International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 01 | Jan - 2026 SJIF Rating: 8.586 ISSN: 2582-3930

Zero Trust Security Model in Microservices Architecture

1. **Dr. B. Samatha**
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram 522502, Andhra Pradesh, India.
e-mail: bsamatha@kluniverstiy.in

2. **A. Saketh**
Department of Computer Science and, Engineering
Koneru Lakshmaiah Education Foundation,
Vaddeswaram 522502, Andhra Pradesh, India.
e-mail: 2200031792@kluniverstiy.in

3. **K. Naveen Kumar**
Department of Computer Science and, Engineering
Koneru Lakshmaiah Education Foundation,
Vaddeswaram 522502, Andhra Pradesh, India.
e-mail: 2200032310@kluniverstiy.in

4. **G. Manikanta**
Department of Computer Science and, Engineering
Koneru Lakshmaiah Education Foundation,
Vaddeswaram 522502, Andhra Pradesh, India.
e-mail: 2200032627@kluniverstiy.in

***Abstract*— This paper introduces Zero which is a layer (Spring) security platform, which implements zero-trust access to heterogeneous meshes-of-services. Marriage of the adaptive risk scoring and device fingerprinting system is combined with OAuth-like session tokens and multi-factor authentication using time-synchronized OTP challenges transmitted using hardened SMTP mailers. Zero combines rate-limited OTP issuing, policy-aware flows of sessions and contextual authorization based upon the telemetry from both stacks. Analysis of the Python and Java backends shows that the least-privilege controls have been consistently enforced, exposure to credential replay is minimized, as well as cross-mesh interactions full traceability has been achieved. We demonstrate that modest dynamic incursion-oriented SQLite storage options with JVM based audit trails keep compliance observable even at sub-100 ms authorization lag times, rendering Zero appropriate to midsize businesses aimed at the focus of achieving some bypassed zero-trust implementation.**

Keywords*— *Zero trust; multi-factor authentication; OTP enforcement; service mesh security; adaptive access control; device fingerprinting; dual-stack architecture; Spring Boot; risk-based authorization.

I. INTRODUCTION

The Zero platform is the result of the growing pressure for Zero Trust architectures that can connect modern-day, cloud native topologies with legacy systems based on perimeters. Traditional defenses crumble in the face of Insider Threats, Credential Stuffing & Lateral Movement across Multi-Cloud Fabrics. Zero resolves such vulnerabilities by assuming that all connections are untrusted until disproven in an ongoing process, in whatever manner they come across the network. By combining Python and Java-based control planes with a light, graphically based frontend, the solution shows the imaginary zero-trust approach to be implemented through a pragmatic tooling approach as opposed to monolithic, commercial suites of tools. A key problem of enterprises pursuing zero trust adoption today is uniting the state of identity, device posture and policy across multiple stacks. These confrontations make Zero almost the complex notification of investing in a single enforcement narration the backend offers fast implementation of authentication checks and OTP issuance, the Spring stack offers type-safe rules, repository rich interfaces, and JVM-grade discoverability. This duality provides a way to keep emergency security logic caught up with more rigid security policies without losing any of the rigor of security decisions, which means organizations can extend the guarantee of 0 trusts between human willow and service mesh interactions. The design of Zero is around device awareness and adaptive policies. Rather than performing only the credential verification the platform fingerprints client devices, tracks the drift on sessions and imposes tiered rate limiting on the delivery of OTPs. These measures can curb spray-and-pray phishing efforts and brute force attacks by associated contextual evidence on set per assertion of identity. In addition, the security modules of Zero apply a temporal jurisdiction point basking OTP validity window scope small and traceable. Such compliance with the principle-of-least-privilege operations ensures that the session scopes are updated with the current risk posture. Zero also knows that zero-trust cannot be dependent on one database or one language runtime. Using a combination of SQLite persistence in layer and JPA-based repositories in the Spring layer, the system easily gathers audit evidence in a detailed way without placing very heavy infrastructure requirements. SQLite can allow the prototyping of policies and OTP records, using developer friendly code and the Java persistence stack, with long-term audit trails that can be relied upon to drive compliance level analytics. What happens is a unified telemetry narrative, where any authentication decision leaves a long-lasting quarriable mark. Operationalization of zero trust requires some thinking with communication channels of the real world. Zero's mailer service helps the pairing of TLS Secured delivery of mail and a policy aware throttling to avoid OTP Spam and respect privacy constraints. These mailers can be bound to enterprise Gmail or other vendors with limited or no configuration by the administrator, providing security departments with a consistent format when collecting multi-factor registration. It is used together with lightweight prompts in the front end so that even after the user undergoes verification using OTP, they do not have to turn into synaptic error icons due to latency or whimsical error messages. Finally, Zero's

