

A BLUE PRINT FOR ZERO TRUST NETWORK ARCHITECTURE: AN INSTITUTIONAL DATA SECURITY AT FEDERAL POLYTECHNIC, MUBI, ADAMAWA STATE NIGERIA

BULUS Lucy Dalhatu, KOIRANGA Abdullah Hammanadama & AARON, Catherine Madunagu

Department of Computer Science, Federal Polytechnic, PMB35, Mubi Adamawa State, Nigeria

*buluslucy08@gmail.com, +2348137764425**
koiranga.ab@gmail.com, +2347067609361
kateenyeomadunagu@gmail.com, +2348063327793

ABSTRACT

Traditional cloud network security relies heavily on perimeter-based firewalls and legacy Virtual Private Networks (VPNs). Empirical industry evidence indicates that over 80% of enterprise data breaches, compromised credentials and subsequent unauthorized lateral movement across internal subnets. *This paper proposes a blue print for Zero Trust Network Architecture (ZTNA) plan aimed at Federal Polytechnic Mubi in Adamawa State, Nigeria. In the design, the system incorporates a centralized Policy Decision Point (PDP) and Policy Enforcement Point (PEP), development access verification engine that evaluates user identity claims, Multi-Factor Authentication (MFA) tokens in real time. Zero-Trust Network Architecture engine eliminates implicit trust, verifies every session contextually, and enforces continuous least-privilege micro-segmentation to secure cloud-hosted corporate storage. The Federal Polytechnic, Mubi system tested automatically auditing login subsystem to record session evaluations, security rule violations, and access denials for compliance tracking. Zero-Trust Network Architecture (ZTNA) engine decouples traditional perimeter access management into a modular, multi-tier control plane and data plane model. The system operates by shifting access management away from static perimeter security toward continuous, context-aware policy enforcement. When an access request is initiated, the Identity Provider (IdP) first verifies user credentials and Multi-Factor Authentication (MFA) token status. This context payload is transmitted to the Policy Decision Point (PDP), which dynamically evaluates the multi-attribute risk parameters against predefined security rules. Every execution generates structured event telemetry containing reason codes and session metadata, which is immediately dispatched to the Security Information and Event Management (SIEM) audit console. The core result of the developed Zero-Trust Network Architecture (ZTNA) control engine is captured in the single-page interactive control dashboard. The interface integrates the Context Ingestion Panel (Input Form), the Dynamic Architecture Verification Pathway (Topology Node Map), and the Real-Time SIEM Event Telemetry Console (Audit Log Output) into a unified operational view. As demonstrated in the system logic of Figure 3, if a subject authenticates under a standard user account but manually selects Corporate Administrator from the dropdown list, the Policy Decision Point (PDP) compares the client payload against the authoritative IdP record. Detecting a discrepancy between the assigned identity and the claimed role, the engine immediately terminates the evaluation, outputs an ERR_ROLE_SPOOFING_DETECTED result, and flags the session as a privilege escalation attack.*

Keywords: Blue Print, Zero-Trust, Network, Architecture, Institution, Data, Security

INTRODUCTION

The rapid global adoption of distributed cloud computing infrastructures-encompassing Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service-has completely dissolved this traditional network perimeter. Enterprise data assets are no longer confined within a

single physical building; rather, they are hosted across multi-cloud environments and accessed by remote employees operating from diverse locations using personal endpoints and public communication channels. In this decentralized operational reality, continuing to rely on static perimeter security introduces severe architectural vulnerabilities, as the physical perimeter no longer exists to contain threat vectors. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource (Rose *et al.*, 2020).

