A Systematic Review of Zero Trust Security: Architecture, Challenges and Future Directions optimization

Dhawani Nanda[1], Dr. Anil Kumar Mishra[2]
[1]Student (I. B.Tech+M.Tech NCS) Amity University, Haryana (Gurugram) 122413, India
[2]Associate Professor, Amity University, Haryana (Gurugram) 122413, India

Abstract—**The growing decentralization of company networks due to cloud computing, remote working and IoT renders conventional perimeter-based security useless. Traditional security strategies based on trust of users inside a network are ineffective against today's modern cyber threats. Therefore, the Zero Trust Security Model has become important, that change the old approach from "trust but verify" model to "never trust, always verify" architecture. Zero Trust Architecture is a security model that assumes no person or device should be trusted by default, within or outside the network. The article presents a full review of the Zero Trust model, including its fundamental ideas, architectural constituents, and implementation approaches. It describes the core components, including identity verification, access control, and network segmentation, that assist mitigate security concerns. It also discusses the role of Artificial intelligence in enhancing security in the future. Zero Trust is a good way to increase cyber security in today's systems. It plays a significant role in current security strategies as it assists in securing sensitive data and lowering threats.**

Index Terms—**Cloud Computing, IoT, Cyber Threat, Zero Trust Security, Artificial Intelligence, Cyber Security**

I. INTRODUCTION

For a long time computer security operated like a "Castle and Moat" that means corporations erected a strong wall (firewalls) around their building. They classified everyone within the wall as "good" and everyone outside as "bad". But now the system is broken. Thanks to cloud storage, home workers and mobile phones, there's no longer just the one wall to guard. Today, this outer layer is readily circumvented by attackers, who may travel freely throughout the system. This causes severe security breaches and elevated security concerns [1–3]. The following connection may be used to understand cybersecurity risk:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact} \quad (1)$$

To solve this problem, a new technology called Zero Trust is presented. "Never Trust, Always Verify" [4] is its simple premise. This Zero Trust system does not implicitly trust any person or device, even if they are inside the network [5-6]. Whether you're at the job or in a coffee shop, the network sees it all as a potential hazard in this system. Anytime you try to open a file or application, you must authenticate who you are and that your device is secure. Every time the access request should be validated to allow only allowed people to access sensitive data [7-8]. This method is based on micro-segmentation, locking down every entrance in the castle, not just the main gate [9-10]. This way if a hacker breaks in, they are limited to one small region. They cannot steal everything and limit the spread of attacks. Zero Trust systems make access decisions based on factors other than network location. It can be written as:

$$\text{Access} = f(\text{Identity, Device, Context}) \quad (2)$$

Access is granted only after verification, device security and contextual considerations.
The detailed study gives a complete overview of the Zero Trust Security Paradigm and its importance in the field of cybersecurity. It emphasises the importance of

the 'never trust, always verify' approach to security through continuous verification of people and equipment. An important principle is least privilege, i.e., users are granted only the minimum privileges necessary [11]. This makes it more likely that there will be a security breach and that people will do damaging things in the system. Zero Trust reduces attack surfaces, prevents lateral movement in networks, and uses tools like continuous monitoring, micro-segmentation, and identity verification [12]. The paper [13-14] also discusses limits in its adoption such as complexity and integration with existing systems. But despite these limitations, Zero Trust remains a very effective strategy because of the benefits of improved security, reduced risk and increased control of resources. The research also looks at future trends, such as the role of emerging technologies in enhancing security frameworks. Cyber threats are growing, and the traditional models are not as reliable as they used to be. Thus, Zero Trust is a key element in building secure and resilient digital ecosystems [15].

