Zero Trust Network Access

Aaron Thach
Department of Computer Science
Emory University
Atlanta, Georgia, USA
athach@emory.edu

Varun Pawar Jetling
Department of Computer Science
Emory University
Atlanta, Georgia, USA
varun.pawar.jetling@emory.edu

Wenzhuo Fan
Department of Computer Science
Emory University
Atlanta, Georgia, USA
wenzhuo.fan@emory.edu

Abstract—**The advances in information technology, such as cloud computing and the Internet of Things (IoT), have exacerbated the complexity and frequency of cybersecurity threats. The advent of the Zero Trust Security framework follows the realization that the traditional perimeter-based security mechanisms are doomed to fail against the onslaught of these sophisticated threats. Zero Trust works with the philosophy that no entity on the network of an organization should be trusted by default. This significantly reduces the risk of data breaches and lateral movement in the event of a compromise in security. In this paper, we consider the evolution of Zero Trust Architecture history and major fundamental principles that underscore a paradigm shift from traditional security models to a framework insisting upon dynamic authentication, stringent access control, and continuous monitoring. We explore how zero trust principles had been implemented in areas such as its control modules and identify assurance infrastructure. In this paper, we give a comprehensive view of how AI integrates with the Zero Trust model and focuses on the application of Q-learning. The integration of this is expected to improve the security framework through more adaptable, efficient, and automated handling of network access and security verification. This review synthesized existing knowledge, analyzed Zero Trust implementation effectiveness, and suggested the way forward for future research. The focus was highlighting problems and possibilities of deploying AI-enhanced zero trust strategies in modern network environments that represent a strong shift toward more resilient cybersecurity architectures.**

Index Terms—Zero Trust Architecture, Cybersecurity, Q-Learning, Network Security

I. Introduction

The introduction of new technologies, such as cloud computing and the Internet of Things (IoT), in the last few decades has created a more complex and dynamic technological landscape, leading to an increase in the number and sophistication of security attacks on businesses [1]. Zero Trust is a security framework proposed as a response to the increasingly complex enterprise infrastructure that the traditional perimeter-based security measures struggle to address effectively. The Zero Trust model operates on the assumption that no entity within an enterprise's environment can be inherently trusted, aiming to prevent data breaches and limit lateral movement within the network in the event of a breach. The Zero Trust Architecture Model consists of an interactive data platform, a supporting control platform, and an identity assurance infrastructure [2]. In this paper, we review the history of Zero Trust Architecture, emphasizing the need for a transition from perimeter-based security models. We provide a comprehensive overview of Zero Trust Architecture principles, including its logical components and deployment scenarios. Key tenets of Zero Trust Architecture involve dynamic authentication, strict access control, continuous monitoring, and adherence to least privilege principles. The control module manages continuous security monitoring, trust evaluation, and dynamic access control [3]. As the name suggests, Zero Trust Security initially assigns devices with minimum authority and permissions, then continuously evaluates access based on various attributes such as user identity, device security posture, and network location. Afterwards, dynamic access control allows or prohibits access to various resources based on the evaluation results [4]. We will also investigate the foundational assumptions for network connectivity within a Zero Trust Architecture framework and the logical components involved, including policy engines, enforcement points, and data sources for decision-making. These approaches encompass enhanced identity governance-driven, logical micro-segmentation, and network-based segmentation strategies. In this paper, we evaluate the effectiveness of implementing Zero Trust Architecture, and review an enhancement to the existing Zero Trust framework using artificial intelligence in the form of Q-Learning. We will also come up with our recommendations for future research in the field of Zero Trust Architecture. Our outcomes in this project include a synthesis of existing knowledge on Zero Trust Architecture, insights into the current state of Zero Trust Architecture and Q-Learning implementation and its impact on cybersecurity, our recommendations for the future of Zero Trust Architecture, and analysis of the papers in this field. We focus on improving the security and efficiency of the Zero Trust framework through the implementation of Q-Learning and discuss the challenges in implementing Q-Learning into Zero Trust security.

