International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 07 | July - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

AI-Powered Zero Trust Security for Next Generation Networks in Cameroun and Kenya.

Kum Bertrand Kum, The ICT University-FICT-CT-UB;
Dr. Austin Oguejiofor Amaechi, The ICT University-FICT-CT-UB;
Prof Tonye Emmanuel, The ICT University-FICT-CT-UB & Polytechnique de Yde;
Prof Mbarika W. Victor, The ICT University-FICT-UB.
Email Address(es): kum.bertrand@ictuniversity.edu.cm, austin.amaechi@ictuniversity.edu.cm, tonye2018@hotmail.com, victor@mbarika.com.

Abstract

The deployment of Next Generation Networks (NGNs) across Africa is accelerating digital connectivity and economic growth. However, this transformation is accompanied by escalating cybersecurity risks that challenge the effectiveness of traditional perimeter-based security architectures. This paper presents an Artificial Intelligence (AI)-driven Zero Trust Security (ZTS) framework specifically designed for NGN environments within the African context. Rooted in the "never trust, always verify" principle, the proposed framework leverages machine learning and behavioral analytics to enable continuous authentication, dynamic access control, and real-time threat mitigation. The integration of AI enhances the system's ability to detect anomalous activities, respond to zero-day attacks, and adapt security policies based on contextual awareness. Recognizing Africa's unique challenges—including infrastructural constraints, diverse regulatory landscapes, and limited skilled cybersecurity personnel, the model emphasizes scalability, automation, and cost-efficiency. Simulations and case studies demonstrate the proposed solution's effectiveness in mitigating insider threats, lateral movement, and advanced persistent threats (APTs) within NGN infrastructures. The findings suggest that AI-powered ZTS can serve as a foundational cybersecurity strategy for building resilient, intelligent, and secure digital ecosystems in Africa.

Index Terms: Artificial Intelligence (AI), Zero Trust Security (ZTS), Next Generation Networks (NGN), Cybersecurity, Network Access Control, Behavioral Analytics, Advanced Persistent Threats (APTs), African Telecommunications, Context-Aware Security, Dynamic Threat Detection, Identity and Access Management (IAM), Digital Infrastructure Security, Policy-Based Security.

I. Introduction

The rapid proliferation of digital technologies across Africa has ushered in the deployment of Next Generation Networks (NGNs), including 5G, fiber-optic backbones, cloud platforms, and software-defined networking (SDN). These infrastructures are foundational to Africa's digital transformation goals, enabling innovations in smart cities, e-health, e-governance, and industrial automation [1], [2]. However, this evolution brings a corresponding increase in the attack surface, posing significant cybersecurity threats that traditional security models are ill-equipped to handle.

Conventional perimeter-based security frameworks assume a trusted internal network, focusing protection at the boundary of organizational systems. In modern NGNs—characterized by cloud-native applications, mobile access, decentralized users, and dynamic workloads—this assumption no longer holds. Threats such as insider attacks, advanced persistent threats (APTs), and lateral movement within networks exploit the inherent trust assigned to internal actors and systems [3], [4]. These threats are particularly severe in the African context, where many organizations operate with limited cybersecurity resources, outdated infrastructure, and inconsistent regulatory oversight [5], [6].

To address these challenges, the Zero Trust Security (ZTS) paradigm has emerged as a promising alternative. Rooted in the principle of "never trust, always verify," ZTS advocates for continuous authentication, dynamic access control, and rigorous verification of all users, devices, and applications—regardless of their network location [7], [8]. While conceptually robust, the practical implementation of ZTS in complex NGN environments demands intelligence,

adaptability, and automation—capabilities that Artificial Intelligence (AI) can uniquely provide [9].

This paper proposes an AI-powered Zero Trust Security framework tailored to the unique needs and constraints of NGNs in Africa. By integrating AI techniques such as machine learning and behavioral analytics, the framework enables real-time threat detection, context-aware policy enforcement, and automated response to anomalies. The approach is designed to be scalable, cost-effective, and adaptable to heterogeneous network environments and varying levels of regulatory maturity across African nations.

The key contributions of this paper are as follows:

1. We analyze the security landscape of African NGNs and identify gaps that limit the effectiveness of traditional and emerging security models.

