work.

Zero Trust Network Access (ZTNA) addresses this is- sue through the principle of "never trust, always verify," ensuring continuous authentication and authorization of users and devices. This project proposes an AI-driven ZTNA framework that uses artificial intelligence and machine learning for behavioral analysis, real-time mon- itoring, and intelligent access control, providing a more secure and scalable network security solution.

Adaptive and Context-Aware Defense: Beyond sim- ple authentication, this framework introduces dynamic risk assessment, where access is not a one-time event but a continuous evaluation. By analyzing contextual signals—such as login time, geographic location, and device health—the AI can automatically adjust permissions or trigger additional security layers the moment ananomaly is detected, effectively neutralizing threats like lateral movement before they reach sensitive data.

A. Existing Systems and their Limitations

Table 1
Existing systems and their limitations

Approach	Limitation
Traditional VPNs	Provides broad network-level access, facilitating lateral movement for insider threats.
Static Firewalls	Rule-based only; fails to adapt to evolving threats or understand user behavior.
Manual Access Control	Time-consuming and inconsistent; lacks the scalability needed for dynamic environments.

B. Problem Statement, Aim & Objectives

The AI-driven Zero Trust Network Access (ZTNA) system is designed to overcome the limitations of traditional network security by integrating artificial intelligence with advanced access control mechanisms. The system ensures secure, real-time, and context-aware access to organizational resources by implementing strong identity verification, contin- uous authentication, and secure communication across cloud and hybrid environments.

1) Problem Statement: Traditional security models and Virtual Private Networks (VPNs) rely on perimeter-based protection and implicit trust once a user gains access. This approach makes systems vulnerable to insider threats, cre-dential misuse, and lateral movement attacks. Additionally, these solutions lack intelligent automation for continuous verification and real-time threat detection. The proposed sys-tem addresses these issues by developing an AI-powered ZTNA platform that provides context-aware access control, continuous monitoring, and real-time threat detection.

2. System Architecture

The AI-Based Behavioral Analysis Module analyzes user activity patterns using machine learning to detect anomalies such as unusual login times or suspicious access requests.

The system also applies micro-segmentation, allowing users to access only specific applications rather than the entire network, which reduces the attack surface. All activities are recorded by the Monitoring and Logging Module, while the Reporting Dashboard provides administrators with insights, alerts, and security reports.

This modular design allows easy integration of new policies, authentication methods, or AI models, ensuring a flexible, adaptive, and secure network access system.

A. Algorithm and Process Design

Key Interactions:

*Corresponding author: rajpatil.rp9892@gmail.com

- *User Input:* Users initiate access requests through web applications, enterprise systems, or cloud platforms, which serve as the starting point for the ZTNA process.
- *System Integration:* The ZTNA framework integrates with enterprise directories, cloud services, and identity providers to fetch user data, roles, and authentication credentials.
- *AI Security Engine:* A machine learning-based module analyzes user behavior and detects anomalies, enabling intelligent and adaptive access control decisions.
- *Access Control & Verification:* The system enforces strict identity verification and ensures that only authorized users gain access to specific resources based on policies.
- *Micro-Segmentation (Feature):* Restricts access to only required applications or services instead of providing full network access, reducing the attack surface.
- *Continuous Authentication (Feature):* Regularly re-assesses user trust levels during active sessions to prevent unauthorized access.

B. Administrator Dashboard

- Provides a centralized interface for monitoring system activity, managing policies, and responding to security incidents.
- *Security Analytics & Reporting:* Generates detailed insights on user activity, threat detection, and system performance to support informed decision-making.
- *Incident Response Mechanism:* Automatically triggers alerts, access revocation, or additional verification steps when suspicious activity is detected.
- *Scalability & Cloud Support:* Ensures seamless deployment across cloud, hybrid, and on-premise environments, supporting organizational growth and flexibility.

