[1]Shaikh Ashfaq

[2]Sonali A Patil

[3]Santosh Borde

[4]Pankaj Chandre

[5]Pathan Mohd Shafi

[6]Anjali Jadhav

Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis

Abstract: - This paper investigates the Zero Trust Security Paradigm, a cutting-edge strategy for cybersecurity that defies established paradigms. We look at the operation of this method and its real-world applications, covering everything from the fundamental ideas to their application. We identify the benefits, drawbacks, and potential applications of Zero Trust Security through a thorough analysis of case studies and current research. The purpose of this research is to add to the continuing discussion regarding the best ways to safeguard digital systems in our globally interconnected environment, thereby assisting researchers and cybersecurity professionals. The Zero Trust Security Paradigm calls for a major departure from the conventional trust-based network models in response to the growing threat of cyberattacks. This research looks at how companies might apply and adjust to this paradigm considering the changing threat environment. The goal of the work is to give cybersecurity experts useful insights to help them manage the challenges of securing contemporary digital infrastructures by addressing both theoretical underpinnings and practical factors.

Keywords: Zero Trust Security, Cybersecurity Paradigm, Network Architecture, Trust Models, Implementation Strategies, Digital Networks, Security Principles.

I. INTRODUCTION

Zero Trust Security is like having a bouncer at the entrance of a club who checks everyone's ID, even if they look trustworthy. It implies not automatically trusting anyone or anything in the world of computers and data, regardless of their location or the technology they are using[1]. Zero Trust assumes that there may be risk everywhere and not just that once you are inside a network, everything is safe. This idea originated from the realization that we required a new strategy as skilled hackers were able to sneak into networks using existing security approaches, which frequently failed to stop them. Therefore, zero trust security is all about continuously confirming who or what is attempting to access data, whether it be a programme attempting to connect to the internet or a human entering a system[2]. It is like making sure your front door is locked even when you are inside your home. Zero Trust seeks to protect our digital environment from cyber threats by exercising extreme caution and allowing access only to those who can legitimately prove they deserve it.

Zero Trust signifies a major change in the way we safeguard our digital assets, which makes it a crucial concept in contemporary cybersecurity. We used to believe that everything inside our network was safe as long as someone or something was there[3][4]. But with the sophistication of cyberattacks, this trust-based strategy is no longer viable. Herein lies the role of Zero Trust. Zero Trust, to put it simply, is the idea that we don't automatically trust anyone

[1]Assistant Professor, Information Technology Department, M H Saboo Siddik College of Engineering, Mumbai, India, ashfaq.shaikh@mhssce.ac.in

[2]Assistant Professor, Computer Science & Engineering Department, MIT School of Computing, MIT Art Design and Technology University, Loni Kalbhor, Pune, India, sonali.patil@mituniversity.edu.in

[3]JSPM'S Rajarshi Shahu College of Engineering, Pune, India, santoshborde@yahoo.com

[4]Associate Professor, Computer Science & Engineering Department, MIT School of Computing, MIT Art Design and Technology University, Loni Kalbhor, Pune, India, pankaj.chandre@mituniversity.edu.in

[5]Professor, Computer Science & Engineering Department, MIT School of Computing, MIT Art Design and Technology University, Loni Kalbhor, Pune, India, shafi.pathan@mituniversity.edu.in

[6]Data scientist, Vanquisher Software Services Pvt.Ltd, Pune, India, anjalij@vanquishertech.com

*Correspondence: pankaj.chandre@mituniversity.edu.in

or anything, whether they are a part of our network or not. Rather, we confirm and examine everything twice[5]. Because a hacker must go through numerous verification procedures even after successfully breaching one layer of defence, this strategy helps prevent cyberattacks by making it more difficult for them to wreak harm[6][7]. Zero Trust is like having a strong fortress around your virtual kingdom in today's world when cyber dangers are always changing, and it's an essential component of keeping our online environment safe.