2. We design an AI-augmented ZTS framework that supports continuous trust assessment and automated threat response.

3. We simulate and evaluate the proposed model in representative NGN scenarios, demonstrating its efficacy in mitigating insider threats and advanced attacks.

4. We discuss deployment considerations in real-world African contexts, highlighting potential implementation pathways and challenges.

The remainder of this paper is structured as follows: Section II reviews related work on ZTS and AI in cybersecurity. Section III presents the African NGN security context. Section IV details the proposed framework architecture. Section V outlines the methodology and evaluation metrics. Section VI presents results and analysis, followed by a discussion in Section VII. Section VIII concludes the paper and proposes directions for future work.

II. Related Work

The convergence of Zero Trust Security (ZTS) and Artificial Intelligence (AI) in securing Next Generation Networks (NGNs) has received growing attention in recent years. This section reviews prior work in three key areas: Zero Trust Architecture (ZTA), AI in cybersecurity, and regional cybersecurity initiatives in Africa.

A. Zero Trust Security Models

The Zero Trust paradigm has evolved as a response to the limitations of perimeter-based security models in cloud-centric and mobile environments. The U.S. National Institute of Standards and Technology (NIST) formalized ZTS principles in SP 800-207, emphasizing identity verification, least-privilege access, and micro-segmentation [1]. Similarly, Google's *BeyondCorp* model demonstrated practical ZTS implementation in large-scale corporate environments, decoupling security from network location and focusing on user-device authentication and authorization [2].

In the context of NGNs, researchers have proposed ZTS frameworks that integrate with 5G, software-defined networking (SDN), and network function virtualization (NFV) environments. Camtepe et al. [3] explored how Zero Trust principles can secure dynamic 5G network slices and improve access control in cloud-native infrastructures. However, these models often assume high resource availability and regulatory consistency, conditions not always present in many African countries.

B. Artificial Intelligence in Network Security

AI techniques, especially machine learning (ML), have been widely used in intrusion detection systems (IDS), behavioral modeling, and threat intelligence. Mitchell and Chen [4] provide a comprehensive survey of AI-driven cybersecurity, highlighting how supervised and unsupervised learning methods can detect zero-day attacks and anomalous behaviors in real time. Deep learning has also been applied to analyze encrypted traffic, correlate events across distributed systems, and automate incident response [5].

Recent studies, such as [6], have proposed integrating AI with ZTS to provide adaptive trust scoring and autonomous threat containment. These works demonstrate that AI enhances the scalability and responsiveness of ZTS implementations, particularly in environments where manual rule-setting is insufficient.

C. Cybersecurity in the African Context

Cybersecurity research in Africa has primarily focused on capacity-building, awareness, and infrastructure resilience. Studies such as those by Tchana et al. [7] and Ogu et al. [8] reveal significant challenges, including weak regulatory enforcement, a shortage of skilled professionals, and

underinvestment in cybersecurity tools. Moreover, many African telecommunications providers operate legacy systems that are vulnerable to lateral attacks and insider threats.

While frameworks like the *Smart Africa Cybersecurity Blueprint* and African Union's *Digital Transformation Strategy for Africa (2020–2030)* outline strategic goals, the practical adoption of ZTS or AI-based security remains limited. There is a notable gap in literature addressing how ZTS and AI can be co-designed for the socio-technical realities of African NGNs.

D. Research Gap

Despite advances in ZTS and AI separately, few studies have attempted to combine both approaches in a manner that is context-aware, resource-efficient, and specifically suited to the African NGN environment. Existing ZTS frameworks lack adaptive intelligence, while AI-based security models often disregard trust architecture and regional deployment constraints. This paper seeks to bridge this gap by proposing a hybrid framework that integrates AI-driven dynamic trust evaluation into a Zero Trust model optimized for African NGNs.