3. Algorithm and Process Design

A. Algorithm Design

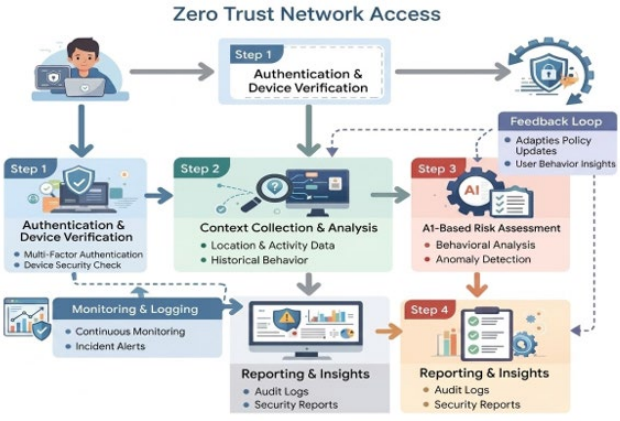

Fig. 1. Algorithm design – Zero Trust Network Access

Step 1: User Authentication and Device Verification

- *Input:* User credentials, device information, and access request.
- *Goal:* Verify identity and ensure device compliance before granting access.
- *Algorithm:* Multi-Factor Authentication (MFA) + de-vice posture assessment (OS status, antivirus, security patches).
- *Output:* Authenticated user and verified device status.

Step 2: Context Collection and Preprocessing

- *Input:* Authenticated user data and device details.
- *Goal:* Collect contextual information for decision-making.
- *Algorithm:* Data aggregation of user role, location, access time, and historical activity logs.
- *Features*: User identity, geolocation, login patterns, de- vice trust level.
- *Output:* Structured contextual dataset for analysis.

Step 3: AI-Based Risk Assessment

- *Input:* Contextual data + user behavior history.
- *Goal:* Evaluate risk level of the access request.
- *Algorithm:* Machine Learning models (e.g., anomaly detection, classification models).
- *Process:* Analyze patterns and compare with normal behavior to detect anomalies.
- *Output:* Risk score and anomaly indicators (e.g., suspicious login, unusual access request).

Step 4: Policy Evaluation and Access Decision

- *Input:* Risk score + contextual dataset.
- *Goal:* Decide whether to grant, deny, or restrict access.
- *Algorithm:* Rule-based Policy Engine (RBAC/ABAC) with dynamic risk-based conditions.
- *Output:* Access decision (Allow/Deny/Conditional Access).

Step 5: Continuous Monitoring and Session Control

- *Input:* Active user session.
- *Goal:* Ensure ongoing security after access is granted.
- *Algorithm:* Real-time monitoring with behavioral tracking and anomaly detection.
- *Output:* Alerts, re-authentication triggers, or session termination if suspicious activity is detected.

Step 6: Logging and Reporting

- *Input:* Access decisions and system activity logs.
- *Goal:* Maintain audit trails and provide insights for administrators.
- *Integration:* Dashboard and reporting systems.
- *Output:* Security reports, alerts, and analytics.

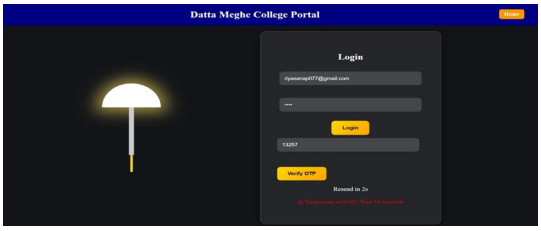

Fig. 2. Login page

B. *Process Design – Data Flow*

- *User Input:* User initiates access request via web application, enterprise system, or cloud platform.
- *Preprocessing:* Authentication and device verification performed → validated identity and device trust level.
- *Context Analysis:* Collection of contextual data such as location, time, role, and previous activity.
- *AI Risk Evaluation:* Machine learning-based analysis to detect anomalies and assign risk score.
- *Continuous Monitoring:* Ongoing session tracking to detect suspicious behavior in real time.
- *Report Consolidation:* Combine logs, alerts, and system insights into structured reports.
- *Feedback Output:* Deliver results through dashboards, alerts, notifications, or downloadable reports.