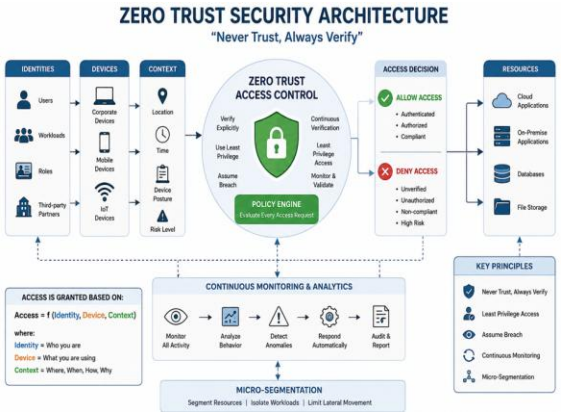

Fig. 1 Zero Trust Architecture [4]

II. LITERATURE REVIEW

Mensah introduces a security architecture based on Zero Trust that has been specifically designed for edge computing systems, where data processing takes place near the end devices. The study focuses on the importance of decentralized security mechanisms, given the distributed nature of edge networks. It offers ongoing authentication and device verification to stop unauthorized access and data integrity. The strength of this paper is the attention paid to emerging edge computing systems, and its attempt to deal with the special security issues [1].

Ahmadi discusses how to secure data access to cloud storage using Zero Trust principles. The study highlights the need for ongoing authentication and tight security measures to ensure that no unauthorized data is accessed. It suggests a set of guidelines that make sure data is secure, using identity verification and encryption methods. The paper also points out several issues, including data privacy and access control in cloud storage. [2].

Adanigbo et al. examines the application of Zero Trust Architecture in multi-cloud environments, where secure data sharing between different cloud platforms is a major concern. The study proposes a framework that ensures secure communication by enforcing strict access control and continuous verification across multiple cloud services. It highlights the importance of interoperability and policy consistency in maintaining security across heterogeneous environments [3].

Jaidi proposes an adaptive Zero Trust middleware architecture designed for decentralized cloud environments. The framework is geared towards dynamic policy enforcement and secure integration across several cloud platforms. It aims to provide flexibility and scalability while maintaining strong security controls. The strength of this work lies in its focus on cloud native environments and adaptability [4].

Iqbal & Abbas focuses on the practical implementation of Zero Trust principles in federated and distributed cyber environments. It emphasizes identity-centric authentication, micro-segmentation, and real-time monitoring to enhance security. The study demonstrates the benefits of Zero Trust in minimizing attack surfaces and detecting anomalous behavior [5].

Ogendi discusses the use of advanced analytics, machine learning, and behavioral analysis to strengthen Zero Trust architecture. It highlights how data-driven approaches can improve threat detection and enable real-time response to security incidents. The study focuses on predictive analytics and automation in decision making [6].

The integration of Artificial Intelligence (AI) techniques with Zero Trust Architecture (ZTA) is discussed by Guo et al. for enhancing threat detection capabilities. The research underscores the capability of ML models to process user activities and identify anomalies dynamically. It proposes a framework that combines AI-based monitoring with continuous authentication to enhance security. The paper also explores the use of predictive analytics to anticipate potential risks ahead of time [7].

A hybrid deep learning-based approach named SmartTrust for detecting threats in real time in cloud environments is suggested by Lilhore et al. The model combines CNN, LSTM, and transformer architectures to capture spatial and temporal characteristics of network traffic. It also features reinforcement learning to dynamically adjust to changing threats under Zero Trust model. Evaluation with benchmark datasets shows that the system has a high accuracy for insider threat detection and privilege escalation attack detection [8].

Ma et al. introduces a lightweight authentication system for IoT applications based on an advanced SM9 cryptographic method and adaptive re-authentication procedure. The model aims to minimize the overhead on communications without compromising the security with continuous verification. It brings context-aware authentication to deal with real-time conditions of distributed IoT systems. The results show less latency, energy usage, and more efficiency [9].

The proposed framework by Pokhrel et al. is a decentralized Zero Trust framework, which combines Federated Learning and Blockchain to enhance security in a distributed system. Secure data sharing without revealing sensitive data by training models locally on the model. It also features anomaly detection features to detect malicious activities. This work is based on privacy-preserving techniques and a decentralized trust model which are the strength of this work. But the complexity of the systems and the computational overhead rise with several advanced technologies and it is difficult to implement these in large scale systems [10].

$$Trust_i = S_i / T_i \quad (3)$$

where:

- S_i= Number of successful interactions of entity i
- T_i= Total interactions of entity i

Aljohani discusses how Zero Trust is applied to enterprise networks, specifically the methods of data privacy and anonymization. The study employs tools that help identify and anonymize sensitive information, reducing the risk of data breaches. It also emphasizes the need for ongoing authentication and rigorous access management in today's networks. This work is useful and relevant in terms of its practical insights and focuses on applications [11].