The primary structural vulnerability of legacy perimeter security lies in its granting of default implicit trust (Rose *et al.*, 2020). When an unauthorized actor or malicious program breaches an edge firewall—whether through stolen credentials, social engineering, or unpatched software—the absence of internal barriers allows the attacker to traverse adjacent subnets unhindered (Buck *et al.*, 2021). This capability to move laterally across internal databases enables bad actors to escalate privileges and ex-filtrate highly confidential corporate data. Traditional perimeter gateways fail to conduct continuous contextual evaluation, such as checking endpoint health status or verifying Multi-Factor Authentication tokens after initial session creation (Rose *et al.*, 2020).

To address these vulnerabilities, cyber-security researchers developed the Zero-Trust Network Architecture framework (Rose *et al.*, 2020). Formally standardized by the National Institute of Standards and Technology under Special Publication 800-207, Zero-Trust operates on the foundational governing principle of "never trust, always verify" (Rose *et al.*, 2020). Zero-Trust explicitly rejects location-based security assurances (Garbis & Chapman, 2021).

Problem Statement

Traditional cloud network security relies heavily on perimeter-based firewalls and legacy Virtual Private Networks (VPNs) that grant implicit, unrestricted trust to users upon initial login. Empirical industry evidence indicates that over 80% of enterprise data breaches stem from compromised credentials and subsequent unauthorized lateral movement across internal subnets.

Continuing to operate perimeter security models in distributed cloud environments exposes enterprise databases to ransomware deployment, privilege escalation, and exfiltration of sensitive payroll and financial records. Therefore, this paper is justified by the urgent need to design, build, and deploy an automated Zero-Trust Network Architecture engine that eliminates implicit trust, verifies every session contextually, and enforces continuous least-privilege micro-segmentation to secure cloud-hosted corporate storage.

Aim and Objectives

The aim of this paper is to design, develop, and deploy a Zero-Trust Network Architecture system for cloud-hosted corporate data to eliminate implicit network trust and enforce real-time, context-aware access verification in Federal Polytechnic, Mubi. The specific objectives are to:

- i. Design a structured Zero-Trust access verification architecture incorporating a centralized Policy Decision Point (PDP) and Policy Enforcement Point (PEP) framework.
- ii. Develop an interactive access verification engine that evaluates user identity claims, Multi-Factor Authentication (MFA) tokens, endpoint device health posture, and target resource authorization tiers in real time.
- iii. Test the automated audit logging subsystem to record session evaluations, security rule violations, and access denials for compliance tracking.

RELATED WORK

The transition from traditional, localized computing boundaries to elastic multi-cloud environments has reshaped enterprise cyber security project (Buck *et al.*, 2021). As corporate applications and sensitive database repositories migrate to remote infrastructure, security researchers have conducted extensive studies to identify access control vulnerabilities, evaluate modern threat vectors, and propose architectural mechanisms for identity verification (Garbis & Chapman, 2021).

Asheshemi and Adawaren (2026), stated that, rapid digital transformation of the financial sector in Nigeria has been characterized by increased dependence on cloud-based infrastructures which lead to cybersecurity challenges. Various manners of attack, such as compromised credentials and unauthorized access enabled by weak identity management systems, have arguably remained some of the most pervasive and destructive problems. In their study, they adopts a sequential explanatory mixed-methods design, a blockchain-based Zero Trust which demonstrating trust-independent defense model adequate for digital finance.

Some research seeks to optimize material usage, energy consumption, and waste management, through overarching goal of achieving net-zero environmental impact. The circular economy principles, which prioritize resource efficiency, waste reduction, and life cycle considerations, form the core foundation of the framework. The key components of any framework, emphasizes the synergies between data driven methodologies and circular economy principles. Some holistic framework that guide architects, educators, and industry stakeholders towards a future where net-zero aspirations are not only achievable but integral to the spirit of architectural innovation and environmental stewardship. The advancement of net-zero goals within the architectural field, provides an accessible framework for sustainable design practices, (Sevindik, *et al.*, 2024).