II. Related Work

In [5], researchers introduce the concept of Zero Trust Security to create an enhanced framework to secure data in the medical cloud and provide an advanced and specific access control process. In [6], researchers introduce a novel Zero Trust Network architecture called Zero Trust Service Function

Chaining, meant to address the lack of integration of monitoring and security functions in existing Zero Trust architectures. These monitoring and security functions include "intrusion prevention systems (IPS) for deep packet inspections (DPI), multi factor authentication systems (MFA) for prompting the client for additional authentication factors, or loggers for packet logging in the network" [6]. In [17], researchers implement a security evaluation model for IoT terminal access and network security based on Zero Trust. They found that it detects malicious access behavior and promotes system stability. While it isn't perfect, it improves the security of the IoT network. In [18], researchers proposed a Zero Trust model with integrated machine learning for security management in the financial sector. While this topic is very similar to ours, the researchers in this paper suggest machine learning as a general improvement to Zero Trust, but do not specifically review any particular machine learning algorithms or techniques. In [19], researchers proposed a Zero Trust-based security architecture to improve the security of token networks. Also, by utilizing the blockchain ledger, their proposal enhances the resilience and transparency of token networks. In [20], researchers provide a framework for securing 5G wireless networks using both Zero Trust, and Defense in Depth, in which multiple security layers are deployed to protect against threats to an organization's assets. The paper concluded that proactive security strategies are necessary to secure 5G networks today.

The concept of Zero Trust Network Access (ZTNA) has emerged as a prominent security model in response to the recent increase in cybersecurity threats. This section highlights key strategies and their implementation within the Zero Trust framework.

Zero Trust Principles: Moving from traditional perimeter-based security to Zero Trust is a radical rethinking of network trust. In ZTNA, each access request should be viewed as skeptical, thus requiring rigorous authentication and authorization. The intention is to minimize the possibility of lateral movement while enhancing overall network security [13].

Role of Artificial Intelligence in Zero Trust: Zero Trust Networking is based on artificial intelligence (AI). The integration of AI and machine learning will help an organization automate its complex decision-making processes, increase the efficiency of the organization, and improve real-time monitoring, which allows for an increase in the speed of work and the accuracy of access control. This then takes up the challenge of continuous verification, for the networks to keep their security tight without necessarily reducing efficiency [14].

AI-driven solutions help in identifying patterns and anomalies within network behaviors to continue to keep the detection and response mechanism of threats at a proactively maintained level [13].

Strategies for Zero Trust Network Access: ZTNA includes various strategies that ensure network security with the principle of Zero Trust.

- Principle of Least Privilege: This practice ensures the minimal level of access both users and devices should have to perform their tasks. This helps decrease the surface area for attack and minimizes potential threats.
- Role-Based Access Control (RBAC): This assigns access rights to users concerning the roles in a manner that ensures permissions granted relate to specified job functions. It enforces the least privilege principle so that users gain access only to the relevant resources.
- Multi-Factor Authentication (MFA): MFA requires a user to provide more than one kind of identification to grant access, adding various layers of security beyond traditional password protection [16]. Continuous MFA, therefore, would build on the above, whereby authentications of users are done in different touchpoints under an active session.
- Dynamic Access Control: In contrast, ZTNA depends on continuously updating access policies based on real-time risk assessment. It allows the organization to shift along with the changes in security threats and user behaviour in making access available only to meet particular security criteria.
- Continuous Monitoring and Verification: ZTNA includes actions on user activity, device health, and network traffic to determine the detected anomalies and potential threats. It ensures that continual monitoring activity is conducted, which can easily identify suspicious behaviour, in this essence, it responds to a security incident in real-time [16].
- Integration with Artificial Intelligence (AI): AI integration and the use of machine learning are increasingly being adopted in ZTNA to enable an automated decision-making process and enhance real-time monitoring. This can reduce pressure for verification every time and improve the accuracy of keeping access [14].
- Policy-Based Approach: This method identifies some specific access policies, which govern the way by which the users and their corresponding devices will gain access to the resources provided in the network. Policies are developed at distinct levels for the implication of security rules to be consistent.

These strategies form the foundation of Zero Trust Network Access, providing a comprehensive framework for building secure network environments while addressing the challenges of implementing Zero Trust.

Challenges and Considerations: Implementing Zero Trust can be costly and challenging, such as aligning with the existing infrastructure and robust authentication mechanism. The transition to Zero Trust needs a heavy investment of money, time, and expertise, making it essential to address potential roadblocks and ensure flexibility to adapt to evolving threats.

Zero Trust in the 5G and Beyond: The development of 5G and 6G networks brought new security issues. Zero trust becomes most relevant under these high-speed environments, with data volumes and device numbers much more than those deployed within traditional networks. An intelligent Zero Trust

architecture can use AI to govern dynamic access control in a 5G network, focusing on real-time monitoring and continuous risk assessment.