Fischer proposes a Zero Trust framework for securing communication in Internet of Things environments. The study emphasizes the need for continuous device authentication and secure data transmission in IoT networks. It introduces mechanisms for verifying device identity and enforcing strict access control policies. The paper also discusses challenges such as resource constraints and scalability in IoT systems. The strength of this work lies in its focus on IoT security, which is a rapidly growing area [12].

Zanasi et al. suggests a flexible Zero Trust solution for an industrial IoT system using the combination of micro-segmentation and software defined networking. The framework separates network resources and implements very strict communication restrictions for the lateral spread of threats. It shows greater resistance and adaptability to industrial settings. The study also validates the approach in prototype implementation. The positive aspects of this work are the practical application to industrial systems and the fact that it can be used with heterogeneous devices [13].

A decentralized Zero Trust access control in 6G environment over an IoT system based on blockchain and inner-product encryption is proposed by Nie et al. Smart contracts are used to enable automated access control, and reputation-based identity management is used to improve trust in the architecture. This system places no reliance on central authority and provides transparency about access decisions to increase security. This work's overall solid security comes from its decentralization and encryption. Incorporating

blockchain, however, adds to system complexity and potentially to performance overhead [14].

Chen et al. introduces Zero Trust architecture for 6G networks, emphasizing distributed access control and ongoing verification. The framework aims to solve problems like large-scale connectivity, heterogeneous devices, and sophisticated cyber-attacks. The simulation results demonstrate increased resilience to attacks such as DDoS and malware [15].

Ramezanpour & Jagannath investigated how the principles of Zero Trust can be implemented in wireless communication networks to enhance communication security. Continuous device authentication, secure communication methods and stringent access control are highlighted. It emphasizes the wireless environment problems to be addressed including mobility, diversity of wireless devices and scalability of wireless networks. The strength of this work is that it is based on wireless communication, which is currently used in plenty [16].

Kanuri covers the deployment of Zero Trust Architecture for securing unified communication systems in enterprise environments that are distributed. The study points out the shortcomings of traditional perimeter-based models and the need for constant authentication and tight control of access over communication platforms. The strength of this paper lies in its relevance to modern enterprise communication challenges and its emphasis on securing collaborative environments [17].

Rautaray deals with the application of Zero Trust to a healthcare system and the protection of sensitive patient information. The research highlights the importance of continuous authentication, robust access control measures, and data encryption to maintain privacy and comply with regulations. It is a reminder of the dangers of data breaches and unauthorized access in healthcare settings. The main goal of the framework is to protect medical systems and electronic health records from external and internal attack [18].

Kumar examines the application of Zero Trust principles in software development environments. It highlights the importance of integrating security measures early in the development of a lifecycle to address modern cybersecurity challenges. The study emphasizes secure coding practice and continuous verification [19].

Zohaib et al. proposes a Zero Trust VPN (ZT-VPN) framework to enhance security in modern enterprise environments, especially for remote work. It replaces traditional VPN trust with continuous verification and least privilege access. The model integrates ZTNA, SD-WAN, and SASE for better security and performance. However, it lacks real-world validation and may be difficult to implement in legacy systems [20].

James et al. proposes a Zero Trust Architecture integrated with AI-behavior analytics to enhance the security of Industrial Control Systems in energy networks. The framework is designed to shift the paradigm from perimeter security to real-time continuous monitoring of user or device activities, which is crucial for SCADA systems. It includes continuous authentication, micro-segmentation, and identity management for greater protection [21].

Table 1 Comparative Analysis of Existing Zero Trust Security Approaches

Author	Year	Core Focus	Key Method	Contribution
Mensah [1]	2024	Enterprise ZT Strategies	Logical Architecture Analysis	Traces NIST/Forrester principles into modern decentralized edge networks.
Ahmadi [2]	2024	Cloud Network Security	Qualitative Thematic Review	Analyzes ZTA's impact on mitigating lateral movement in cloud-native systems.