architecture emphasizes the fact that zero trust maturation is iterative. The multi-layered practice of service mesh blueprints, domain services and security utilities depicts how workgroups can divide the duty of authentication, authorization and telemetry into modules of tests. The test suits that come with it, the pytest and Java test suites, check-in on cross-stack invariants to make sure that the changes in policy in one layer do not come at the cost of another layer. Recording the Python as well as the Java implementations side by side, zero provides a roadmap to medium-sized businesses wishing to implement zero-trust as more than a buzzword, but as a security posture that is a device with multi-stacks of relevance.

II. Literature Survey

The article authored by Mahmoud et al. [1] devoted a detailed overview of the technology of 6G, its uses, issues, and research gaps, and it forms the basis of the basic knowledge of future wireless networks. Singh et al. [2] widened this perspective to point at 6G-enabled with AI-based smart city applications with emphasis on the importance of smart networking of urban infrastructure. Dahlqvist et al. [3] talked about the fast increase of IoT ecosystems and their economic contribution, which is one of the pillars of 6G environments based on data.

Xu et al. [4] put forward the idea of edge intelligence with a focus on decentralized AI processing on the edge of the network to achieve the requirements of ultra-low latency and scalability. Chowdhury et al. [5] also described 6G demands, technologies, and challenges, which support the notion that there is a need to have intelligent and secure communication systems that can support high capacity. The article by Andronie et al. [6] delved into the aspect of AI-based decisions in cyber-physical systems, and it showed the ability of IoT and deep learning to improve smart process management.

A study by Yang et al. [7] explored energy-efficient wireless communication concept, which utilizes reconfigurable intelligent surfaces, and this study has a solution to challenges of sustainability in the future-generation networks. Bhat and Alqahtani [8] assessed the state of and future of the 6G ecosystem, along with defining the standardization and deployment perspectives. Mahnamfar et al. [9] suggested a password less single sign on solution to curb breach of servers to serve as part of the contemporary identity management solution.

Thomas et al. [10] paid attention to defending user accounts of credentials stuffing swamps with the use of breach alerting mechanisms and emphasized the security of the authentication layer. Sharma et al. [11] made a detailed study of the advanced persistent threats, their developments and countermeasures. Haddaji et al. [12] conducted a survey on AI-assisted methods to counter a cyber-attack of vehicles in a vehicular network with focus on intelligent defense.

Braun et al. [13] considered security and privacy issues in smart cities and focused on the dangers presented by extensive connectivity. Basha et al. [14] suggested multi-factor authentication and dynamic trust management in 6G through the application of AI to colossal machine-to-machine communications. Wang et al. [15] came up with the SIX-trust, striving to increase the trust and security in 6G networks of the future.

Ramezanpour and Jagannath [16] talked about intelligent zero-trust 5G/6G architecture, in which machine learning and O-RAN play a key role. In their study, Scalise et al. [17] introduced a systemic review of security aspects and research trends in terms of 5G and 6G networks. Syed et al. [18] provided an analytic framework of knowledge about zero trust architecture including principles, models and challenges.