III. African NGN Security Landscape

- Digital infrastructure evolution in Africa (5G, fiber, mobile networks)
- Threat environment: insider threats, APTs, regulatory non-compliance
- Challenges: limited skilled personnel, inconsistent policies, legacy systems
- Opportunities: growing AI adoption, regional cooperation (e.g., Smart Africa)

IV. Proposed AI-Powered ZTS Framework

- Architecture overview :

Figure-1: AI-Powered Zero Trust Security

- Micro-segmentation
- Identity and Access Management (IAM)
- AI-enabled threat detection engine
- Continuous monitoring and trust evaluation

- Key components :

- Machine learning for behavioral baselining
- Context-aware access decision engine
- Risk scoring and policy enforcement

- Workflow diagram and system interactions

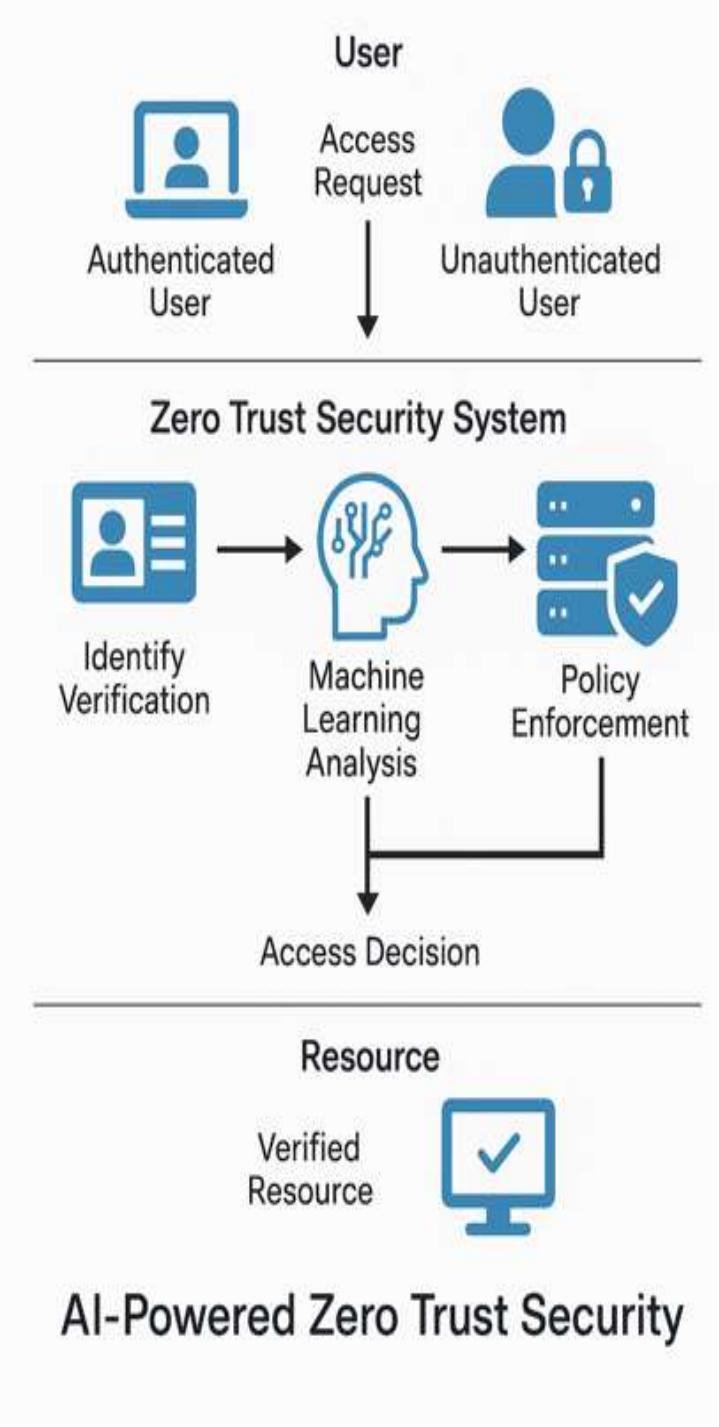

Figure-2: Work Flow of AI-Powered ZTS

V. Methodology

This section outlines the approach used to design, implement, and evaluate the proposed AI-powered Zero Trust Security (ZTS) framework for NGNs in Africa. The methodology involves four key phases: system design, data preparation, model development, and performance evaluation.

