Survey on ZTNA – A Secure Alternative to VPN

Ms. S. Nivedha
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
nivedha.s2805@gmail.com

Mr. S. Lokesh
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
lokesh.saravanan2212@gmail.com

Mr. D. Manoj
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
2004manojd@gmail.com

Mr. K. Hariharan
Dept. of Cyber Security
SRM Valliammai Engineering College
Kattankulathur, India
hariharan09tgk@gmail.com

 DOA:01.12.2025 / DOP: 10.12.2025 ISSN: 3048-619X
Volume 2 Issue 3 [Sep – Dec 2025] DOI:

Abstract— **Zero Trust Network Access (ZTNA) links Micro-Segmentation and Identity-Based Access Control (IBAC) so security improves through user-controlled device access of needed resources based on established policies. Zero Trust Network Access (ZTNA) acts as a contemporary security framework which develops security by eradicating hidden trust then implementing rigorous user and resource authorization protocols. The new system design adopts ZTNA instead of VPN-based access for secure encrypted link establishment with automated security controls. Micro-Segmentation discontinues lateral movement by dividing network sections and IBAC utilizes Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) as well as continuous verification to enforce authentication. The project uses Keycloak along with OpenZiti and Tailscale and Wazuh and Prometheus to provide a reasonably priced solution for hybrid and cloud environments with scalable security features. This method protects contemporary security protocols which decreases cyber threat risks from inside attacks as well as illegal access and cybersecurity attacks therefore bolstering overall security standards.**

Keywords— Zero Trust Network Access, Role and Identity-Based Access Control.

I. INTRODUCTION

Standard security approaches use perimeter protection systems yet they trust network operators and devices to be trustworthy by default. This security approach becomes insufficient because cloud computing expansion and changing cyberthreats combined with remote work environments have emerged. Zero Trust Network Access (ZTNA) represents the modern security approach which established strict access restrictions for user identities instead of trusting devices or their health status and contextual elements. This project's main goal is The surveyer conducts a study on deploying ZTNA through Micro-Segmentation and Identity-Based Access Control (IBAC) to enhance security measures in hybrid IBAC with its dynamic nature uses user roles and authentication levels and device compliance for access authorization while micro- segmentation creates network segmentation barriers to control unauthorized network movements. for. This combined method greatly reduces the assault risk. surface and reduces the dangers of unwanted access and insider threats.

The implementation uses a number of open-source security tools to build a scalable and effective ZTNA framework: Tailscale is used to set up VLAN segmentation, firewall rules, and intrusion detection, which further improves network security; Ansible and Kubernetes are used for automated deployment and infrastructure management, which ensures seamless scalability; Prometheus and Grafana offer real-time security monitoring and visualization, which enables proactive threat detection and incident response; and Keycloak is used for Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and session recording, which ensures secure authentication and access control.

The project implements ZTNA-based access instead of traditional VPN networks to maintain security policies which automatically apply permission changes according to contextual requirements. These security benefits become more powerful through automated systems in addition to continuous monitoring. This project proves contemporary businesses can achieve reliable scalable extremely secure network access by combining ZTNA with micro-segmentation and identity-based access control to decrease their exposure to evolving cyberthreats.

II. LITERATURE SURVEY

In this survey Identity-based access, automation, real-time monitoring and open-source software along with blockchain technology enable the survey to enhance network administration security while providing flexible and safe management functions. The details are revealed by following the process.

A. Zero Trust Network Access

Sungmin Hong.et.al.[13] Modern security infrastructure which Zero Trust leads brings abundant change by validating users and resources continuously without trusting them automatically. The current ZTNA implementation only addresses network security but fails to offer system-level security policies or abstract methods toward them. Instead ZTNA implementation introduced a new system security framework which accepts ZTNA policies from system administrators for deployment needs and provides flexibility during real-time System-wide security improves through

combined evaluation of operation.time risk and pre-defined user or system security logic verification processes. Y. Liu et al.[10] explains how the ZTNA architecture works through continuous access request evaluation which eliminates all trust by design. The entire system operates through exact authentication and authorization to ensure user access only reaches resources matching their operational needs following the least privilege principle. A secure ZTNA system depends on uniting identity management capabilities with access control networks and Properly Distributed Protection systems (PDPs) and Properly Enforcing Protection systems (PEPs) through management functions.

B. Identity and Role Based Access Control

Yinbin Miao.et.al [3] In his work, Role-based access control helps model users' access permissions over encrypted files which allows more precise splitting of access permissions. Every role maintains an associated access permit. Each person possesses one or multiple roles in the authentication system. A parent role inherits entire access permissions from its child roles while having their hierarchical organization. The access control system features a hierarchical role model which grants the parent role's permissions to the child roles and all their sub-roles. The identity authentication system implements both inter- company collaboration and permission management through its identity authentication system. Our system provides efficient user management methods whenever changes occur to the user sets associated with identical roles. The application accessible through Fig. 1 links multiple users to each role-based access control position.