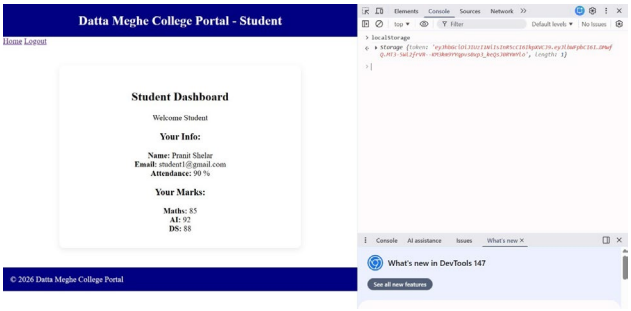

Fig. 3. Dashboard and tokens

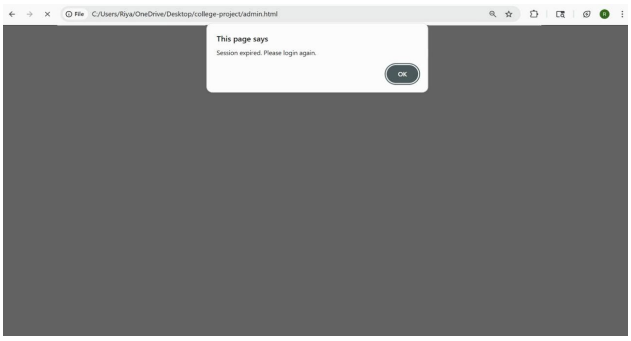

Fig. 4. Token session timeout

Table 2
Challenges and solutions

Challenges	Solution (AI-Driven ZTNA)
Implicit Trust	*Explicit Verification:* Enforces "Never Trust, Always Verify" for every request.
Broad Exposure	*Granular Access:* Limits access to specific, authorized applications only.
Static Login	*Continuous Monitoring:* Real-time session analysis to detect active hijacking.
Identity-Only	*Context-Aware AI:* Evaluates behavioral patterns and device health dynamically.
Visible Assets	*Invisible Infrastructure:* Resources remain "dark" and hidden from unauthorized users.

The Fig. 3, illustrates a token-based authentication and authorization flow within a Zero Trust framework. It depicts a sequence where a user requests access, triggers a validation process (likely via MFA or device health checks), and receives a secure token that grants granular, time-bound permission to specific applications rather than the entire network. This ensures that every session is explicitly verified and isolated, preventing unauthorized lateral movement.

Table 3
Software stack

Component	Technologies and Tools
Frontend	HTML, CSS, JavaScript
Backend	Python, Flask, FastAPI
AI Engine	GroQ
Integration	GitHub API
Deployment	Docker, Render / Vercel

4. Conclusion and Future Scope

A. *Conclusion*

In this work, we presented an AI-driven Zero Trust Network Access (ZTNA) system designed to improve modern cybersecurity through strict identity-based access control and continuous verification. The system uses artificial intelligence and machine learning to analyze user behavior, assess risk in real time, and provide secure access to organizational resources. By replacing traditional perimeter-based security models with a dynamic and adaptive framework, the system reduces the risk of unauthorized access and cyber threats.

The proposed solution integrates identity verification, device validation, behavioral monitoring, and policy-based access control into a unified framework. It ensures that users access only authorized resources based on contextual factors such as role, location, and device status. Continuous monitoring and centralized reporting enable administrators to detect anomalies and respond quickly. Overall, the project demonstrates that combining AI with Zero Trust principles can enhance network security, improve operational efficiency, and provide a scalable solution for modern distributed environments.

B. *Future Scope*

Enhanced AI Models: Improve behavioral analysis and anomaly detection using advanced and adaptive AI techniques.

Multi-Platform Integration: Support seamless integration with cloud platforms and enterprise systems.

Threat Intelligence: Use predictive analytics to detect and prevent emerging threats.

Automated Incident Response: Enable automatic blocking and quick response to suspicious activities.

IoT Security Support: Extend Zero Trust security to IoT devices and connected systems.

Improved Dashboard: Provide better visualization and real-time monitoring for administrators.

References

[1] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," Forrester Research, 2010.

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, NIST Special Publication 800-207, 2020.

[3] Google, "BeyondCorp: A new approach to enterprise security," Google Research, 2014.

[4] J. Shin *et al.*, "Behavior-based authentication for continuous security," *IEEE Security & Privacy*, vol. 15, no. 5, pp. 50–57, 2017.

[5] V. C. Hu, D. Ferraiolo, and D. Kuhn, "Attribute-based access control," National Institute of Standards and Technology, 2014.

[6] M. Almorsy, J. Grundy, and A. S. Ibrahim, "Collaboration-based cloud computing security management framework," in *Proc. IEEE International Conference on Cloud Computing*, 2012.

[7] E. Bertino, F. Paci, and R. Ferrini, "Identity and access management in open cloud computing," in *Proc. IEEE International Conference on Cloud Computing*, 2011.

[8] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[9] A. Behl and K. Behl, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, U.K.: Oxford University Press, 2017.

[10] M. A. Khan *et al.*, "Machine learning-based network security frameworks: A review," *Journal of Network and Computer Applications*, vol. 150, Art. no. 102439, 2020.