Chapter-IV

ZERO TRUST ARCHITECTURE FOR ENHANCED CYBERSECURITY

Dr. Priya Kapoor, Senior Researcher in Cyber Law and Defense, Symbiosis International University, Pune.

Dr. Rohan Malhotra, Senior Researcher in Cyber Law and Defense, Symbiosis International University, Pune.

Abstract--- Information security is threatened by traditional-based security concepts, which are thought to be inadequate and unable to control the dynamics of information system trust. In an effort to bridge the trust gap in information security, a novel framework known as Zero Trust Architecture (ZTA) combines identity-based policies with ongoing authentication and verification. In an effort to bridge the trust gap in an information system, this architecture is based on a number of trust nodes and logical elements. This framework's acceptance is still in its infancy due to a number of incorrect presumptions and conclusions. We make an effort to investigate the framework's complexities and fill up the current knowledge gap. Although we don't criticize other approaches, this article examined the benefits and features of the zero-trust security architecture in an effort to give a general overview of the model and fill the knowledge gap on the efficacy of implementing a zero-trust philosophy. Therefore, in order to establish a zero-trust architecture, organizations need to continuously check and verify that a user and their device have the correct rights and characteristics. It requires the development of a policy that considers user and device risk in addition to compliance or other requirements to be considered before permitting the transaction. In addition to being aware of all their services and privileged accounts, the organization must be able to control what and where they connect. One-time validation is insufficient since user traits and threats can change at any time.

Keywords--- Cybersecurity, Threats, Zero Trust Architecture.

1. INTRODUCTION

Globally, cybersecurity threats continue to be a significant issue and are only growing. Malicious attacks and incursions on servers and other hardware components have resulted in data theft for corporations worldwide, putting people at danger. It stands to reason that this matrix would not contain the government (Rebouças Filho, 2025). The most frequent target is still, surprisingly, the government; in 2021, there were approximately 1862 breaches, a 68% rise from 2020. When major security breaches were made public in January 2022, mostly impacting the governments of Canada, Australia, and Belarus, similar situations occurred for the US Department of Homeland Security in 2021 (Hubbard et al., 2021). Because users' perceptions of the security and privacy of their data are so negative, this entropy keeps spreading mistrust. People's perceptions of information technology are hence constrained. While there are many more types of these threats, some of the more current trends and attacks include ransomware, data breaches, identity fraud, phishing, cloud vulnerability, insider threats, and the internet of things (Zanasi et al., 2024). Both individuals and businesses are impacted by these actions; for instance, ransomware attacks have been connected to decreased productivity, slow response times, and disruptions in information systems. This has had a major impact, reducing the capacity of institutions such as hospitals and other essential infrastructure. In another scenario, the victims of the attack are threatened with losing their data or being forced to pay, which often damages the organization's reputation (Roy et al., 2024). Porous network surfaces and insiders are two types of weak surfaces that hackers try to exploit by getting past an organization's weakest point. Numerous studies have shown that insiders are the information security attack surface that is most vulnerable (Stafford, 2020; Sharma, 2022).