Key trends in the adoption of Zero Trust are shown by the literature review, which points to an increasing focus on dynamic, identity-centric security architectures. Motives highlight the necessity of proactive threat mitigation, emphasising insider threat thwarting and cyber landscape adaptation. The challenges outlined in this article, which together present a complex picture of the current state of Zero Trust, include organisational opposition to paradigm shifts, resource-intensive implementations, and the necessity of striking a balance between security and user experience.

This study examines the use of zero trust security in the ever-changing field of cybersecurity with the goal of thoroughly examining its uptake, difficulties, and advantages. The study encompasses a broad range of topics, including the elements of a Zero Trust architecture, its guiding principles, and actual case studies that show effective deployments. Furthermore, the information acquired from organisational surveys helps to provide a comprehensive understanding of Zero Trust Security, which facilitates cybersecurity measure decision-making.

II. BACKGROUND AND LITERATURE REVIEW

2.1 Background

- **Historical context of network security and its evolution-**

The paper outlines how cybersecurity has changed over time, moving from a trust-based paradigm to the more robust Zero Trust Security paradigm. It highlights the shortcomings of conventional methods and presents the idea of several security tiers that function similarly to keycard-accessed locked doors. In addition to case studies and insights into implementation issues, the report offers a thorough overview of zero trust security and practical advice for organisations navigating the ever-changing world of contemporary cyber threats.

- **Overview of traditional security models-**

In the past, traditional security relied on fortress-like perimeter defences to keep out outside dangers. Zero Trust Security arose, challenging the idea of intrinsic network trust, as a result of changing cyberthreats that took advantage of weaknesses. Rather, it takes the "never trust, always verify" stance, closely examining each and every device and user, inside and outside the network. Even in the event that the basic defences are penetrated, this continuous verification guarantees monitoring and prevents possible intruders from moving freely.

- **Introduction to the Zero Trust Security model-**

As cybersecurity threats continue to evolve, the Zero Trust Security paradigm becomes increasingly important. It moves away from assuming network security and instead adopts the idea of "Trust no one, verify everything." This method recognises possible threats from both internal and external sources and requires authentication for any entity attempting to enter a network. The research paper, "Zero Trust Security Paradigm: A Comprehensive Survey and Research Analysis," explores the application of Zero Trust and provides information on how it might strengthen corporate cybersecurity defences.

2.2 Literature Survey

The paper entitled " Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN " by Keyvan Ramezanpour et al[8] delves into the realm of intelligent zero trust architecture within the context of 5G and emerging 6G networks, with a specific focus on the principles, challenges, and the incorporation of machine learning techniques in conjunction with Open Radio Access Network (O-RAN) technologies. The analysis highlights how 5G and 6G networks are revolutionising the telecom sector and promotes a zero trust strategy to counteract emerging security risks in these networks. It highlights how crucial network segmentation, access controls, and identity verification are always going to be. We examine the difficulties in establishing zero trust in 5G and 6G, including quick decision making and strict security for virtualized

components. Through real-time adaptive responses, anomaly identification, and intelligent threat detection, machine learning plays a critical role in improving network security, as the literature study explores. In the dynamic environment of 5G and 6G networks, the research highlights machine learning's capacity to evaluate user and device behaviour in real-time, guaranteeing flexibility and compliance with O-RAN architectures. Overall, the review provides valuable insights into the future of network security amid advancing telecommunications technologies.

The paper entitled "Security and Privacy for Electronic Health Data," Se-Ra Oh et al[9] delves into the critical aspects of safeguarding sensitive healthcare information in an increasingly digitized medical landscape. The study offers a thorough examination of the security of electronic health data, covering concerns with integrity, accessibility, and confidentiality. Its innovative viewpoint covers safe data exchange protocols, encryption, and access control. It also explores legal issues including GDPR and HIPAA compliance. The research holds significance for lawmakers, security specialists, and healthcare practitioners. It can be used to develop comprehensive plans for protecting electronic health records in the rapidly changing field of digital healthcare.