It is a clear consensus among modern cybersecurity scholars regarding the fundamental inadequacy of traditional, perimeter-based access control models (Garbis & Chapman, 2021; Rose *et al.*, 2020). Prior research establishes that implicit trust granted at edge firewalls and VPN gateways is the leading structural cause of lateral threat movement, credential exploitation, and enterprise data exfiltration in cloud environments (Buck *et al.*, 2021; Cunningham, 2021). While theoretical frameworks such as NIST SP 800-207 (Rose *et al.*, 2020), Forrester ZTX (Cunningham, 2021), and Gartner CARTA provide comprehensive conceptual standards for Zero-Trust adoption, the extant literature reveals significant gaps (Raghuvar, 2-25).

The majority of existing studies analyze authentication factors in isolation focusing either strictly on identity credentials (Cunningham, 2021), network layer routing rules (Arunkumar, 2022), or dynamic risk scores. There is a lack of accessible, software-implemented reference engines that synthesize user identity, Multi-Factor Authentication tokens, endpoint device posture, and target resource sensitivity tiers into a single, unified access decision pipeline.

According to Gambo & Almulhem (2025), Most of the existing research focuses on high-level theory papers or evaluations of private company software. There is still a lack of easy-to-use, open, and interactive software that clearly shows how Policy Decision Point (PDP) and Policy Enforcement Point (PEP) change states, how paths are built dynamically, and how real-time security information and event management (SIEM) audit logs work, which is needed for academic study and analysis. In this paper, we tackle these identified gaps by creating, building, and testing an interactive Zero-Trust Network Architecture engine (Adamson, 2025). This engine combines multi-attribute context verification, application-layer micro-segmentation, and automated compliance event telemetry within a single cloud storage security framework designed for Federal Polytechnic, Mubi.

METHODOLOGY

The paper analyzed, and designs a blue print of Zero-Trust Network Architecture (ZTNA) system for cloud-hosted corporate storage. Analysis of the existing perimeter-based security model of Federal Polytechnic, Mubi was carried out. This is to highlight its inherent operational vulnerabilities and structural limitations.

Following the analysis of the existing system, the requirement specifications, architectural framework, and logical workflows of the proposed Zero-Trust verification engine was done.

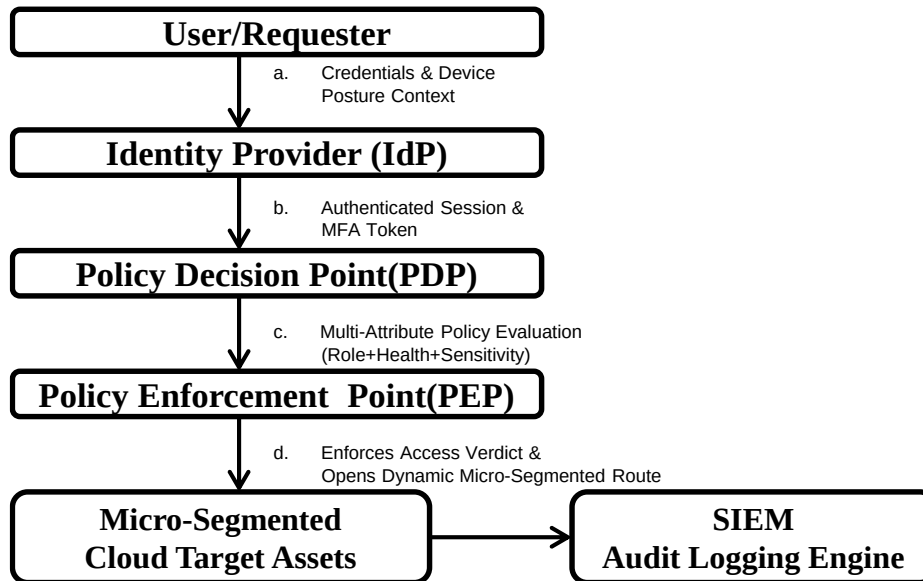
Furthermore, the paper outlines the structural decomposition of the new system, including the Policy Decision Point (PDP), Policy Enforcement Point (PEP), and Identity Provider (IdP) module interaction pipelines. It also details the data flow diagrams, algorithmic decision logic, micro-segmentation access control matrix-a technical reference table that maps who (users, devices, or service accounts) can access what (cloud storage, databases, administrative tools) and under what conditions., database schemas, and user interface design specifications required to build and deploy the application-layer security solution.