Adanigbo et al. [3]	2024	Multi-Cloud Microservices	Synthesis of Industry Best Practices	Proposes a framework for policy consistency across heterogeneous cloud platforms.
Jaidi [4]	2025	Adaptive Middleware	AI-driven Policy Learning	Introduces "pluggable" middleware using real-time context for access decisions.
Iqbal & Abbas [5]	2024	Federated Environments	Identity-centric Implementation	Operationalizes ZT to reduce attack surfaces in multi-tenant cyber environments.
Ogendi [6]	2025	Cybersecurity Analytics	ML & Behavioral Analytics	Reinforces ZTA with predictive threat detection and automated response.
Guo et al. [7]	2023	Intelligent SDN	Deep Learning	Achieves 99.56% anomaly detection accuracy using the CALSeq2Seq model.
Lilhore et al. [8]	2025	SmartTrust Framework	Hybrid DL (CNN-LSTM-Transformer)	Uses Reinforcement Learning for dynamic trust adjustment in cloud traffic.
Ma et al. [9]	2025	Lightweight IoT	FAST-SM9 Cryptography	Reduces energy by 63% and latency by 56% for resource-poor "end" devices.
Pokhrel et al. [10]	2024	Federated Learning	Joint Blockchain & Anomaly Detection	Jointly uses Blockchain and FL to detect zero-day attacks while preserving privacy.
Aljohani [11]	2023	Privacy & Anonymization	Presidio Tool Evaluation	Successfully masks PII in cryptographic enterprise systems using the Presidio tool.
Fischer [12]	Jan 2026	IoT / Industry 4.0	Theoretical /Analytical Framework	Architecting trustless security specifically for distributed micro-

				industrial services.
Zanasi et al. [13]	2024	Industrial IoT (IIoT)	SDN-based Micro-segmentation	Offers a unified SDN abstraction layer for policy enforcement across IIoT assets.
Nie et al. [14]	2025	6G IoT Access Control	Blockchain & Inner-Product Encryption	Improves encryption efficiency by 14% and reduces latency by 18% in 6G.
Chen et al. [15]	2022	6G Security	Software-Defined ZTA	Uses collaborative control domains to secure high-volume 6G connectivity.
Ramezanpour & Jagannath [16]	2022	Intelligent ZT (i-ZTA)	O-RAN & MED Components	Leverages O-RAN interfaces for real-time Monitoring Evaluating-Deciding (MED). .
Kanuri [17]	2025	Unified Communications	Modular Trust Engine Framework	Secures collaborative remote sessions through a modular Trust Engine framework.
Rautaray [18]	2025	Insider Threat Mitigation	Multi-sector Case Studies	Demonstrates a 67-73% reduction in insider threat incidents across healthcare.
Kumar [19]	2025	Software Development	DevSecOps Lifecycle Integration	Integrates ZT verification directly into modern software engineering pipelines.
Zohaib et al. [20]	2024	Zero Trust VPN (ZT-VPN)	SD-WAN & SASE Integration	Replaces legacy VPNs with ZTNA at the edge to solve performance/security flaws.
James et al. [21]	2023	Energy Distribution ICS	AI-based Behavior Analytics	Autonomously detects operational deviations in critical power grid SCADA systems.

III. METHODOLOGY

The first step was to identify the problem space and scope of the study. Zero Trust Security is a very wide area, so it was decided to limit the scope to its architecture, components, and its use in modern networking environments like cloud, IoT and distributed systems. This enabled the exclusion of irrelevant information and ensured the study was focused. After that, research papers were searched from reputed academic websites like IEEE Xplore, Springer, ScienceDirect and Google Scholar. Appropriate papers were found using a keyword search method. Some of the keywords used were "Zero Trust Architecture", "ZTNA", "Zero trust in cloud", "micro segmentation security". The search targeted research articles that were published in 2020-2026.

A large number of papers were first identified and then filtered. Those that were not specifically focused on Zero Trust or had insufficient technical details were excluded. Those that presented models, frameworks or implementation were preferred. Lastly, a subset of papers was chosen for further study. Then, the papers were examined in detail. Relevant information, including the methodology, techniques, technologies, domain of application and findings was recorded. Special attention was given to techniques like identity-based access control, micro-segmentation, artificial intelligence, and blockchain integration.

After thoroughly reviewing the papers, a comparative analysis was conducted to determine commonalities and variations between them. This analysis helped to know what techniques are used, and what approach offers better outcomes. In addition, a comparison table was introduced to clearly present this analysis.