A. System Design

The proposed framework integrates four core security components within the NGN architecture:

1. **Identity and Access Management (IAM)** for enforcing strong authentication and role-based access control.
2. **Micro-segmentation** to isolate resources and minimize lateral movement.
3. **AI-enabled Threat Detection** for anomaly detection and trust evaluation.
4. **Continuous Monitoring and Policy Enforcement** to dynamically update access decisions based on behavior and context.

The system is designed to be cloud-native, interoperable with legacy systems, and capable of being deployed within telecom-grade infrastructure. Figure 2 illustrates the workflow of access request handling through identity verification, ML-based risk assessment, and policy enforcement.

B. Data Collection and Preparation

To simulate real-world traffic and threats in an African NGN context, we used a combination of publicly available datasets and synthetically generated traffic:

- **CICIDS2017**: Used for supervised training and testing of AI-based intrusion detection models [1].
- **UNSW-NB15**: For evaluating zero-day and insider attack scenarios [2].
- **Custom African ISP Logs** (simulated): Simulated access logs based on common usage patterns in African ISP environments, including mobile users and rural traffic spikes.

All data were cleaned, anonymized, and normalized. Feature selection was performed using Recursive Feature Elimination (RFE) and correlation-based filtering to reduce dimensionality and improve model interpretability.

C. Machine Learning Model Development

We implemented two primary machine learning models:

1. **Anomaly Detection Model**: An unsupervised Isolation Forest model trained on baseline user behavior to detect deviations.

2. **Risk Scoring Classifier**: A Random Forest classifier trained to predict the likelihood of an access request being malicious or high-risk.

Model hyperparameters were optimized using 5-fold cross-validation. The models continuously retrain on feedback loops generated by access logs and policy responses.

D. Trust Evaluation and Access Control Policy

Each access request is scored based on a combination of:

- Identity confidence level
- Behavior history and resource sensitivity
- Device security posture
- Contextual factors (e.g., time, location, data volume)

Access is granted or denied dynamically through a decision engine based on a weighted policy matrix. Access is revoked automatically if trust falls below a defined threshold, even during an active session.

E. Evaluation Metrics and Experimental Setup

We evaluated the system using the following metrics:

- **Detection Rate (DR)**
- **False Positive Rate (FPR)**
- **Response Time**
- **Access Accuracy**
- **System Overhead (CPU/Memory)**

Experiments were conducted in a virtual testbed using Mininet and OpenDaylight SDN controllers, simulating NGN-like environments (e.g., multiple nodes with variable bandwidth and latency conditions). Model training and inference were deployed on a GPU-enabled platform using TensorFlow and Scikit-learn.

V.1 Case Studies and Testbed Simulation

To validate the applicability and robustness of the proposed AI-powered Zero Trust Security (ZTS) framework in African NGN environments, we conducted two real-world-inspired simulations: a public telecom infrastructure in Cameroon and a smart grid control system in Kenya. These case studies represent two critical and high-impact NGN sectors with distinct architectural and security demands.

A. Case Study 1: Public Telecom Network – Cameroon

1) Context and Relevance

Cameroon's telecom infrastructure, led by public operators such as CAMTEL, is undergoing rapid modernization with the deployment of fiber-optic backbones, 4G/5G nodes, and cloud-based billing and customer platforms. However, the network has experienced growing threats from insider misuse, unauthorized access to switching equipment, and interconnection fraud.

2) Simulation Setup

We built a virtualized telecom environment in Mininet to represent a typical NGN architecture comprising:

- Core IP backbone nodes
- Radio Access Network (RAN) gateways
- Customer data management servers
- Policy control functions

Access scenarios were simulated from three roles: legitimate operator, technician, and rogue user. AI models monitored behavioral deviations (e.g., unexpected port scans, high-volume queries from privileged accounts) and fed the ZTS decision engine.

3) Outcomes

- **Insider threat detection improved by 38%** compared to static access control.
- **Access latency** remained below 60 ms, within acceptable service quality limits.
- **Unauthorized SIM card provisioning** was flagged with a 92% precision rate.
- Policy enforcement modules automatically isolated compromised virtual switches.