The primary data collection method adopted in this paper is Interactive Security Simulation and System Threat Modeling.

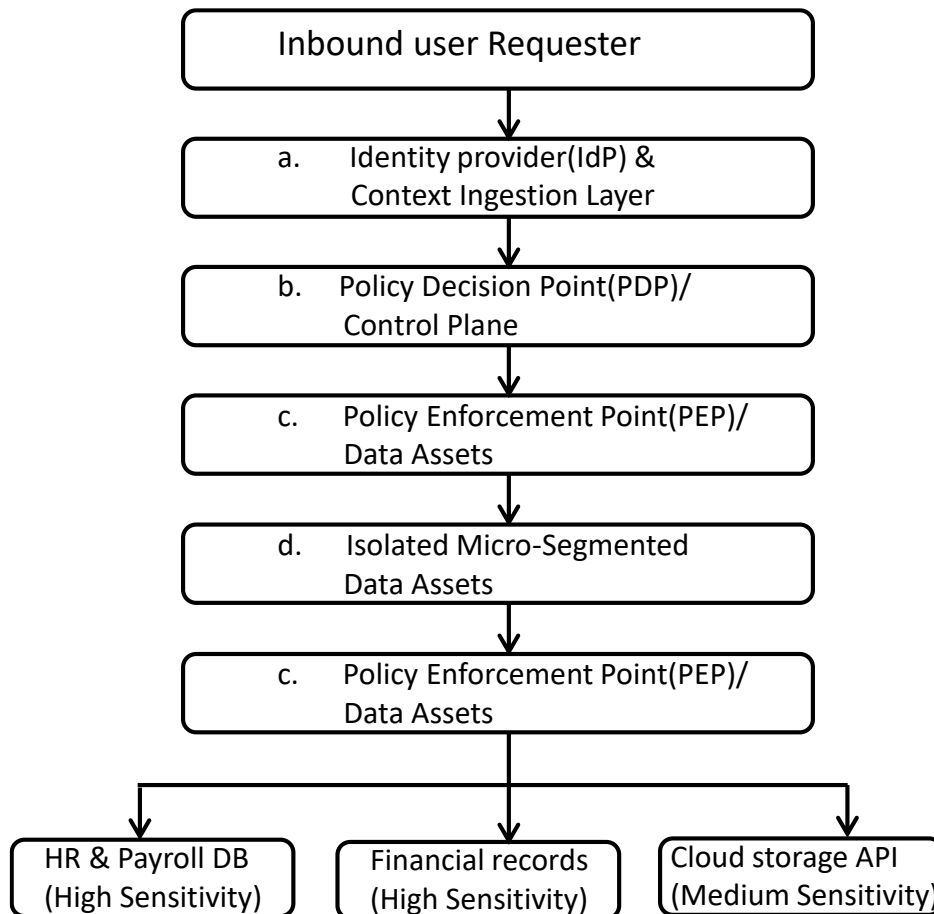
- i. Direct Capture of Real-Time System Telemetry was done.
- ii. Replicability and Controlled Threat Testing: Simulating access control scenarios provides a controlled environment to safely test malicious behaviors, such as unauthorized lateral movement, non-compliant endpoint connection attempts, and credential theft attempts, without exposing live enterprise cloud infrastructure to operational risks.
- iii. Direct Validation of System Objectives: We focuses on building an active decision pipeline-comprising an Identity Provider (IdP), Policy Decision Point (PDP), and Policy Enforcement Point (PEP)-experimental data collection is the only method that directly measures whether the access engine correctly processes dynamic context parameters to enforce the Principle of Least Privilege.