Following the analysis of the selected papers, trends were identified. It was noted that emerging research is focusing on incorporating Zero Trust with other technologies such as machine learning and blockchains. Additionally, some of the challenges were noted, including complexity of implementation, lack of scalability and absence of networks. These identified gaps suggest the need for research. The study simplifies the operation of Zero Trust systems by assuming that the decision to allow or deny access is not just based on a particular factor but on a range of factors, including identity, device status, context and risk. This is in line with the understanding that security decision making is not static but rather evolving.

IV. RESEARCH GAP AND FUTURE ROADMAP

A. Research Gaps Identified

Based on the existing literature available for Zero Trust Security the following issues are detected where more work has to be done; these are mainly focusing on theoretical or isolated environments rather than a fully integrated and scalable system [1-3]. This reflects a need for practical and adaptable systems.

One of the many problems found in the reviewed studies is the lack of consistency and standardization in the reference architecture of Zero Trust [4-6]. Current research is narrowed towards specific domains such as cloud, IoT, enterprise etc [7]. which reduces interoperability and scalability across different models, leading to the need for a flexible, cross domain structure [8]. Another limitation is the poor level of integration with legacy systems, with very few studies offering a real-world approach for migrating or hybrid deployment option for Zero Trust [9-10].

Besides, the current work does not provide a balance between static and dynamic security models [11-12]. Static rule-based systems are stable and inflexible, while fully dynamic systems are adaptable but complicated and resource-intensive. Limited work exists that combines both stability and adaptability that is necessary for deployment in practice, as a hybrid model [13-14]. Moreover, not many studies consider the effect of security measures on the usability and performance of the system [15-16]. Ruddy authentication and monitoring can stifle workflows, particularly in highly time-sensitive environments, highlighting the need for more user-aware and context-driven security designs [17].

Finally, the absence of long-term adaptability in Zero Trust system is a significant gap [18]. Most frameworks are reactive and are not built to adapt to the changing threat landscape, which decreases their longevity. Further research should be conducted on designing an automatic and intelligent security system with the ability to learn and adapt [19]. For wireless networks, there are extra obstacles to overcome, including the mobility of devices, network variability, and management of a large number of devices in a

wireless setting, which makes it even more crucial to find lightweight, scalable, and adaptive solutions that accommodate changing wireless environments [20-21].

B. Future Research Roadmap

The next phase in Zero Trust should shift from theoretical models to deployable systems. That will need a modular, standardized framework that can be used across each of the various environments, from cloud to enterprise network, and that will enable organizations to incrementally move to more robust security layers without having to replace their current infrastructure. AI/ML can be leveraged for their ability to trigger real-time alerts on user behavior and detect threats, and Blockchain can help with decentralized identity management, eliminating single points of failure. Future systems need to be neither rule-based nor fully dynamic, but they must have some stability for normal activities but be adaptable for unusual ones. A key aspect is lightweight and efficient solutions, particularly for resource-constrained environments like IoT devices, sensors, and industrial systems. Security mechanisms should be designed to be both performance and power efficient, as well as enabling hybrid implementations where legacy systems are used safely with modern infrastructure. Lastly, Zero Trust needs to become a self-learning system, adapting itself to changing conditions, and improving gradually over time. Especially in wireless networks, where mobility, variable connectivity and large number of devices necessitate flexible and responsive security mechanisms. Rather than needing constant manual updates, future systems should be adaptive and reliable, functioning seamlessly as a part of normal business operations and providing long-term solutions to meet the needs of the changing cyber landscape.

V. CONCLUSION

Zero Trust Security has emerged as a necessary shift in modern cybersecurity, especially as traditional perimeter-based models continue to lose effectiveness. Built on the principle of “never trust, always verify”, it enforces continue authentication and context-aware access across systems such as cloud, IoT, and advanced networks. A review of existing research shows that most proposed models remain limited to specific domains or controlled settings, creating a gap between theory and real-world implementation. Also, maintaining a balance between strong security and system performance remains a challenge, as rigid controls can affect system usability while adaptive system increase complexity. Many Zero Trust approaches lack long-term adaptability and practical integration strategies, highlighting the need for scalable, flexible, and self-adaptive solutions for effective deployment.

REFERENCES

[1] F. Mensah, "Zero Trust Architecture: A Comprehensive Review of Principles, Implementation Strategies, and Future Directions in Enterprise Cybersecurity," Int. J. Adv. Res. Ideas Innov. Technol., vol. 10, no. 6, 2024.