Zero Trust architecture for 5G draws new emphasis on advanced automation and orchestration to remain reliable with complex security controls of such network environments. The rapid development of 5G technology requires flexible and adaptive security strategies, and Zero Trust is an ideal approach for 5G networks.

User Education and Awareness: Zero Trust Networking includes an imperative part of user education and awareness. In Zero Trust, the users need to be warned about the principles of such a security model and the threats related to unallowable access, while the access requests need to be precise for the process of authentication and authorization. Organization should sensitize and educate the users to enforce and reduce the security breaches arising out of human errors.

Education plays a crucial role in helping ensure a smooth transition to Zero Trust. Organization can help shape a security culture and reduce resistance to change by clearly sharing with their users both new security policies and why they need to be in place.

These components form the basis of Zero Trust Network Access, underpinning the pivotal strategies and role of AI, 5G and user education in building secure network environments.

III. Challenges in Zero Trust Network Access

One of the core principles of the Zero Trust is, "Never Trust, and Always Verify" [9], which leads to strict control measures being taken before granting access to resources in the network requested by a device or a person. Every attempt to access network resources is treated with suspicion as to whether the request that is being made is genuine or not regardless of the origin of the request (whether from inside or outside of the network's perimeter). This leads to a longer verification process to authenticate the request before granting access to the network resources. The reason for the longer verification is because there are many checks that an access request has to pass such as Identity Verification (in which the identity of the device or the person is being authenticated with the help of usernames and passwords, one-time codes, or digital certificates), Device Security Status (in which the device requesting access is checked for any security measures, antivirus status, or system configurations to see if the device is compromised in any way), User and Device Behaviour (in which the behaviour of the users or the devices is checked as to whether there is any deviation from the normal behavior, such as the types of resources that are usually accessed, working periods during which those resources are accessed, and any significant differences in the size of file transfers), Location and the Communication Channel (in which the location where the access request is made is checked, and if the location is from a place which is deemed as a high risk environment, the request will be thoroughly checked more and more or even denied outright, and the type of communication channel that is being used (public or private) at the time of request access is also considered), Compliance with Policies and Regulations (access decisions are also influenced by the compliance of policies and regulations that are put in place by the organization), VPNs (VPNs can also influence the access decisions, sometimes a connection has to be secure to transmit data or to grant the request to the resources in the network), Multi Factor Authentication (organizations sometimes require the request to also pass the multi factor authentication test before any access is granted), Dynamic Monitoring and Analysis (where the zero trust systems employ dynamic monitoring of the security levels of the device from which the request originated) before accessing the network resources. To ease with this longer verification process, a solution of integrating the Zero Trust with AI has been proposed to speed up the verification process.

IV. Enhancing Zero Trust Security with AI

AI can learn from the patterns of access requests and user behaviour, therefore enabling the system to dynamically adjust security measures based on the perceived risk level. Using the machine learning models, AI can process large volumes of data in real time to make instant decisions on access rights. By analyzing the access requests, trends and user behavior AI can then flag unusual behavior and prompt a pre-emptive action. AI enhances the verification process by deciding which type of verification is needed for a particular request, thereby separating low risk scenarios or requests from trusted devices and high-risk scenarios or unusual requests. All of these will lead to faster verification process when integrating Zero Trust with AI. Q-Learning has been proposed as a solution that leads to a faster verification process.

V. Reinforcement Learning and Q-Learning

Reinforcement learning [15] is characterized by having an agent and a set of states and actions. An agent in a state s1, upon performing an action, transitions to state s2. Each transition results in a reward being granted to the agent, either in the form of a positive reward, or a negative penalty based on how close the agent is to the goal state. Q-Learning is a reinforcement learning policy that will find the next best action given a current state. Q-Learning chooses this action and aims to maximize the reward. Q-Learning allows the systems to take optimal actions in various states based on rewards and penalties. Q-learning works by updating the Q-values in the Q-table which represent state-action pairs and values associated with them. The Q-values tell us that on a given state, taking a particular action will lead to maximum reward in the future and that it will be part of the optimal path. The core of the Q-Learning is the Bellman Equation, which is shown below.