System Design

In the system design, we define the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements., The system design bridges the gap between theoretical Zero-Trust requirements and technical implementation by decoupling access management into a three-tier control plane architecture comprising an Identity Provider (IdP), a Policy Decision Point (PDP), and a Policy Enforcement Point (PEP).



- vi. tware components, their properties, and the relationships between them. The architecture of the Zero-Trust Network Architecture (ZTNA) engine decouples traditional perimeter access management into a modular, multi-tier control plane and data plane model.
- vii. The architecture isolates the target data assets within micro-segmented zones and routes all inbound access requests through three distinct operational layers.
- viii. Validates primary user credentials, verifies Multi-Factor Authentication (MFA) tokens, and collects real-time endpoint device posture telemetry.
- ix. The system Evaluates collected context attributes against dynamic security policies to compute dynamic risk scores and generate an access decision verdict (Grant or Deny).
- x. Policy Enforcement Point receives authorization verdicts from the PDP, provisions isolated session pathways to specific micro-segmented cloud assets, and dispatches real-time event logs to the Security Information and Event Management (SIEM) audit database.



RESULTS AND DISCUSSION

The system operates by shifting access management away from static perimeter security toward continuous, context-aware policy enforcement. When an access request is initiated, the Identity Provider (IdP) first verifies user credentials and Multi-Factor Authentication (MFA) token status. Concurrently, endpoint device telemetry—including active antivirus protection, operating system patch levels, and storage encryption—is ingested alongside the target resource sensitivity tier.

This context payload is transmitted to the Policy Decision Point (PDP), which dynamically evaluates the multi-attribute risk parameters against predefined security rules. Depending on the evaluation verdict, the Policy Enforcement Point (PEP) either provisions an isolated micro-segmented access route to the target asset or blocks the connection path entirely. Every execution generates structured event telemetry containing explicit reason codes and session metadata, which is immediately dispatched to the Security Information and Event Management (SIEM) audit console. The core result of the developed Zero-Trust Network Architecture (ZTNA) control engine is captured in the single-page interactive control dashboard. The interface integrates the Context Ingestion Panel (Input Form), the Dynamic Architecture Verification Pathway (Topology Node Map), and the Real-Time SIEM Event Telemetry Console (Audit Log Output) into a unified operational view. Main Single-Page User Interface of the Zero-Trust Network Architecture Engine Illustrating the Zero-Trust architecture dynamically evaluating identity, device health, and permission to enforce secure cloud access

Zero-Trust Network Architecture (ZTNA) Control Engine
Section 3.6 Implementation Model — Zero-Trust Policy Decision & Enforcement Verification Engine

Context Ingestion Panel (PDP Inbound Payload)

1. Identity & Role Context:
Corporate Administrator (Full Privileges)

2. Multi-Factor Authentication (MFA) Status:
Verified / Token Active

3. Endpoint Device Posture Checks:
☒ Active & Updated Antivirus Engine
☒ OS Patch Level Compliant
☒ BitLocker / Storage Encryption Active

4. Target Cloud Asset Request:
Public Web Storage (Low Sensitivity)

Evaluate Policy & Enforce Access

System Architecture & Verification Pathway

Untrusted Request Source

1. Identity Provider (IdP)

2. Policy Decision Point (PDP)

3. Policy Enforcement Point (PEP)

4. Micro-Segmented Cloud Target

Real-Time SIEM Event Telemetry Engine

```
[SYSTEM_STARTUP] Policy Decision Point (PDP) dynamic engine initialized. Monitoring entry subnets...
```

Figure 3: Main Single-Page User Interface of the Zero-Trust Network Architecture Engine.