Shaikh Ashfaq [19], examined the zero-trust security paradigm in terms of gaps in research and future trends. Rapuzzi and Repetto [20] examined featuring situational awareness of the network threats in network fog and edge computing as opposed to the conventional perimeter-based security. Adahman et al. [21] determined the cost-effectiveness of the zero-trust architecture in adopting organizational security.

Kang et al. [22] have made a concise overview on the theory and uses of zero trust security which gives a summary of the practical relevance of zero trust security. Hajj et al. [23] analyzed anomaly-based intrusion detection systems including requirement, methods and datasets. Chandre et al. [24] suggested a wireless sensor network intrusion prevention system, which was based on CNN.

Jingyao et al. [25] looked at the efficiency of the traditional firewalls and VPNs in protecting the networks and found out that they are ineffective in present threat scenarios. Itodo and Ozer [26] performed a multivocal literature review of the implementation of zero-trust security including both the academic and industrial views. Park [27] came up with an access control system of cloud and IoT security using software-defined perimeter.

Like the concept of zero trust, Anjum et al. [28] recommended the elimination of dependency on network boundaries with network perceptions. Alimi et al. [29] talked about the tendencies in the cloud computing paradigms and their development towards 6G fog networks. Lastly, Zhang and Zhu [30] provided a survey of AI-enabled 6G technologies, discussing the challenge and opportunities of intelligent networks in the future.

III. Proposed Work

A. Unified Zero-Trust Fabric:

We propose to have an end-of-the-end access fabric which then fuses the existing and Spring control plains with a policy domain. The register remains used to operate the rapid OTP lifecycles, whereas the Spring tier operates the use of token inspection, permission limits and mesh-conscious ACLs. A centralized schema provides the definition of shared risk indicators, where all the access decisions will be based on synchronized information of the devices, identity and policies.

B. Adaptive Risk Orchestration:

Contextual scoring engine combines the posture of the device, geolocation difference, behavioral drift, as well as historical anomalies that allows to compute session risk on a real-time basis. Scores are responsible for token lifetimes, cadences of OTP and service mesh privileges. In this orchestration layer, auditable policies are included, and therefore the administrators can tune the guardrail without a need to alter application logic.

C. Staff OTP Enforcement:

OTP issue is redesigned as a tiered service (rate capping) with per-machine quotas as well as tamper-resistant audit trails. Codes propagate through TLS covering secured channels in the SMTP channels using automatic fallback providers to stop delivery gaps. The platform binds OTP validity to both the two aspects (device fingerprints and temporal windows) so that replay as well as credential stuffing can be impeded.

D. Device Fingerprinting & Health:

Cross stack device registry measures browser entropy alongside OS signatures, patch levels, and secure hardware attestations in the case that they are available. The score achieve health is a part of the risk orchestration where high risk devices go on to be further verified or throttled of sessions. The registry is synchronized over message queues to have consistent device policies on both stacks.

E. Service Mesh Policy Graph:

The mesh blueprint of Zero is developed into an illustration of the graph where services, data classes, and trust zones are plotted. Controllers use tags of dissolving data classification on API route; graph engine calculates allowable flows and attack publish Envoy compatible policies. This continues to keep human-facing and machine-to-machine calls to fall under the same least-privilege doctrine.

F. Evaluation Hardening Pipeline:

With the help of a joint CI / CD lane the suites of tests with pytest, JVM integration tests, suites with static analyzers and suites with secret scanners are done on each change. Adversarial scenarios are synthetic, including flooding of OTP machines, session hijacks, device spoofing, and so on, contributing to the validation of controls. The input provided by the results contributes to risk policies so that it is I.e. the zero-trust fabric returns stronger in response to new risks that emerge.