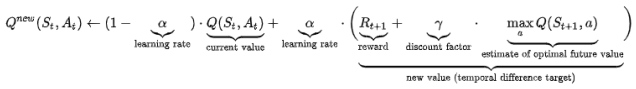

Fig. 1. Bellman Equation

The alpha in the Bellman Equation is the learning rate, which is a crucial parameter. The value of alpha determines how new information influences the learned information. A higher alpha value means that the new information has more influence on the learned information making the agent learn faster, but it also comes with the risk of instability. A lower alpha value means that the new information has less influence on the learned information thereby making the agent more stable but slower, as the changes to the knowledge are more gradual in this case. The Gamma in the Bellman Equation is the discount factor, which is another crucial parameter that takes values between 0 and 1. A value closer to 0 means the agent is short-sighted, meaning the agent values immediate awards more than those in the future. A gamma value close to 1 means that the agent is far-sighted which means that the agent values future awards more significantly than immediate rewards. Integrating human inputs during training phase to specify the safe and unsafe actions guiding the reinforcement learning agent towards safer decision making is also very important while training a model [10].

VI. Application of Q-Learning in Zero Trust Systems

In the context of the Zero Trust, Q-Learning can be applied to dynamically adjust network access policies based on interactions and outcomes. This means that Q-Learning learns the most secure and efficient ways to verify and authenticate devices and users. Q-Learning evaluates and updates policies using a Q-table that maps states (device or user requesting access) to actions (authenticate, deny access) based on a reward system. By learning from the past authentication events, Q-Learning optimizes the verification process which reduces the unnecessary delays and focuses the resources on higher-risk access requests or unusual requests. The AI uses historical data and real-time input to make informed decisions which helps in maintaining a robust security and provides a faster verification process. The AI-enhanced Zero Trust model incorporating Q-learning reduced network access time by 18% compared to the traditional methods [8].

VII. Challenges in implementing Q-Learning in Zero Trust Systems

Although implementing Q-Learning in Zero Trust systems could lead to a faster verification process, there are also some challenges which we need to be aware of as well. One of the prominent challenges is the case of false positives. Implementing Q-Learning instead of traditional verification process can lead to the rise of false positive cases since sometimes a request access could seem unusual but be genuine—oftentimes in the real world, we will come across genuine data that might not agree with the majority of the data that we have trained our model on—and based on the information that the model is trained on, the genuine access request could be considered unusual or high-risk and be subject to more and more strict verification processes due to its unusual behaviour. This can lead to the request being denied access to the resources in the network completely as well. There is also computational overhead one needs to consider while implementing intelligent systems like Q-Learning on top of the existing Zero Trust Systems. Since our learning system learns from the data we feed to it, there should also be a good balance and variety of data that our model should get trained on so that it can make good decisions without bias. Since Q-Learning is not inherently part of Zero Trust systems and is an enhancement proposed to make the verification process of the devices requesting access to the network faster, there needs to be more research done before we implement this in real world scenarios [17]. The transition to Zero Trust is also complex and filled with challenges such as integration issues with existing systems, lack of industry standards, and disruptions during migration [11]. It is also very important for our AI model to be explainable, such that we understand why it makes the decisions that it does, and how it reaches the decisions that it does [12].

VIII. Conclusion

The Zero Trust Security framework transformed the field of cybersecurity, improving upon the issues faced by the previous perimeter defense security model. By implementing artificial intelligence, we can streamline the Zero Trust model further using AI's abilities to handle large volumes of data and machine learning techniques to manage the access request and verification process. This would allow the security system to continuously learn, effectively addressing ever-evolving cyber threats. As Q-Learning in the Zero Trust model is a relatively new topic, there is currently a lack of research in the field. Along with further research into applications of Q-Learning in Zero Trust, we recommend future research on integrating Q-Learning with existing security systems, improving Q-Learning Zero Trust scalability and efficiency for large networks, the development of industry standards for AI enhancements to Zero Trust, and privacy and ethical considerations of AI Q-learning Zero Trust implementation.

References

[1] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access Control Policy Enforcement for Zero-Trust-Networking," *2018 29th Irish Signals and Systems Conf. (ISSC)*, Dec. 2018, doi: 10.1109/ISSC.2018.8585365.

[2] R. Zeng, N. Li, X. Zhou, and Y. Ma, "Building A Zero-trust Security Protection System in The Environment of The Power Internet of Things," *2021 2nd Int. Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, Oct. 2021, doi: 10.1109/AINIT54228.2021.00114.

[3] T. Cheng, C. Chi, Y. Zhang, and Z. Yin, "The Appliance of Decentralized Identifiers in Zero Trust Network," *2023 IEEE Int. Conf. on Blockchain*, Dec. 2023, doi: 10.1109/Blockchain60715.2023.00041.

[4] B. Ali, M. A. Gregory, S. Li, and O. A. Dib, “Zero Trust Security Framework for 5g MEC Applications: Evaluating UE Dynamic Network Behaviour,” *2023 33rd Int. Telecommunication Networks and Applications Conf.*, Nov. 2023, doi: 10.1109/ITNAC59571.2023.10368551.