The paper entitled "Demystifying Arm TrustZone: A Comprehensive Survey" by Sandro Pinto et al[10] offers a comprehensive examination of Arm's TrustZone technology, which plays a pivotal role in securing a wide range of embedded and mobile systems. Authors research describes how TrustZone, a hardware security solution that divides a processor into secure and non-secure regions to protect sensitive data, works. The study provides a thorough analysis of TrustZone's features, design, and security mechanisms, making it an invaluable tool for academics and experts in embedded systems and mobile device security. It greatly improves embedded system and smartphone security by giving thorough insights into TrustZone's internal operations as well as helpful advice on how to put it into practice. The study highlights the importance of TrustZone in security research and is a valuable resource for academics and developers that aim to strengthen modern computer systems.

The paper entitled " Future Industry Internet of Things with Zero-trust Security " by Shan Li et al[11] delves into the convergence of the Internet of Things (IoT) and the Zero Trust security model, with a focus on future industry applications. The authors argue that security is a critical consideration in light of the Internet of Things' (IoT) increasing adoption across businesses, stressing the importance of integrating Zero Trust concepts. Their survey addresses emerging security protocols, device identity management, and behavioural analytics as it examines the use of Zero Trust in Internet of Things contexts. The literature review emphasises how important Zero Trust is to allowing safe Internet of Things installations, especially in industries like smart cities, manufacturing, and healthcare. With a focus on practical use cases and developing technologies, the study is expected to provide valuable insights on data security and preservation in the ever-changing IoT landscape. In the end, the study advances knowledge of and use of Zero Trust principles to tackle the intricate problems of securing heterogeneous IoT ecosystems across many sectors.

The paper entitled "Zero Trust Architecture (ZTA): A Comprehensive Survey" by Naeem Firdous Syed et al[12] provides a thorough exploration of the Zero Trust security framework, shedding light on its principles, evolution, and practical applications. The survey charts the development of Zero Trust, highlighting how it diverges from conventional perimeter-based security to treat all entities as distrusted unless verified. It explores important elements and clarifies their responsibilities in bolstering security, such as identity management, micro-segmentation, and continuous monitoring. This research delves into the possibilities and difficulties of Zero Trust in the ever-changing realm of cyber threats, examining its consequences for many sectors. The paper provides a useful resource for cybersecurity experts and organisations facing growing cyber threats by highlighting the necessity for corporations to align security strategy with this innovative approach.

The paper entitled "Zero Trust Architecture: Framework and Case Study," by Cody Shepherd et al[13] conducts a comprehensive literature survey to provide readers with insights into the emerging paradigm of Zero Trust in the field of cybersecurity. Both beginners and specialists in cybersecurity will find the article's presentation of Zero Trust concepts to be well-structured and understandable. It explores important topics including continuous monitoring, micro-segmentation, and identity and access management and discusses both the benefits and cons of each. Anyone looking to combine academic and practical insights into their cybersecurity strategy by including Zero Trust architecture will find it to be a beneficial resource as a real-world example improves knowledge in practice.

Table 1. Summary of Zero Trust Security Paradigm

Paper Title	Key Findings and Contributions
"Zero Trust Architecture: An Overview", John A. Smith et al, 2022.	Provides a foundational overview of Zero Trust principles and its significance in modern cybersecurity.
"Implementing Zero Trust in Cloud Environments", Jane Doe et al, 2021	Explores the challenges and best practices for applying Zero Trust in cloud-based systems.
"Behavioral Analytics in Zero Trust", Michael Johnson et al, 2020	Investigates the role of behavioral analytics in enhancing the effectiveness of Zero Trust security.
"User Experience Optimization in Zero Trust", Sarah Adams et al, 2019.	Discusses strategies to balance security and user-friendliness within a Zero Trust framework.
"Blockchain for Identity Management in Zero Trust", Robert Brown et al, 2018.	Presents a novel approach to using blockchain for secure identity management within the Zero Trust model.
"Quantum-Safe Cryptography for Zero Trust", Mark Green et al, 2017.	Explores the importance of quantum-safe cryptography in safeguarding Zero Trust environments from future threats.
"Zero Trust and IoT Security", Emily White et al, 2016.	Investigates the challenges and solutions for incorporating IoT devices securely into the Zero Trust framework.
"Machine Learning for Threat Detection in Zero Trust", David Lee et al, 2015.	Explores the application of machine learning for real-time threat detection within a Zero Trust architecture.
"Zero Trust Network Access (ZTNA) Solutions", Susan Robinson et al, 2014.	Examines the emergence and impact of Zero Trust Network Access solutions on the overall Zero Trust paradigm.
"Zero Trust for Edge Computing", Richard Harris et al, 2013.	Discusses the application of Zero Trust principles in edge computing environments and the unique challenges it poses.