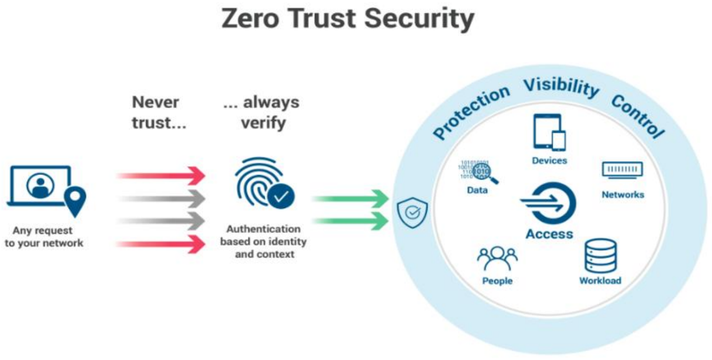

Figure 1: Zero Trust Architecture for Enhanced Cybersecurity

As technology develops and virtual working becomes more prevalent, organizations must take proactive measures to safeguard their resources and assets because a perimeter-based security framework is not enough to meet the demands of the dynamism in information security, especially with regard to cloud computing where data may be accessed remotely (Ogendi, 2024). Therefore, a preventive framework and an effective countermeasure are required to meet these goals. A more comprehensive strategy that prioritizes user identification, validation, verification, and sporadic security checks is needed for information security assurance. Hackers still exploit an organization's weakness despite the fact that there are several security architectures that try to mitigate the effects of an attack. As a result, a comprehensive framework is required in this regard, and the Zero-Trust Architecture (ZTA) has recently drawn increasing interest. This will therefore eliminate any uncertainty regarding the implementation of ZTA and provide a conceptual understanding of it (Khan et al., 2023).

2. LITERATURE REVIEW

There is a dearth of thorough study on ZTA's long-term operational impact, despite the fact that several studies emphasize its immediate security benefits. Few research has examined how ZTA increases operational efficiency over time, notwithstanding Marc's (2023) demonstration of a decrease in security breaches. More thorough research is needed in this area, but Shah et al. (2022) showed a 25% gain in efficiency as a result of automation and decreased manual oversight. This study fills that vacuum by looking at the long-term operational gains made possible by ZTA in actual case studies (Chokkanathan et al., 2024).

ZTA adoption is nevertheless hampered by legacy system integration, especially in sectors that depend on antiquated infrastructure. Many businesses have technological challenges when attempting to adopt micro-segmentation and continuous verification on older systems, according to Arachchige et al. (2020). There aren't many real-world instances of how these difficulties are resolved, though. This report makes a contribution by offering thorough case studies on the time and money needed to manage ZTA integration with legacy systems in healthcare and financial institutions (Kim et al., 2024). ZTA's capabilities are being improved by emerging technologies like artificial intelligence (AI) and machine learning (ML), especially in automating threat identification and response. Although there is little research on AI's measurable effects (Tiwari et al., 2022), Marc (2023) talked about how it aids in real-time anomaly detection. This study builds on this by illustrating how AI-driven solutions in the financial services sector cut down on manual monitoring efforts by 45%, indicating the possibility of additional ZTA optimization through the integration of AI and ML (Manda et al., 2022).

In order to overcome the drawbacks of conventional perimeter-based approaches, Zero Trust Architecture (ZTA) has become a crucial cybersecurity architecture. Its fundamental ideas—continuous authentication, micro-segmentation, and least-privileged access—have been successful in reducing security risks in a variety of sectors. Although Ghasemshirazi et al., (2023) highlighted ZTA's broad applicability, there aren't many industry-specific insights, especially in fields like healthcare and financial services. According to a literature review, there aren't many (Bashir et al., 2024; Abbas & Gul, 2025) models that adhere to the Zero Trust principle and meet all of the aforementioned IoT requirements. The relevant work's specifics are covered in the corresponding chapters. By creating a blockchain-based access control system and hardware-based device identities for authentication, the thesis aims to address the difficult security requirements of IoT networks. In the network, measures are taken to isolate and lessen Byzantine attacks. When combined, these two methods aid in achieving each of the aforementioned goals. By taking these steps, the organization improved security in a number of ways, including:

1) Enhanced visibility into network traffic, improving threat detection and response.
2) Strengthened security posture, reducing the risk of data breaches and unauthorized access.
3) Improved access control policies and encryption, safeguarding sensitive data at rest and in transit.

The agency's security resilience has been greatly improved by adhering to the White House's Zero Trust policies, which have decreased vulnerabilities in its networks, apps, and data. effectiveness in hybrid and cloud contexts.