[5] H. Nana and Y. Yuanyuan, “A Research on Data Secure Access Control Mechanism Based on Zero Trust and Attribute Encryption in Medical Cloud,” *2022 IEEE 8th Int. Conf. on Computer and Communications (ICCC)*, Dec. 2022, doi: 10.1109/ICCC56324.2022.10065956.

[6] L. Bradatsch, O. Miroshkin, and F. Kargl, “ZTSFC: A Service Function Chaining-Enabled Zero Trust Architecture,” *IEEE Access*, vol. 11, pp. 125307-125327, Nov. 2023, doi: 10.1109/ACCESS.2023.3330706.

[7] A. Singh, R. K. Dhanaraj, A. K. Sharma, B. Balusamy, G. Sharma and S. Agrawal, "Q-Learning Based Network Access Policy Management for Zero Trust Security in IIoT," *2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM),* Roorkee, India, 2023, pp. 1-5, doi: 10.1109/ELEXCOM58812.2023.10370294.

[8] A. Wylde, "Zero trust: Never trust, always verify," *2021 Int. Conf. on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland, 2021, pp. 1-4, doi: 10.1109/CyberSA52016.2021.9478244.

[9] S. Veerabathraswamy and N. Bhatt, "Safe Q-Learning Approaches for Human-in-Loop Reinforcement Learning," *2023 Ninth Indian Control Conf. (ICC)*, Visakhapatnam, India, 2023, pp. 16-21, doi: 10.1109/ICC61519.2023.10442899.

[10] P. Phiayura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," *IEEE Access*, vol. 11, pp. 19487-19511, 2023, doi: 10.1109/ACCESS.2023.3248622.

[11] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," *IEEE Access*, vol. 10, pp. 93104-93139, 2022, doi: 10.1109/ACCESS.2022.3204051.

[12] M. Shore, S. Zeadally, and A. Keshariya, “Zero Trust: The What, How, Why, and When,” *Computer*, vol. 54, no. 11, pp. 26–35, Nov. 2021, doi: https://doi.org/10.1109/mc.2021.3090018.

[13] “Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN,” *Computer Networks,* https://ar5iv.labs.arxiv.org/html/2105.01478.

[14] J. Jia and W. Wang, "Review of reinforcement learning research," *2020 35th Youth Academic Annual Conf. of Chinese Association of Automation (YAC*), Zhanjiang, China, 2020, pp. 186-191, doi: 10.1109/YAC51587.2020.9337653.

[15] “8 Areas of Future Research in Zero Trust,” *Carnegie Mellon University Software Engineering Institute*, Apr. 2023, https://insights.sei.cmu.edu/blog/8-areas-of-future-research-in-zero-trust/.

[16] S. Munasinghe, N. Piyarathna, E. Wijerathne, U. Jayasinghe and S. Namal, "Machine Learning Based Zero Trust Architecture for Secure Networking," *2023 IEEE 17th International Conference on Industrial and Information Systems (ICIIS)*, Peradeniya, Sri Lanka, 2023, pp. 1-6, doi: 10.1109/ICIIS58898.2023.10253610.

[17] R. Qiu, J. Zhang, L. Chen, W. Li, and N. Lin, “Internet of Things Terminal Access Security Based on Zero Trust,” *2022 6th Int. Symp. on Computer Science and Intelligent Control (ISCSIC),* Nov. 2022, doi: 10.1109/ISCSIC57216.2022.00013.

[18] Y. C. Wei and T. W. Yu, “Zero Trust Framework in Financial Sector: The Handling of Machine Learning Based Trust Management,” *2023 Int. Conf. on Consumer Electronics - Taiwan (ICCE-Taiwan),* Jul. 2023, doi: 10.1109/ICCE-Taiwan58799.2023.10226959.

[19] P. H. Ho, H. Y. Chen, and T. N. Lin, “Zero Trust Architecture of Token Network,” *2023 IEEE Int. Conf. on Metaverse Computing, Networking and Applications (MetaCom)*, Jun. 2023, doi: 10.1109/MetaCom57706.2023.00120.

[20] K. Singh, B. Kumar, R. Saxena, and V. Lohani, “A Defense in Depth with Zero Trust Architecture for Securing 5G Networks,” *2023 31st Telecommunications Forum (TELFOR),* Nov. 2023, doi: 10.1109/TELFOR59449.2023.10372633.