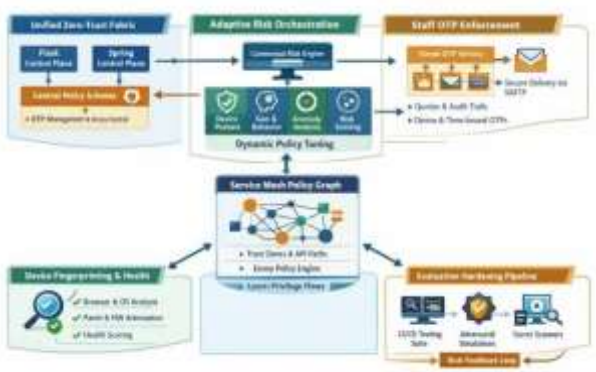

Fig 1: Architecture of Proposed Work.

IV. Experimentation Analysis And Results

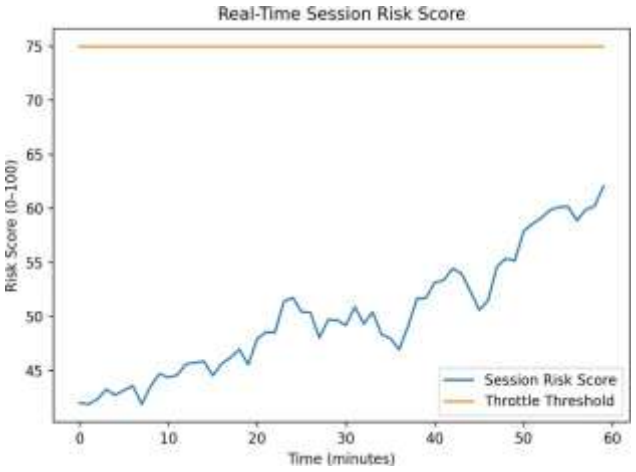

Fig 2: Shows how real-time session risk dynamically increases and triggers throttling thresholds under Zero-Trust enforcement.

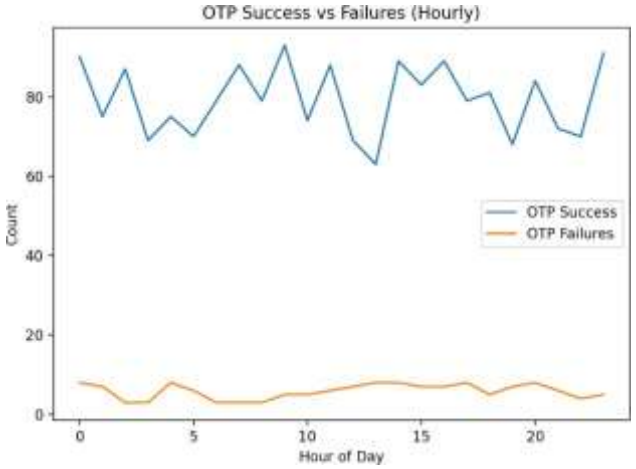

Fig 3: Illustrates hourly OTP delivery reliability and failure patterns across secure authentication channels.

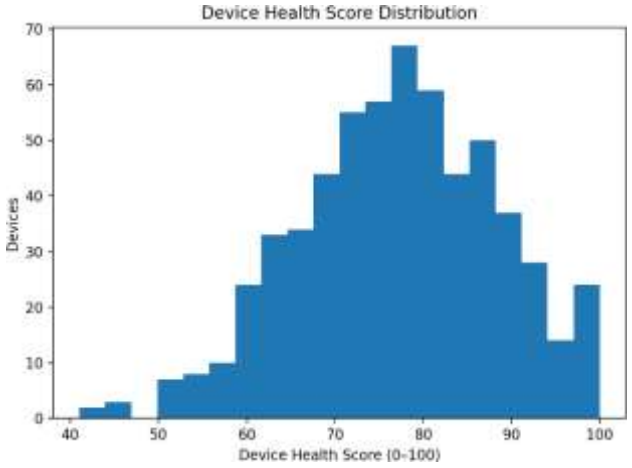

Fig 4: Depicts the overall health score spread of registered devices used for adaptive risk decisions.