[2] S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," J. Eng. Res. Rep., vol. 26, no. 2, pp. 215–228, Feb. 2024.

[3] O. S. Adanigbo et al., "Implementing Zero Trust Security in Multi-Cloud Microservices Platforms: A Review and Architectural Framework," Int. J. Adv. Multidiscip. Res. Stud., vol. 4, no. 6, pp. 2402–2409, 2024.

[4] S. R. Jaidi, "Adaptive Zero-Trust Middleware Architecture for Decentralized Cloud Integrations: A Dynamic Policy Enforcement Framework," J. Comput. Sci. Technol. Stud., vol. 7, no. 3, Sep. 2025.

[5] J. Iqbal and A. Abbas, "Operationalizing Zero-Trust Principles in Federated and Distributed Cyber Environments," Preprint, Dec. 2024.

[6] E. G. Ogendi, "Leveraging Advanced Cybersecurity Analytics to Reinforce Zero-Trust Architectures within Adaptive Security Frameworks," Int. J. Res. Publ. Rev., vol. 6, no. 2, pp. 691–704, Feb. 2025.

[7] X. Guo et al., "An intelligent zero trust secure framework for software defined networking," PeerJ Comput. Sci., vol. 9, p. e1674, Nov. 2023.

[8] U. K. Lilhore et al., "SmartTrust: a hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture," J. Cloud Comput., vol. 14, no. 1, p. 35, 2025.

[9] Z. Ma et al., "A lightweight zero-trust authentication architecture for IoT via unified

enhanced FAST-SM9 and dynamic re-authentication," PLoS ONE, vol. 20, no. 10, p. e0332943, Oct. 2025.

[10] S. R. Pokhrel, L. Yang, S. Rajasegarar, and G. Li, "Robust Zero Trust Architecture: Joint Blockchain based Federated learning and Anomaly Detection based Framework," arXiv preprint arXiv:2406.17172, Jun. 2024.

[11] A. Aljohani, "Zero-Trust Architecture: Implementing and Evaluating Security Measures in Modern Enterprise Networks," Shifra, vol. 2023, pp. 1–13, Jul. 2023.

[12] L. K. Fischer, "Architecting Trustless Cybersecurity: A Comprehensive Theoretical Framework for Zero-Trust Architecture in IoT, Industry 4.0, and Distributed Systems," Eur. Int. J. Multidiscip. Res. Manag. Stud., vol. 6, no. 1, pp. 215–226, Jan. 2026.

[13] C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," Ad Hoc Netw., vol. 156, p. 103414, 2024.

[14] S. Nie et al., "Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment," Sensors, vol. 25, no. 2, p. 550, Jan. 2025.

[15] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero Trust Architecture for 6G Security," arXiv preprint arXiv:2203.07716, Mar. 2022.

[16] K. Ramezanpour and J. Jagannath, "Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN," arXiv preprint arXiv:2105.01478, Jul. 2022.

[17] P. K. Kanuri, "Zero Trust Security Architecture for Unified Communications in Distributed Enterprise Environments," Int. J. Comput. Math. Ideas, vol. 17, no. 2, pp. 17299–17312, Feb. 2025.

[18] A. Rautaray, "Implementing a Zero-Trust Security Framework to Mitigate Insider Threats in Cloud-Based Infrastructure," Power Syst. Prot. Control, no. 244, Jul. 2025.

[19] P. Kumar, "A Zero Trust-Based Approach to Modern Cybersecurity Challenges in Software Development," Int. J. Emerg. Res., vol. 5, no. 2, Aug. 2025.

[20] S. M. Zohaib et al., "Zero Trust VPN (ZT-VPN): A Cybersecurity Framework for Modern Enterprises to Enhance IT Security and Privacy in Remote Work Environments," Preprints.org, Oct. 2024.

[21] U. U. James, C. N. Idika, and L. A. Enyejo, "Zero Trust Architecture Leveraging AI-Driven Behavior Analytics for Industrial Control Systems in Energy Distribution Networks," Int. J. Sci. Res. Computer. Sci. Eng. Inf. Technol., vol. 9, no. 4, pp. 685–709, Jul. 2023.