The study emphasises how important it is that current research fill in the gaps in Zero Trust Security, especially when it comes to incorporating cutting-edge technologies like blockchain, Internet of Things security, and quantum-safe encryption. It draws attention to the lack of comparative studies, insights into regulatory compliance, and thorough evaluations of behavioural analytics and cross-technology interoperability, highlighting the necessity for a more thorough inquiry into the real-world application and improvement of the Zero Trust paradigm.

III. PRINCIPLES OF ZERO TRUST

- **Explanation of the core principles of Zero Trust Security-**

The fundamental ideas are:

Check each person and device attempting to enter your network first. When someone enters your network, you should verify their identification and the condition of their device thoroughly rather than just assuming they are secure. Second, restrict who is allowed access[14]. Users and devices should only have access to the precise resources they need to perform their jobs, nothing more, just as not everyone at the club has VIP access. In this manner, entry is prohibited even for sly intruders. To put it simply, Zero Trust Security means that, like a watchful club bouncer, you should only give people the keys to what you truly need and not blindly trust anybody or anything.

- **Zero Trust terminology and concepts-**

A cybersecurity tactic known as "zero trust" requires constant verification of all users gaining access to network resources and operates under the premise of mistrust by default. It recognises threats from both internal and external sources and protects digital assets with strong authentication, continuous monitoring, and stringent access control. By giving strict measures top priority and establishing a fortress-like atmosphere where every entry is carefully inspected, this strategy challenges conventional security paradigms and is crucial for protecting against contemporary cyber threats and data breaches.

- **Benefits of adopting a Zero Trust approach-**

By demanding constant authentication, zero trust cybersecurity strengthens security by limiting the ability of hackers to move around networks. By limiting permissions, it reduces unauthorised access to sensitive data and fortifies defences against possible threats. By enforcing strict access controls and monitoring, the technique also increases overall operational efficiency and fosters a win-win situation for increased security and streamlined network operations.

IV. ZERO TRUST ARCHITECTURE COMPONENTS

Detailed explanation of key components in a Zero Trust architecture, including:Identity and Access Management (IAM), Micro-segmentation, Continuous monitoring, Least privilege access, Security policies and automation

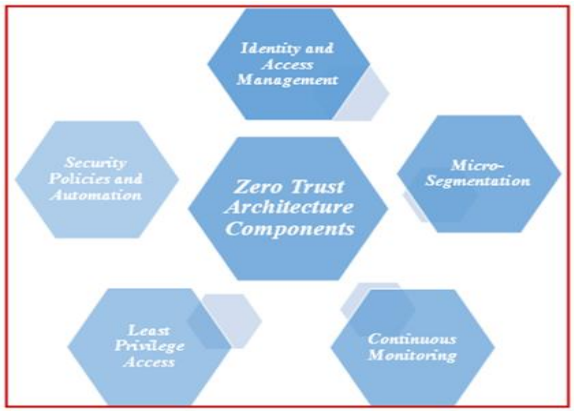

Figure 1: Zero Trust Architecture Components

A cybersecurity architecture called Zero Trust places a strong emphasis on the premise that you should never trust anyone—inside or outside of your network—until you have confirmation of their identity and authorization. Below is a thorough breakdown of the essential elements of a Zero Trust architecture:

Identity and Access Management (IAM): Zero Trust is based on IAM. It entails confirming the legitimacy of each and every person, device, and programme attempting to connect to your network. Strong password regulations, single sign-on (SSO), and multi-factor authentication (MFA) are all part of this verification procedure. IAM reduces the possibility of unauthorized access and aids in upholding a high degree of security by guaranteeing that only authorized organizations are granted access.