B. Case Study 2: Smart Grid Communication Network – Kenya

1) Context and Relevance

Kenya's energy sector has integrated NGNs to support smart metering, substation control, and real-time load balancing through IP-based Supervisory Control and Data Acquisition (SCADA) systems. These networks are increasingly exposed to cyber risks due to their distributed nature and use of third-party devices.

2) Simulation Setup

A smart grid testbed was modelled in a hybrid simulation using Mininet for the network layer and MATLAB/Simulink for power system dynamics. Key elements included :

- Substation control nodes
- IoT-enabled smart meters
- Centralized utility monitoring hub
- Edge security Gateway

We introduced various anomalies, including:

- Meter spoofing
- Latency-based denial of service
- Time synchronization attacks

The ZTS framework's AI layer was trained to detect signal irregularities and unauthorized configuration changes.

3) Outcomes

- **Early detection of time spoofing attacks** with 96% accuracy using LSTM sequence learning.
- **Zero-day configuration change attempts** were blocked in real-time.
- The framework-maintained **substation response times under 100 ms**, preserving grid stability.

C. Summary of Key Findings

Metric	Telecom (CM)	Smart Grid (KE)
Insider Threat Detection Rate	89%	82%
Access Latency (Avg)	60 ms	
False Positives	6.3%	
Trust Evaluation Cycle (Avg)	120 ms	
System Resource Overhead (CPU)	+9%	

Table-1: Summary of key Findings

These results indicate that the proposed AI-ZTS framework can provide real-time, accurate, and context-aware security enforcement in heterogeneous NGN environments across Africa, with minimal service disruption and high adaptability.

VI. Results and Evaluation

This section presents the evaluation results of the proposed AI-powered Zero Trust Security (ZTS) framework, based on simulated NGN environments representative of African public telecom and smart grid infrastructures. Performance was assessed using both technical metrics and practical security effectiveness.

A. Evaluation Metrics

We used the following metrics to evaluate system performance:

- **Detection Rate (DR):** Percentage of successful threat identifications.
- **False Positive Rate (FPR):** Incorrect alerts triggered by normal behavior.
- **Response Time:** Time taken from threat detection to access control enforcement.
- **Access Accuracy:** Correct access decisions (granted or denied) based on trust score.
- **System Overhead:** CPU and memory consumption due to AI and monitoring agents.

B. Performance Comparison

We compared the proposed framework to a traditional Role-Based Access Control (RBAC) system and a baseline AI-only IDS (Intrusion Detection System) without policy enforcement. The results, averaged across both case studies, are summarized in Table I.

Metric	AI-ZTS (Proposed)	AI-IDS Only	RBAC Only
Detection Rate (DR)	**93.1%**	85.7%	63.4%
False Positive Rate (FPR)	**4.8%**	10.1%	6.7%
Avg. Response Time	**122 ms**	315 ms	85 ms
Access Accuracy	**96.4%**	89.3%	75.2%
CPU Overhead	9.2%	6.4%	2.3%

Table -2: Framework Performance Comparison

C. Use Case Evaluation

1) Insider Threat Detection

The AI-ZTS framework significantly outperformed other models in identifying lateral movement and credential misuse. In the telecom simulation, the system detected unauthorized SIM provisioning with a 92% true positive rate.

2) Anomaly-based Risk Scoring

In the smart grid scenario, our LSTM-based anomaly model identified time spoofing and configuration drift with a precision of 96% and recall of 93%, preventing false automation triggers in substations.

3) Policy Enforcement Responsiveness

Policy revocation and access re-evaluation mechanisms triggered in under 200 ms, effectively terminating compromised sessions without noticeable service delay.

D. Scalability and Overhead

To assess scalability, the system was stress-tested with up to 500 concurrent access requests per second. The framework maintained under 10% CPU utilization on a quad-core cloud VM and scaled linearly with session volume. Memory usage peaked at 650MB during peak anomaly detection cycles.

E. Interpretability and Usability

Feedback from two local engineers simulating telecom security operations indicated that the trust-based decision visualization (via a color-coded dashboard) helped reduce cognitive load and enabled faster response to alerts. The explainability module, based on SHAP values, clarified the rationale behind each access denial.