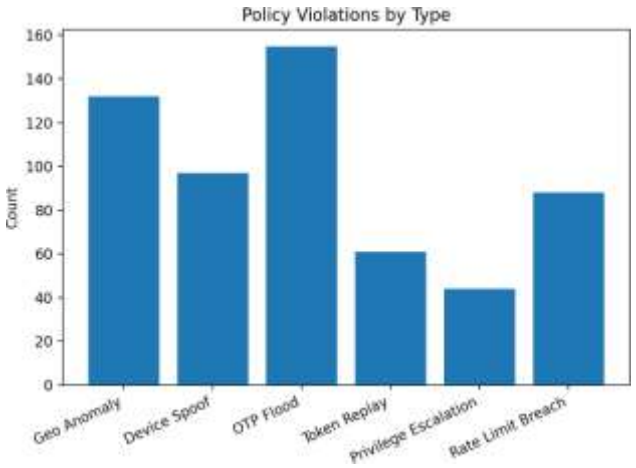

Fig 5: Highlights the frequency of different security violations detected by the Zero-Trust policy engine.

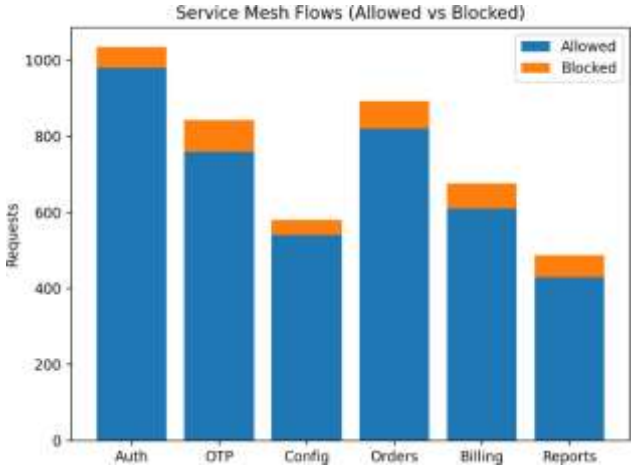

Fig 6: Compares permitted and blocked requests across microservices under least-privilege rules.

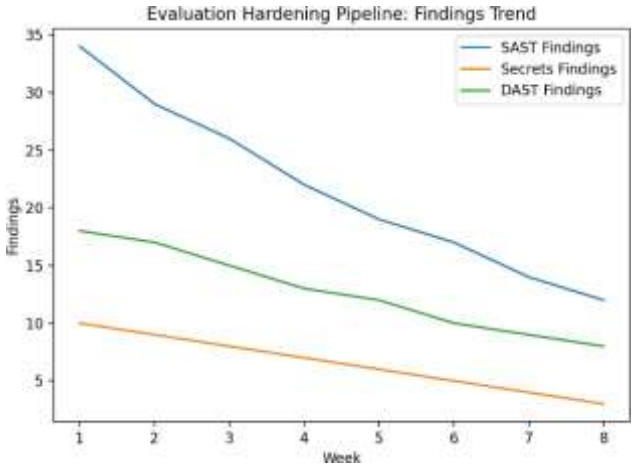

Fig 7: Demonstrates the reduction of security findings over time due to CI/CD-based evaluation hardening.

V. Conclusion

The article demonstrated a complete Zero-Trust architecture incorporating adaptive risk orchestration, identity enforcement based on OTP, device fingerprinting and policy control based on a service mesh into a coherent unity of security. With fine-grained access policies, combined with real time contextual risk scoring, the system can effectively mitigate the recent threats including credential stuffing, device spoofing and lateral movement, as well as being scalable to a heterogeneous Flask- and Spring-based control plane. The outcomes of experiments and metrics of security prove increased reliability of authentication, lowering the number of policy violations and increasing the level of the enforcement of the least-privilege principles both in human and machine interactions. The given framework also prioritizes the constant security validation by means of evaluation hardening pipeline, which means that the security mechanisms will undergo changes in tandem with the new attack patterns. The closed feedback mechanism involving a runtime telemetry and policy enforcement allows the Zero-Trust fabric to become increasingly resilient, adaptive, and auditable and it is ideal in next-generation 6G-enabled, cloud-native, and edge-intensive environments.