3. IMPORTANCE OF NETWORK SECURITY

For many different applications, system and network technology is essential. Applications and networks depend on security. Despite the fact that network security is an essential necessity for developing networks, there aren't many readily implementable security techniques. Network developers and security technology developers are separated by a "communication gap." The Open Systems Interface (OSI) concept serves as the foundation for the well-established process of network design (Patel et al., 2024). When developing networks, the OSI model offers a number of benefits. It provides standardization of protocols, ease of usage, flexibility, and adaptability. It is simple to combine the protocols of several levels to create stacks that enable modular development. Individual layer implementation can be altered at a later time without requiring further changes, providing development flexibility. Secure network design is a less evolved method than network design. The intricacy of security requirements cannot be managed using any methodology. The benefits of network design are greater than those of secure network design (Hung-Jen, 2013). The fact that the entire network is secure must be underlined while discussing network security. The security of the computers at each end of the communication chain is not the only aspect of network security. The communication channel shouldn't be open to intrusions when data is being transmitted. The communication channel might be targeted by a potential hacker, who would then take the data, decode it, and reintroduce a fake message. Encrypting the communication and protecting the network are equally crucial as protecting the computers (Alagappan et al., 2022).

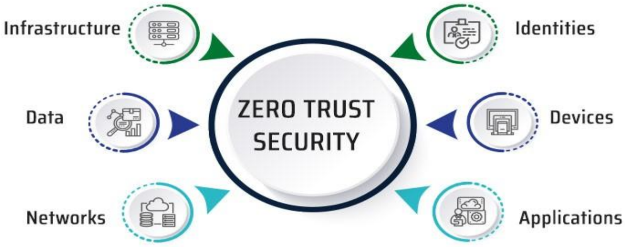

Figure 2: Flow of the Work

4. BACKGROUND AND MOTIVATION FOR ZERO TRUST

IoT connects many devices and networks, which present risks on multiple fronts, whereas traditional M2M applications are usually targeted. It is difficult to safely move several data streams between chosen networks when there is a mix of diverse devices, networks, platforms, and users. Trust boundaries must therefore cover protocol security and all possible communication routes for the devices involved. In an intricately linked Internet of Things, a strong foundation of trust in security begins at the device level and extends across platforms, networks, and the cloud. To guarantee end-to-end security and integrity, each agent in the IoT system must uphold a certain degree of trust. To identify IoT-specific intrusions and assaults, a thorough investigation by IoT security analytics will be necessary. An adversary can compromise nodes when they are deployed in unsupervised, potentially hostile environments without physical protection. Low power IoT nodes cannot employ traditional security measures because they were not created for the Internet of Things and need a lot of resources. Since users (or devices) are no longer limited to a network's perimeter, the traditional method of categorizing them as internal and external to thwart an attack is no longer applicable. A device must be trusted based on its identification and past conduct rather than the network to which it belongs, as we have learned from the IoT assaults previously discussed. If appropriate steps are not taken to stop it, even legitimate nodes in the network could be the source of a significant attack. Therefore, a Zero Trust (Sharma, 2022) approach should be used by the new security mechanism.

In the past, the majority of networks adhered to the security concept "verify, then trust." This suggests that the person or device is trusted and granted network access once its credentials have been validated. The device is blindly trusted, particularly if it has been confirmed to be a part of the internal network. But according to the Zero Trust mechanism put forth by the analyst at Forrester Research, a network should not presume that any user requesting access to a resource, whether inside or outside its boundaries, is trustworthy; rather, it should confirm whether or not the access is necessary. The Zero Trust framework's three fundamental tenets are:

1) Never trust, always verify;
2) Principle of Least Privileges; and

3) Assume there is an impending breach.

Every time a device wishes to connect to the network, it should be authenticated and granted only the minimal amount of access necessary to carry out its intended role. This is crucial given the evolving security landscape of today, particularly with regard to IoT networks. Imagine a situation where a conference room's smart TV serves as the display screen. It can end up being a bot that launches a DDoS attack or a spying gadget that compromises data or privacy. There is a great deal of risk because it is linked to the same network as the company that houses sensitive information like finances and human resources. Therefore, greater duty to prevent data misuse accompanies increased capabilities (Ghasemshirazi et al., 2023). Every effort is being made to minimize human involvement in order to improve the Quality-of-Experience (QoE) in a seamless manner. An exploit's risk surface grows as a result. When an attack targets medical, emergency, or mission-critical communication systems—where communication must be dependable—the casualties are devastating. The loss could be financial, private, or life-threatening. Therefore, fine-grained access control must be put in place and each device requesting access to a resource must first be authenticated. The emphasis is now on selectively protecting the data or resources based on the potential harm they could create, rather than protecting the network's perimeter.