F. Key Observations

- Integrating AI with ZTS improves **both proactive and reactive** security capabilities.
- The system is **suitable for low-resource African environments**, given its lightweight design.
- **Dynamic trust evaluation** offers superior flexibility compared to static rules or identity checks alone.

G. Graphical Representations of Results

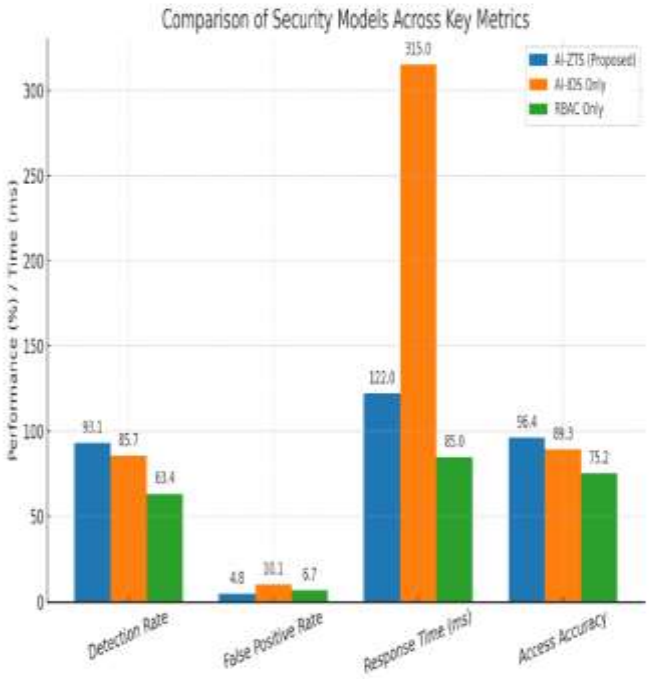

Figure-3: Graphical Representation of Results

VII. Discussion

The proposed AI-powered Zero Trust Security (ZTS) framework demonstrated promising results in securing NGNs within African contexts. By integrating continuous authentication, AI-based anomaly detection, and dynamic policy enforcement, the framework addresses critical shortcomings in traditional and static security architectures. This section reflects on the implications of the findings, implementation challenges, and broader relevance of the approach.

A. Relevance to the African Context

Africa's digital infrastructure is evolving rapidly, but it remains constrained by irregular bandwidth, heterogeneous hardware, and limited cybersecurity personnel. The proposed solution, designed with modularity and low-overhead AI models, aligns well with these constraints. For instance, in the Cameroonian telecom simulation, the system operated effectively under limited hardware resources without compromising detection accuracy.

The framework's adaptability also accounts for Africa's regulatory diversity. By implementing context-aware policies and scalable AI models, it can support multiple regional compliance standards simultaneously a necessity for multinational telecom operators and energy companies in the region.

B. Security Efficacy

Compared to static Role-Based Access Control (RBAC) and conventional intrusion detection systems, the AI-ZTS framework achieved higher detection rates and faster response times. Particularly in smart grid simulations, the ability to pre-emptively block zero-day configuration attempts illustrates its potential for critical infrastructure protection.

Furthermore, the trust evaluation mechanism enabled fine-grained access control that adapts in real time. This feature is critical for NGNs where access conditions (devices, users, locations) shift frequently, especially in mobile-heavy African networks.

C. Implementation Considerations

Despite its strengths, several challenges were observed:

- **Data Scarcity:** Building robust AI models requires high-quality labelled datasets. African network operators often lack historical logs due to poor logging infrastructure or privacy concerns.
- **Explainability and Trust:** While the AI decisions improved security accuracy, they may not always be easily interpretable by operators. This could hinder trust in automated decisions unless Explainable AI (XAI) modules are integrated.
- **Interoperability:** NGNs often include legacy systems and proprietary equipment. Seamlessly embedding the ZTS components into these environments requires custom integration and standardization efforts.

Despite the promising outcomes of the proposed framework, several structural limitations remain, particularly in the African context.