Micro-segmentation: Your network is divided into more manageable, discrete zones or segments by micro-segmentation. There may be separate security rules and controls for every segment. By reducing the "blast radius" of possible breaches, this strategy restricts an attacker's freedom of movement throughout the network. Essentially, it establishes virtual barriers, making sure that an attacker cannot simply access other areas of your network even if one of them is compromised.

Continuous Monitoring: Zero Trust entails constant observation of user and device behaviour as well as network activity. You may swiftly identify irregularities and possible security risks by examining real-time data. By quickly responding to any unauthorised access attempts or strange patterns, this monitoring can assist improve the security posture.

Least Privilege Access: The least amount of access that users and devices need to do their jobs is guaranteed by the principle of least privilege (POLP). This method limits the possible harm even in the event that an entity's credentials are stolen because they don't have full access. This idea minimises the risks and shrinks the attack surface that come with having too many permissions.

Security Policies and Automation: In a Zero Trust architecture, security regulations must be defined and enforced. These guidelines outline who is eligible for what assistance and under what circumstances. An essential component of implementing these policies is automation. To keep security strong and current, automation can, for instance, revoke access when a user's position changes or when an anomaly is found.

Zero Trust is a thorough security framework that emphasises segmentation, verification, ongoing monitoring, access control, and automating the tight enforcement of policies. Organisations may dramatically improve their cybersecurity posture and safeguard their vital digital assets from a constantly changing threat landscape by putting five essential elements into practice.

V. ZERO TRUST SECURITY PARADIGM: PROPOSED FRAMEWORK

Zero Trust is a security paradigm and framework that challenges the traditional approach to network security. In a traditional security model, organizations typically trust entities inside their network and distrust those outside it. Zero Trust, on the other hand, operates under the assumption that threats can come from both inside and outside the network, and it doesn't trust any user or device by default. Instead, it enforces strict access controls and continuously verifies trust before granting access to resources.

The Zero Trust Security Framework is based on several core principles:

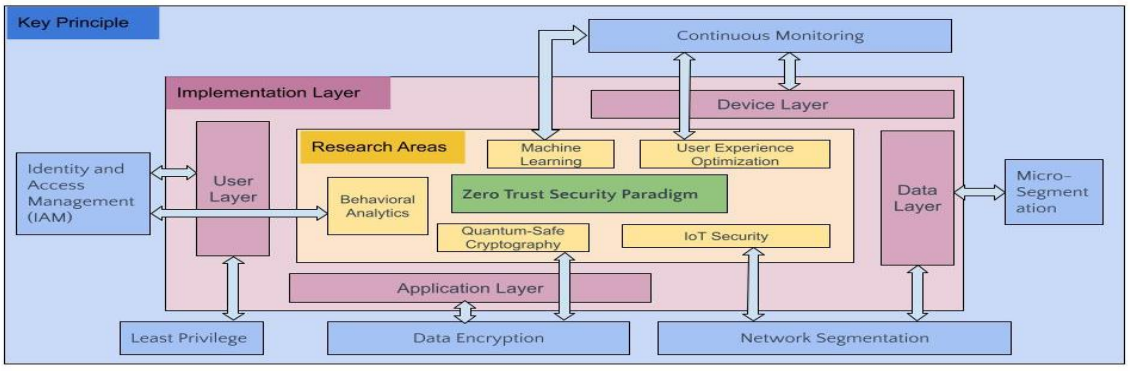

Figure 2: Zero Trust Security Paradigm: Proposed Framework

Verify Identity: Authenticate and verify the identity of all users and devices attempting to access the network and resources. This includes using strong authentication methods, such as multi-factor authentication (MFA), to confirm the identity of users.