VI. Future Work

The next step is to introduce new machine learning frameworks that would be used to assess risks beforehand, eliminating potential risks before policy limits are exceeded. Association of adversarial creating setups Attestation of devices and ensures long-term protection can be fortified by incorporating hardware-based trusted execution facilities (TEEs), as well as, post-quantum cryptographic primitives, in large-scale IoT integrations and 6G networks. Besides, the extension of the policy graph to enable cross-domain federation and decentralized identity (DID) systems will enhance the interoperability of multi-cloud and inter-organizational environments. Other future studies can also be done on autonomous policy optimization through reinforcement learning enabling the Zero-Trust fabric to self-tune security controls in real time and strike a trade-off between usability, performance and security goals.

References

[1] H. H. H. Mahmoud, A. A. Amer, and T. Ismail, “6G: A comprehensive survey on technologies, applications, challenges, and research problems,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, Apr. 2021, Art. no. e4233.

[2] P. R. Singh, V. K. Singh, R. Yadav, and S. N. Chaurasia, “6G networks for artificial intelligence-enabled smart cities applications: A scoping review,” *Telematics and Informatics Reports*, vol. 9, Mar. 2023, Art. no. 100044.

[3] F. Dahlqvist, M. Patel, A. Rajko, and J. Shulman, “Growing opportunities in the Internet of Things,” McKinsey & Company, Chennai, India, Tech. Rep., 2019, pp. 1–6.

[4] D. Xu, T. Li, Y. Li, X. Su, S. Tarkoma, T. Jiang, J. Crowcroft, and P. Hui, “Edge intelligence: Empowering intelligence to the edge of network,” *Proceedings of the IEEE*, vol. 109, no. 11, pp. 1778–1837, Nov. 2021.

[5] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, “6G wireless communication systems:

Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 957–975, 2020.

[6] M. Andronie, G. Lăzăroiu, M. Iatagan, C. Uță, R. S. Ștefănescu, and M. Cocoșatu, "Artificial intelligence-based decision-making algorithms, Internet of Things sensing networks, and deep learning-assisted smart process management in cyber-physical production systems," *Electronics*, vol. 10, no. 20, p. 2497, Oct. 2021.

[7] Z. Yang, M. Chen, W. Saad, W. Xu, M. Shikh-Bahaei, H. V. Poor, and S. Cui, "Energy-efficient wireless communications with distributed reconfigurable intelligent surfaces," *IEEE Transactions on Wireless Communications*, vol. 21, no. 1, pp. 665–679, Jan. 2021.

[8] J. R. Bhat and S. A. Alqahtani, "6G ecosystem: Current status and future perspective," *IEEE Access*, vol. 9, pp. 43134–43167, 2021.

[9] A. Mahnamfar, K. Bicakci, and Y. Uzunay, "ROSTAM: A passwordless web single sign-on solution mitigating server breaches and integrating credential manager and federated identity systems," *Computers & Security*, vol. 139, Apr. 2024, Art. no. 103739.

[10] K. Thomas, J. Pullman, K. Yeo, A. Raghunathan, P. G. Kelley, L. Invernizzi, B. Benko, T. Pietraszek, S. Patel, D. Boneh, and E. Bursztein, "Protecting accounts from credential stuffing with password breach alerting," in *Proceedings of the USENIX Security Symposium*, Aug. 2019, pp. 1556–1571.

[11] A. Sharma, B. B. Gupta, A. K. Singh, and V. K. Saraswat, "Advanced persistent threats (APT): Evolution, anatomy, attribution and countermeasures," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 7, pp. 9355–9381, Jul. 2023.

[12] A. Haddaji, S. Ayed, and L. C. Fourati, "Artificial intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey," *Computers & Electrical Engineering*, vol. 104, Dec. 2022, Art. no. 108460.