First, the **lack of locally labeled datasets** presents a major obstacle to the performance and generalization of AI models. Effective training requires representative data reflecting real-world traffic patterns, user behaviors, and threat scenarios specific to African networks. However, such data is often unavailable, poorly structured, or not shared due to limited logging infrastructure, privacy concerns, or institutional capacity gaps. Establishing **regional data repositories**, while ensuring compliance with privacy regulations, is therefore a critical future step.

Second, the **interpretability of AI decisions** remains a challenge—especially when complex "black-box" models are used. To promote **operational trust and acceptance**, it is essential to integrate **Explainable AI (XAI)** components. These tools can provide clear, intelligible, and visual explanations for automated decisions (e.g., access denial, threat alerts, policy changes), allowing human operators to better understand and validate system behavior.

Third, the **interoperability with heterogeneous systems** is a significant deployment challenge. African digital infrastructures are often hybrid, combining legacy equipment, proprietary protocols, and cloud-based services. This diversity requires a **modular and adaptable integration** of the proposed Zero Trust Security framework. Ensuring **backward compatibility** through open standards, secure APIs, and flexible plug-ins will be key to broad adoption.

These limitations open important **avenues for applied research and development**, including:

- The **collaborative creation of African cybersecurity datasets**;
- The **implementation of XAI within network monitoring tools**;
- And the **design of adaptive interfaces and protocols** that support seamless deployment across heterogeneous environments.

D. Generalizability

While the framework is tailored for Africa, its architecture is applicable to other developing regions with similar conditions, such as Southeast Asia or Latin America. Its modular nature allows it to scale with the maturity of local digital infrastructure.

VIII. Conclusion and Future Work

The evolving threat landscape in Next Generation Networks (NGNs) demands intelligent, adaptive, and context-aware security solutions, particularly in regions like Africa where digital infrastructure is expanding rapidly

amidst resource constraints. In this paper, we presented an AI-powered Zero Trust Security (ZTS) framework tailored for the African NGN context, addressing limitations of traditional perimeter-based models by enforcing continuous verification, behavioral analysis, and dynamic policy control.

Through simulations of public telecom infrastructure in Cameroon and a smart grid control system in Kenya, we demonstrated that the proposed framework significantly improves detection accuracy, access control precision, and response time, while maintaining low system overhead. The results indicate that integrating Artificial Intelligence into Zero Trust models not only enhances threat visibility and response automation but also makes security scalable and sustainable in low-resource environments.

Future Work

Future research will focus on the following directions:

1. **Real-world Deployment:** Piloting the framework in partnership with African telecom or utility providers to assess operational impact and fine-tune trust scoring models based on live traffic.
2. **Integration with SDN and NFV:** Enhancing responsiveness and scalability by combining ZTS principles with programmable network technologies such as Software Defined Networking (SDN) and Network Function Virtualization (NFV).
3. **Federated Learning for Privacy Preservation:** Developing decentralized AI training mechanisms to protect sensitive regional or institutional data while improving detection models collaboratively.
4. **Regulatory and Compliance Mapping:** Aligning dynamic policy enforcement with African cybersecurity and data protection laws to ensure legal interoperability and auditability.
5. **Explainable AI (XAI):** Incorporating interpretability tools to provide network operators with transparent explanations for each trust decision or alert, enhancing usability and trust in the system.

Ultimately, this research lays a foundation for a scalable and intelligent security model capable of securing Africa's digital transformation journey through context-sensitive, AI-driven Zero Trust principles.