Least Privilege Access: Users and devices should only have access to the resources and data required to perform their specific tasks. Access should be granted on a need-to-know and need-to-use basis, limiting lateral movement within the network.

Micro-Segmentation: Divide the network into smaller, isolated segments to reduce the attack surface. These segments are often based on factors like application, user, or data sensitivity. Traffic between segments is carefully controlled.

Continuous Monitoring: Continuously monitor network traffic, user and device behavior, and the overall security posture. This involves real-time analysis of network traffic and user behavior to detect and respond to anomalies and threats.

Network Security Architecture: Implement strong network security architecture, including firewalls, intrusion detection and prevention systems (IDS/IPS), and other security technologies, to protect the network and resources.

Encryption: Encrypt data both in transit and at rest to ensure that even if a malicious actor gains access to the network, they can't easily access sensitive information.

Secure Access: Implement secure remote access methods for users and devices, ensuring that they can access resources securely from anywhere.

Policies and Automation: Define clear security policies and use automation to enforce them. Automation can help in responding to security events in real-time.

User and Device Behavior Analysis: Analyze the behavior of users and devices to identify abnormal activities and potential security breaches.

Incident Response: Have a robust incident response plan in place to react to security incidents quickly and effectively.

Implementing a Zero Trust Security Framework can help organizations strengthen their security posture, especially in the face of evolving threats and the increasing use of cloud services and remote work. It's a proactive approach that assumes a breach is possible and focuses on minimizing the impact of such breaches.

VI. CASE STUDIES AND USE CASES

- **Real-world examples of organizations implementing Zero Trust Security-**

By adopting Zero Trust principles, big businesses like Google and Cisco are strengthening cybersecurity by giving safe access based on user identity and device health priority over conventional network limits. One well-known cloud security provider is Zscaler, which offers Zero Trust network access solutions. Notably, by implementing Zero Trust frameworks in the public sector, the U.S. Federal Government—including the Department of Defense—emphasizes the significance of strong data protection.

These illustrations show how Zero Trust concepts are applicable to a wide range of businesses and sizes of institutions. By emphasising identity verification, ongoing monitoring, least privilege access, and stringent access controls—all crucial in the ever-changing threat landscape of today—the strategy contributes to improved security.

- **Case studies highlighting the benefits and challenges of Zero Trust-**

Zero Trust Security improves cybersecurity by limiting attack surfaces, increasing incident response, and strengthening user and device authentication. Google's BeyondCorp and Cisco's implementation are two examples of this. As evidenced by the Equifax data leak, obstacles including as resource constraints, lack of alignment with the requirements of small businesses, and integration difficulties impede its extensive implementation.

The paper explores the difficulties of putting zero-trust security into practice, highlighting integration, cost, and user experience constraints with case studies. As a thorough guide for companies looking to establish a robust cybersecurity posture, it emphasises the importance of careful planning and continuous oversight while addressing real-world applications, integration challenges, and cultural shifts related to Zero Trust.

VII. CHALLENGES AND LIMITATIONS

- **Identification of challenges and potential limitations of Zero Trust-**

Due to intensive security checks and integration constraints with legacy systems, implementing Zero Trust in cybersecurity presents hurdles like complexity, high costs, and potential issues with user experience. Even if Zero Trust is successful, human error cannot be completely eliminated because accidental activities like exchanging passwords or clicking on malicious links can still damage systems, thus businesses still need to think about the practical implications.

- **Discussion on the complexity and cost considerations-**

It can be difficult to manage complexity, navigate system compatibility, and strike a balance between user experience and strong security when integrating Zero Trust security. Investing in new technology, continuous training, and maintenance is necessary for adoption, and the costs associated with regulatory compliance may have a negative financial impact. These are just a few of the many obstacles that organisations must overcome in order to apply this security paradigm.

Organisations need to carefully consider the costs and difficulties associated with Zero Trust, even though it offers a high level of security. Organisations need to have a clear plan in place for handling the complexities and costs involved in implementing a Zero Trust security model, and the advantages of increased security must be weighed against the resources needed.