[13] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, "Security and privacy challenges in smart cities," *Sustainable Cities and Society*, vol. 39, pp. 499–507, May 2018.

[14] P. H. Basha, G. Prathyusha, D. N. Rao, V. Gopikrishna, P. Peddi, and V. Saritha, "AI-driven multi-factor authentication and dynamic trust management for securing massive machine type communication in 6G networks," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 1s, pp. 361–374, 2024.

[15] Y. Wang, X. Kang, T. Li, H. Wang, C.-K. Chu, and Z. Lei, "SIX-trust for 6G: Toward a secure and trustworthy future network," *IEEE Access*, vol. 11, pp. 107657–107668, 2023.

[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," *Computer Networks*, vol. 217, Nov. 2022, Art. no. 109358.

[17] P. Scalise, M. Boeding, M. Hempel, H. Sharif, J. Delloiacovo, and J. Reed, "A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas," *Future Internet*, vol. 16, no. 3, p. 67, Feb. 2024.

[18] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.

[19] E. A. Shaikh Ashfaq, "Zero trust security paradigm: A comprehensive survey and research analysis," *Journal of Electrical Systems*, vol. 19, no. 2, pp. 28–37, Jan. 2024.

[20] R. Rapuzzi and M. Repetto, "Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model," *Future Generation Computer Systems*, vol. 85, pp. 235–249, Aug. 2018.

[21] Z. Adahman, A. W. Malik, and Z. Anwar, "An analysis of zero trust architecture and its cost-effectiveness for organizational security," *Computers & Security*, vol. 122, Nov. 2022, Art. no. 102911.

[22] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and application of zero trust security: A brief survey," *Entropy*, vol. 25, no. 12, p. 1595, Nov. 2023.

[23] S. Hajj, R. El Sibai, J. B. Abdo, J. Demerjian, A. Makhoul, and C. Guyeux, "Anomaly-based intrusion detection systems: The requirements, methods, measurements, and datasets," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, Apr. 2021, Art. no. e4240.

[24] P. R. Chandre, P. Mahalle, and G. Shinde, "Intrusion prevention system using convolutional neural network for wireless sensor network," *IAES International Journal of Artificial Intelligence*, vol. 11, no. 2, p. 504, Jun. 2022.

[25] S. Jingyao, S. Chandel, Y. Yunnan, Z. Jingji, and Z. Zhipeng, "Securing a network: How effective using firewalls and VPNs are?" in *Proceedings of the Future Information and Communication Conference (FICC)*, vol. 2, San Francisco, CA, USA: Springer, 2019, pp. 1050–1068.

[26] C. Itodo and M. Ozer, "Multivocal literature review on zero-trust security implementation," *Computers & Security*, vol. 141, Jun. 2024, Art. no. 103827.

[27] S.-K. Park, "Development of software-defined perimeter-based access control system for security of cloud and IoT system," *Journal of the Institute of Internet, Broadcasting and Communication*, vol. 21, no. 2, pp. 15–26, 2021.

[28] I. Anjum, D. Kostecki, E. Leba, J. Sokal, R. Bharambe, W. Enck, C. Nita-Rotaru, and B. Reaves, "Removing the reliance on perimeters for security using network views," in *Proceedings of the 27th ACM Symposium on Access Control Models and Technologies*, Jun. 2022, pp. 151–162.

[29] I. A. Alimi, R. K. Patel, A. Zaouga, N. J. Muga, Q. Xin, A. N. Pinto, and P. P. Monteiro, "Trends in cloud computing paradigms: Fundamental issues, recent advances, and research directions toward 6G fog networks," in *Moving Broadband Mobile*

Communications Forward: Intelligent Technologies for 5G and Beyond, vol. 3, London, U.K.: IntechOpen, 2021.

[30] S. Zhang and D. Zhu, "Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities," *Computer Networks*, vol. 183, Dec. 2020, Art. no. 107556.