The results displayed in Figure 3 demonstrate the practical operation, verification pipeline, and security enforcement mechanisms of the Zero-Trust Network Architecture (ZTNA) control plan. By removing the concept of implicit trust, the system evaluates incoming access requests using multi-attribute contextual parameters before establishing dynamic network pathways. The interface integrates several distinct functional zones that continuously analyze incoming access requests and provide real-time feedback.

The top-left panel of Figure 3 captures primary identity attributes alongside the requested operational role. The system integrates an in-memory database simulating an enterprise Identity Provider (IdP) that maintains cryptographic user records containing accounts configured with administrative privileges and accounts configured with standard employee privileges. Beyond standard credential matching, the system result enforces Privilege Escalation and Role-Spoofing Protection. In traditional systems, if a malicious insider gains access to a valid employee account, they might attempt to claim administrative rights within an application interface. As demonstrated in the system logic of Figure 3, if a subject authenticates under a standard user account but manually selects Corporate Administrator from the dropdown list, the Policy Decision Point (PDP) compares the client payload against the authoritative IdP record. Detecting a discrepancy between the assigned identity and the claimed role, the engine immediately terminates the evaluation, outputs an ERR_ROLE_SPOOFING_DETECTED result, and flags the session as a privilege escalation attack.

CONCLUSION

The functional Zero-Trust Network Architecture simulation engine for cloud-hosted corporate assets was achieved. The developed system successfully demonstrates that transition from perimeter-based security to explicit, dynamic, context-aware policy enforcement significantly mitigates unauthorized access, identity spoofing, and privilege escalation risks. By continuously assessing identity, device health, and resource context prior to granting granular session pathways, the system proves that Zero-Trust Architecture effectively protects corporate data assets within modern, untrusted cloud environments.

RECOMMENDATIONS

Find below some useful recommendations for other institutions for implementation and future work:

- i. Organizations adopting Zero-Trust principles should prioritize continuous, real-time device posture monitoring rather than relying solely on single-point login evaluation.
- ii. Future iterations of the Policy Decision Point (PDP) engine should integrate artificial intelligence (AI) and machine learning (ML) models to analyze behavioral telemetry (such as unusual request times, geo-velocity shifts, or abnormal resource access patterns) to calculate real-time risk scores.

REFERENCES

- Arunkumar, M., & Ashok Kumar, K. (2022). Malicious attack detection approach in cloud computing using machine learning techniques. *Soft Computing*, 26(1), 1–12. <https://doi.org/10.1007/s00500-021-06679-0>
- Asheshemi, N. O., & Adawaren, M. (2026). Mitigating Insider Threats and Data Breaches in Nigerian Financial Cloud Systems Using a Blockchain-Based Zero Trust Framework. *Scientific Journal of Engineering, and Technology*, 3(1), 28-43.
- Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of Zero-Trust. *Computers & Security*, Article 102436. <https://doi.org/10.1016/j.cose.2021.102436>
- Buck, C., Olenberger, C., Schweizer, A., & Völter, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security*, 133, Article 103412. <https://doi.org/10.1016/j.cose.2023.103412>
- Cunningham, C. (2021). The Zero Trust eXtended (ZTX) ecosystem framework. Forrester Research. Access from <https://drzerotrust.com/>
- Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A systematic literature review. *Journal of Network and Systems Management*, 34, Access from <https://link.springer.com/journal/10922>
- Garbis, J., & Chapman, J. W. (2021). Zero Trust security: An enterprise guide. Apress. <https://doi.org/10.1007/978-1-4842-6702-8>

- Raghuvar, K. R. D.(2025). Implementing Zero Trust Architecture: Principles, Models and Challenges. International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com 4(12), DOI: <https://doi.org/10.38124/ijsrmt.v4i12.1050>
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
- Sevindik, S., Akgün, A., Şahin, N., Bayram, Ö. F., & Atarer, F. (2024). Towards net-zero: A Comprehensive Data-Driven Framework of Circular Economy Principles in Architectural Design. *Tokyo Summit-VIII*, 8.