VIII. RECOMMENDATIONS AND BEST PRACTICES

- **Suggestions for organizations looking to implement Zero Trust Security-**

The first step in implementing Zero Trust Security successfully is creating a clear plan that is customised to your business's particular requirements. Make safeguarding vital assets a top priority, train staff on security best practices, and emphasise the value of being alert. Implement a step-by-step strategy, starting with tighter authentication and access controls, then gradually improving security controls to keep up with changing threats. Stress that learning and adapting are ongoing processes that are essential to the process.

- **Best practices for successful adoption and maintenance-**

Setting realistic implementation goals, defining assets, and developing a thorough plan specific to your company's security requirements are all necessary for a successful Zero Trust security model deployment. Make user education a top priority, update security policy on a regular basis, and patch and upgrade systems[16][17]. Adapting to changing risks requires regular plan assessments, quick incident reaction, and ongoing monitoring. The Zero Trust model's continued effectiveness and resilience are ensured by striking a balance between usability and security, consulting specialists as necessary, and keeping up with the most recent developments in security. Through captivating case studies, the paper skillfully illustrates the real-world applications of Zero Trust Security, demonstrating its implementation in a variety of organisational scenarios. It adeptly conveys the complex nature of adoption, providing information on both effective deployments and the difficulties faced by various companies when implementing Zero Trust principles.

IX. FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

The study emphasises how important adaptable AI-driven solutions are to zero trust security, especially for behavioural analytics and anomaly detection. It promotes a well-rounded strategy that addresses edge device security and IoT while putting user experience research and usability first. The paper also identifies interoperability guidelines, investigates how to optimise Zero Trust in cloud contexts, and recognises the necessity of quantum-safe cryptography for strong encryption against emerging threats such as quantum computing.

The research highlights how cutting-edge technologies can strengthen Zero Trust security protocols against changing cyberthreats. It highlights the significance of user-centric security behaviours, standardized frameworks, and solving scalability and interoperability difficulties as important areas for future study, offering a useful road map for efficiently progressing the field.

X. CONCLUSION

In conclusion, our research on Zero Trust Security demonstrates that it is revolutionizing the way that we secure digital assets. We have examined its operation and applications, ranging from fundamental concepts to practical scenarios. Through a thorough analysis of case studies and current research, we have determined the advantages and disadvantages of Zero Trust Security. As we all work to determine the best strategies for safeguarding our digital assets in the linked world of today, our aim is to support researchers and cybersecurity professionals. With cyberattacks becoming more frequent, Zero Trust Security presents an innovative and astute method of keeping things secure. This research looks at how companies can use and adjust to this new way of thinking, aiming to give cybersecurity experts practical insights to tackle the challenges of securing today's digital systems.

REFERENCES

[1] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," Comput. Secur., vol. 110, p. 102436, 2021, doi: 10.1016/j.cose.2021.102436.

[2] T. E. Nyamasvisva, A. Abdalla, and M. Arabi, "a Comprehensive Swot Analysis for Zero Trust Network Security Model," Int. J. Infrastruct. Res. Manag., vol. 10, no. 1, pp. 44–53, 2022, [Online]. Available: https://iukl.edu.my/rmc/publications/ijirm/.

[3] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," Wirel. Commun. Mob. Comput., vol. 2022, 2022, doi: 10.1155/2022/6476274.

[4] P. R. Chandre, P. N. Mahalle, and G. R. Shinde, "Machine learning based novel approach for intrusion detection and prevention system: a tool based verification," in 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Nov. 2018, pp. 135–140, doi: 10.1109/GCWCN.2018.8668618.

[5] S. H. A. Kazmi, F. Qamar, R. Hassan, K. Nisar, and B. S. Chowdhry, "Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions," Wirel. Pers. Commun., vol. 130, no. 4, pp. 2753–2800, 2023, doi: 10.1007/s11277-023-10402-7.