C. Automation and Monitoring in Zero Trust Security

Real-time monitoring and automated systems serve as essential requirements for Zero Trust operations since they ensure permanent security policy implementation. continuous enforcement of security policies. Automation through Ansible together with Kubernetes allows organizations to manage security component deployment automation and configuration as well as scaling processes thus decreasing human involvement and human error rates. Organiations can detect threats proactively through security event visualization and monitoring that Prometheus and Grafana jointly provide. The combination of Intrusion Detection Systems (IDS) and behavioural analytics supports organizations in detecting questionable activities to block breaches from worsening. Zero Trust security benefits from the strength of automated security plus continuous monitoring and artificial intelligence analytics because it maintains both real-time threat visibility and automatic reaction capabilities.

D. Comparison of Open-Source VS Commercial ZTNA solution

Security industry vendors have created commercial plus open-source ZTNA solutions which offer different organizational benefits to users. The Enterprise security features and management solutions along with compliance features are found in proprietary products from companies like Google Beyond Corp and Microsoft Zero Trust. The open- source ZTNA solutions Keycloak, Wire Guard, and Tailscale enable organizations to get better cost efficiency while promoting vendor independence through community involvement. The solutions enable companies to design security policies that work with their infrastructure and maintain independence from third-party vendors which makes them ideal for secure cloud environment expansion. Yinbin Miao.et.al[3] explains that the Role Management (RM) system operates as an algorithm to establish role-user data and handle roles together with users as well as their relationship connections while the Trusted Authority(TA) becomes offline. The role management system holds access only to role secret keys to maintain data privacy in its stored material.

E. Research Gap and Motivation

The traditional security models of VPNs along with perimeter-based defences prove insufficient against the current threats from inside attackers along with credential compromisers and lateral attackers that exist in contemporary cloud and hybrid setups. Security requirements for Zero Trust models became necessary to deal with modern cyber threats that include ransomware along with data security breaches. The project implements Keycloak alongside OpenZiti and WireGuard and pfSense to deliver strong authentication along with restricted access while real-time security monitoring thus substituting traditional VPN access with ZTNA. The established approach delivers a flexible price-effective secured network entry system that automates security policy implementation.

III. EXISTING WORK

Currently Zero Trust Network Access (ZTNA) includes several notable implementations that have influenced current cybersecurity practices. Google's BeyondCorp model pioneered the Zero Trust approach by shifting access decisions from the network perimeter to user and device identity, setting the foundation for modern ZTNA frameworks. Open-source tools like Headscale, a self-hosted version of Tailscale, enable device-based secure access and have gained popularity for decentralized ZTNA deployments. Teleport offers secure infrastructure access with certificate- based authentication and MFA, often integrated with Python for automation and access control. Additionally,

pfSense, a widely used firewall platform, is commonly paired with Python scripts for managing policies and network configurations. Academic and student projects frequently use Python to build ZTNA prototypes, incorporating elements like multi-factor authentication, role-based access control, real-time logging, and user-friendly GUIs. These efforts collectively demonstrate the growing trend of using open- source, Python-based tools to implement scalable and cost- effective ZTNA solutions.

IV. INFERENCE AND DISCUSSION

Zero Trust Network Access (ZTNA) project has shown a strong, expandable and safe access control mechanism through a practical and well -integrated web application. The project has increased the effectiveness of the traditional VPN access to the modern ZTNA frame focusing on policies by combining the main safety principles such as micro segments, identity -based access control (IBAC) and continuous user verification. The system has successfully implemented OTP
-based authentication with expired, back limit and speed limit, not only improving the safety of connectivity but also reducing the vulnerability of the brute force and automatic connection attacks. Access control based on the role (RBAC) has allowed access to user roles (administrators, users, guests), ensuring that sensitive activities and data are only available to users. The ZTNA-based secure web access model developed in this project marks a significant improvement over traditional VPN solutions by continuously verifying user identity, device health, and contextual access. Key strengths included multi-factor authentication using facial recognition and OTP, which greatly reduced the risk of unauthorized access. Role-Based Access Control (RBAC) effectively enforced the principle of least privilege, limiting users to only necessary resources and minimizing internal threats. The system also demonstrated strong real-time protection against web-based attacks like SQL injection and XSS through proactive input filtering. While setup challenges such as facial recognition sensitivity and OTP delays were noted, overall, the model proved to be a robust and scalable alternative to VPNs. It successfully upheld Zero Trust principles—"never trust, always verify"—and enhanced security without compromising usability, making it highly relevant for organizations managing sensitive data or operating in distributed environments.

V. CONCLUSION

The survey evaluates the superior capabilities of Zero Trust Network Access (ZTNA) compared to traditional VPN-based security models. Network segmentation combined with continuous verification and least privilege access under ZTNA enhances security at the same time it reduces exposure to insider threats along with lateral network movement and unauthorized access. Security solutions gain enhanced depth through Identity-based access control (IBAC which allows real-time administration of authorizations according to context variables and authentication variables and user identification information. This survey benefits from the efficient open-source ZTNA security framework capabilities demonstrated by Keycloak, WireGuard, OpenZiti and Tailscale solutions. The policy implementation and execution are enhanced through Kubernetes and Ansible automation tools which are complemented by Prometheus and Grafana to deliver real-time threat detection and response features.