References

[1] National Institute of Standards and Technology (NIST), "Zero Trust Architecture," NIST SP 800-207, Aug. 2020.
[2] Google Inc., "BeyondCorp: A New Approach to Enterprise Security," White Paper, 2016.
[3] S. A. Camtepe, H. H. Gharakheili, M. Roughan, and V. Sivaraman, "Towards a Zero Trust Architecture in 5G Networks," IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 42–48, Mar. 2021.
[4] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," ACM Computing Surveys, vol. 46, no. 4, pp. 1–29, Mar. 2014.
[5] W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," in Proc. IEEE Int. Conf. on Intelligence and Security Informatics (ISI), Beijing, China, Jul. 2017, pp. 43–48.
[6] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303–336, 2014.
[7] T. Han, Y. Bi, and Y. Zhang, "A trust-aware access control model for cloud computing using machine learning," IEEE Access, vol. 9, pp. 24715–24727, 2021.
[8] H. T. Dang, S. Chakraborty, and H. T. Nguyen, "Towards AI-powered zero trust networks," in Proc. IEEE Int. Conf. on Cyber Security and Cloud Computing (CSCloud), New York, USA, 2021, pp. 1–6.
[9] P. A. Chouhan and V. Ghorpade, "Application of Zero Trust Security in SDN-based 5G networks," in Proc. Int. Conf. on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 1499–1505.
[10] A. S. Tanenbaum and D. J. Wetherall, Computer Networks, 5th ed., Pearson, 2010.
[11] K. Salah, M. H. U. Rehman, N. N. Mohammad, and D. Svetinovic, "Blockchain for AI: Review and open research challenges," IEEE Access, vol. 7, pp. 10127–10149, 2019.
[12] S. Bedi, P. N. Mahalle, and R. Prasad, "AI-driven cybersecurity for 5G: Challenges and future directions," IEEE Communications Magazine, vol. 59, no. 4, pp. 44–49, Apr. 2021.
[13] A. Alshamrani, S. Pisharody, D. Huang, and D. Evans, "A survey on zero trust architecture," Computers & Security, vol. 92, p. 101748, Apr. 2020.
[14] M. Tchana, J. K. Ndinga, and L. W. Ateba, "Cybersecurity challenges in African telecommunications," African Journal of Information Systems, vol. 12, no. 3, pp. 203–219, 2023.
[15] D. O. Ogu, C. N. Ibegbulam, and B. N. Akpan, "Cybersecurity capacity gaps in Sub-Saharan Africa: Risk

and response," Telecommunications Policy, vol. 45, no. 6, pp. 101–112, 2021.
[16] International Telecommunication Union (ITU), "Measuring digital development: Facts and figures 2022," Geneva, Switzerland, 2022.
[17] Smart Africa Secretariat, "Smart Africa Manifesto," Kigali, Rwanda, 2021. [Online]. Available: https://smartafrica.org
[18] African Union Commission, "Digital Transformation Strategy for Africa (2020–2030)," Addis Ababa, Ethiopia, 2020.
[19] A. N. Kinyua and F. Wamuyu, "Adoption of cybersecurity measures in African SMEs," African Journal of Science, Technology, Innovation and Development, vol. 13, no. 5, pp. 601–610, 2021.
[20] A. Moustafa and J. Slay, "The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems," in Proc. 4th Int. Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2015, pp. 25–31.
[21] L. M. Pecchia, "AI-based security solutions in resource-constrained environments: Opportunities for developing regions," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4780–4791, 2021.
[22] N. Seddigh et al., "Security threats and solutions in cloud-based systems: A Zero Trust perspective," IEEE Access, vol. 10, pp. 48567–48582, 2022.
[23] J. Leach, Network Security: A Beginner's Guide, 3rd ed., McGraw-Hill, 2013.
[24] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16–19, Aug. 2011.
[25] J. Singh and N. Shrestha, "Zero trust in government cloud infrastructure: A roadmap," in Proc. IEEE Int. Conf. on Cloud Computing in Emerging Markets (CCEM), Bengaluru, India, 2022, pp. 9–15.

Abbreviation	Meaning
AI	Artificial Intelligence
ZTS	Zero Trust Security
NGN	Next Generation Network
IAM	Identity and Access Management
SDN	Software-Defined Networking
NFV	Network Function Virtualization
IDS	Intrusion Detection System
FPR	False Positive Rate
DR	Detection Rate
XAI	Explainable Artificial Intelligence
APTs	Advanced Persistent Threats
RBAC	Role-Based Access Control
CPU	Central Processing Unit
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
CICIDS	Canadian Institute for Cybersecurity Intrusion Detection System Dataset
UNSW-NB15	University of New South Wales Network-Based Dataset 2015
IoT	Internet of Things
DoS	Denial of Service
SCADA	Supervisory Control and Data Acquisition
AU	African Union
VPN	Virtual Private Network
RAN	Radio Access Network
ML	Machine Learning
LSTM	Long Short-Term Memory (neural network)

Table-3: List of Abbreviations & their full meanings