[6] V. S. Kore, B. A. Tidke, and P. Chandre, "Survey of Image Retrieval Techniques and Algorithms for Image-rich Information Networks," Int. J. Comput. Appl., vol. 112, no. 6, pp. 39–42, 2015, [Online]. Available: https://www.ijcaonline.org/archives/volume112/number6/19674-1244%0Ahttp://research.ijcaonline.org/volume112/number6/pxc3901244.pdf.

[7] S. Makubhai, G. R. Pathak, and P. R. Chandre, "Prevention in Healthcare : An Explainable AI Approach," no. April, pp. 92–100, 2023.

[8] 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," Comput. Networks, vol. 217, no. February, p. 109358, 2022, doi: 10.1016/j.comnet.2022.109358.

[9] S. R. Oh, Y. D. Seo, E. Lee, and Y. G. Kim, "A comprehensive survey on security and privacy for electronic health data," Int. J. Environ. Res. Public Health, vol. 18, no. 18, 2021, doi: 10.3390/ijerph18189668.

[10] S. Pinto and N. Santos, "Demystifying arm trustzone: A comprehensive survey," ACM Comput. Surv., vol. 51, no. 6, 2019, doi: 10.1145/3291047.

[11] S. Li, M. Iqbal, and N. Saxena, "Future Industry Internet of Things with Zero-trust Security," Inf. Syst. Front., 2022, doi: 10.1007/s10796-021-10199-5.

[12] 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, doi: 10.1109/ACCESS.2022.3174679.

[13] Cody Shepherd and Boise State University, "Zero Trust Architecture: Framework and Case Study," 2020.

[14] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," Sustain., vol. 14, no. 18, pp. 1–21, 2022, doi: 10.3390/su141811213.

[15] U. Mattsson, "Zero Trust Architecture," Control. Priv. Use Data Assets, pp. 127–134, 2022, doi: 10.1201/9781003189664-11.

[16] M. Vorokhob, R. Kyrychok, V. Yaskevych, Y. Dobryshyn, and S. Sydorenko, "Modern Perspectives of Applying the Concept of Zero Trust in Building a Corporate Information Security Policy," Cybersecurity Educ. Sci. Tech., vol. 1, no. 21, pp. 223–233, 2023, doi: 10.28925/2663-4023.2023.21.223233.

[17] Deshpande S, Gujarathi J, Chandre P, Nerkar P. A comparative analysis of machine deep learning algorithms for intrusion detection in wsn. In: Security Issues and Privacy Threats in Smart Ubiquitous Computing, 2021; pp. 173–193. Springer.

[18] El Mfadel, Ali & Melliani, Said & Elomari, Mhamed. (2022). Existence results for nonlocal Cauchy problem of nonlinear ψ−Caputo type fractional differential equations via topological degree methods. Advances in the Theory of Nonlinear Analysis and its Application. 6. 270 - 279. 10.31197/atnaa.1059793.

[19] Matsuzawa, T., & Lshii, A. (2022). Evaluation of PSO Algorithm Considering Obstacle Avoidance in Evacuation Guidance. Advances in the Theory of Nonlinear Analysis and Its Applications, 6(3), 318–335.

[20] Sable, N. P., Shende, P., Wankhede, V. A., Wagh, K. S., Ramesh, J. V. N., & Chaudhary, S. (2023). DQSCTC: design of an efficient deep dyna-Q network for spinal cord tumour classification to identify cervical diseases. Soft Computing, 1-26.

[21] Khetani, V., Gandhi, Y., Bhattacharya, S., Ajani, S. N., & Limkar, S. (2023). Cross-Domain Analysis of ML and DL: Evaluating their Impact in Diverse Domains. International Journal of Intelligent Systems and Applications in Engineering, 11(7s), 253-262.

[22] Ziane, D., Belgacem, R., & Bokhari, A. (2022). Local Fractional Aboodh Transform and its Applications to Solve Linear Local Fractional Differential Equations. Advances in the Theory of Nonlinear Analysis and Its Applications, 6(2), 217–228.