REFERENCES

[1] X. Xiang, J. Cao and W. Fan, "Secure Authentication and Trust Management Scheme for Edge AI-Enabled Cyber- Physical Systems," in *IEEE Transactions on Intelligent Transportation Systems*, Vol. 26, No. 3, pp. 3237-3249, 2025.

[2] M. Nawaz Khan, H. Ur Rahman, T. Hussain, B. Yang and S. Mian Qaisar, "Enabling Trust in Automotive IoT: Lightweight Mutual Authentication Scheme for Electronic Connected Devices in Internet of Things," in *IEEE Transactions on Consumer Electronics*, Vol. 70, No. 3, pp. 5065-5078, 2024. Y. Miao et al., "REKS: Role-Based Encrypted Keyword Search With Enhanced Access Control for Outsourced Cloud Data," in IEEE Transactions on Dependable and Secure Computing, Vol. 21, No. 4, pp. 3247-3261, July-Aug. 2024.

[3] L. Yang, M. E. Rajab, A. Shami and S. Muhaidat, "Enabling AutoML for Zero-Touch Network Security: Use-Case Driven Analysis," in *IEEE Transactions on Network and Service Management*, Vol. 21, No. 3, pp. 3555-3582,2024.

[4] J. Mongay Batalla *et al*., "Multi-Layer Security Assurance of the 5G Automotive System Based on Multi-Criteria Decision Making," in *IEEE Transactions on Intelligent Transportation Systems*, Vol. 25, No. 5, pp. 3496-3512, 2024.

[5] D. Bringhenti, S. Bussa, R. Sisto and F. Valenza, "A Two-Fold Traffic Flow Model for Network Security Management," in *IEEE Transactions on Network and Service Management*, Vol. 21, No. 4, pp. 3740-3758, 2024.

[6] E. Zeydan, J. Baranda, J. Mangues-Bafalluy, S. S. Arslan and Y. Turk, "A Trustworthy Framework for Multi-Cloud Service Management: Self-Sovereign Identity Integration," in *IEEE Transactions on Network Science and Engineering*, Vol. 11, No. 3, pp. 3135-3147, 2024.

[7] J. M. J. Valero, V. Theodorou, M. G. Pérez and G. M. Pérez, "SLA- Driven Trust and Reputation Management Framework for 5G Distributed Service Marketplaces," in *IEEE Transactions on Dependable and Secure Computing*, Vol. 21, No. 4, pp. 1863-1875, 2024.

[8] Fang, Y. Zhu, Y. Zhang and X. Wang, "Decentralized Edge Collaboration for Seamless Handover Authentication in Zero-Trust IoV," in *IEEE Transactions on Wireless Communications*, Vol. 23, No. 8, pp. 8760-8772, 2024.

[9] Y. Liu *et al*., "Secure and Scalable Cross-Domain Data Sharing in Zero-Trust Cloud-Edge-End Environment Based on Sharding Blockchain," in *IEEE Transactions on Dependable and Secure Computing*, Vol. 21, No. 4, pp. 2603-2618, 2024.

[10] L. Zhu and D. Wang, "Robust Multi-Factor Authentication for WSNs With Dynamic Password Recovery," in *IEEE Transactions on Information Forensics and Security*, Vol. 19, pp. 8398-8413, 2024.

[11] W. Lei, Z. Pang, H. Wen, W. Hou and W. Li, "Physical Layer Enhanced Zero-Trust Security for Wireless Industrial Internet of Things," in *IEEE Transactions on Industrial Informatics*, Vol. 20, No. 3, pp. 4327-4336, 2024.

[12] Y. Ge and Q. Zhu, "GAZETA: GAme-Theoretic ZEro-Trust Authentication for Defense Against Lateral Movement in 5G IoT Networks," in *IEEE Transactions on Information Forensics and Security*, Vol. 19, pp. 540-554, 2024.

[13] *S. Hong, L. Xu, J. Huang, H. Li, H. Hu and G. Gu, "SysFlow: Toward a Programmable Zero Trust Framework for System Security," in IEEE Transactions on Information Forensics and Security, Vol. 18, pp. 2794-2809, 2023.*

[14] G. R. da Silva and A. L. dos Santos, "Adaptive Access Control for Smart Homes Supported by Zero Trust for User Actions," in *IEEE Transactions on Network and Service Management*,2024.

[15] *H. Zhu, X. Xue, M. Xu, B. -G. Kim, X. Lyu and S. Rani, "Zero-Trust Blockchain-Enabled Secure Next- Generation Healthcare Communication Network," in IEEE Transactions on Network and Service Management,2024.*

[16] *S.M. Nagarajan , G.G. Devarajan, M.S. Thangakrishnan, T.V. Ramana ,A.K. Bashir and A.A. AlZubi, "Artificial Intelligence - Based Zero Trust Security Approach for Consumer Industry," in IEEE Transaction on Computer Electronics, Vol. 70 , No. 3 ,pp. 5411-5418,2024.*