5. CHALLENGES IN TRUST

It is likely that researchers are aware of the many beneficial services that cloud computing has provided. It also takes into account a lot of security risks and challenges. Since a lot of data is sent over networks and kept in cloud resources, malicious components can cause a number of vulnerabilities. In this study, we analyze the security status of cloud scenarios that are divided into seven types based on a Singh et al. (2016) study (Ahmadi et al., 2024). It should be noted that each of this area's subsections corresponds to a distinct security attribute. As seen in Fig. 2, cloud protection challenges can be divided into seven categories: trust and conviction, security policies, client management issues, operating system base issues, application security, data storage security, and network security. Starting with the trust and conviction issue, which aids in making a reliable decision, the classification covers all seven security difficulties. This section also focuses on issues at the application level. These security rules ought to safeguard the workplace. We outline several actual cluster flaws and a simulated cluster assault on the network cloud to demonstrate how clustering issues and all operating systems commonly affect the cloud. There are still a number of flaws in the desktop operating system that make network servers and cellphones susceptible to serious attacks.

5.1. Security

Cloud data security is becoming increasingly important as we move our gadgets, data centers, corporate activities, and more to the cloud. The quality of cloud data security is ensured by comprehensive security policies, cloud security solutions, and enterprise security culture. Cloud security, also known as cloud computing security, is the result of combining a number of policies, processes, controls, and technologies to protect cloud-based systems, data, and infrastructure. These security measures are in place to protect cloud data, help with regulatory compliance, protect client privacy, and set up authentication rules for certain individuals and devices. Every facet of cloud security, including traffic filtering and access authentication, can be tailored to the specific requirements of the company. The development of a workable cloud application security engineering that provides control and remediation is further examined by the ElasticaQ2 2015 and CSA. Furthermore, according to the International Organization for Standardization (ISO), data security issues that can be resolved with cloud computing are essential security requirements for an effective and safe cutting-edge technical solution.

Trust and Conviction

Regarding trust, we calculated it as the belief that leverages the company's experience and sticks to the trustworthy selection of cloud partners, virtualization, web-based access, storage hardware, and the computational algorithm that has been proven to be trustworthy. Assessing trust is a complex, multi-phase process that depends on the multidimensional factor that Chen, D. et al. (2012) identified (Tiwari et al., 2022). Actually, the TCP protocol has security, which means that the service provider is protecting the confidentiality and integrity of the data.

Security Policies Security

Policies include the rules necessary to prevent attacks by adopting preventative measures. According to a 2019 study by Asma Shaikh et al., these guidelines should guarantee the cloud workspace without sacrificing its dependability and performance (Manda et al., 2022). Security policies, which include service-level agreements (SLAs), forerunner trust, and service-client management challenges, are dependent on authorities. SLAs also fulfil customer requests and validate the terms that exempt suppliers from liability for outages or problems with execution. SLA is unable to guarantee that a certain task will be completed.

Client Management Issue

From a security standpoint, one of the major concerns with cloud computing is client administration. Information in the client organization system is not available in the open cloud.

Application Issues

The weakest aspect of a software program is its security. The more important components of the apps are front-end, back-end, parallelism, structure, and a variety of platforms with a variety of flaws. The software is written by a variety of developers in a variety of languages, and many programming dialects have flaws.

Cloud Data Storage Issue

Data storage is one of the most important aspects of cloud computing. Information storage and cloud computing security are major concerns as a result of the proliferation of online apps and devices (Rhoads & Smith, 2024). Network Cloud computing has faced a major challenge known as network security because it has always been essentially dependent on the network. A developing subfield of computer security, network security, and information security is the main connection between network and cloud security. In practice, there are several security issues with networks. According to R. Buyya et al. (2017) (Syed et al., 2022, network administrators must thus implement preventive components and administrations and adopt suitable security ways to safeguard the data and cloud infrastructure. Regrettably, network security has encountered significant association accessibility threats, such as flooding attacks, denial of service (DoS), distributed denial of service (DDoS), and flaws in internet conventions.

Operating System Base Issue

A number of virtual computers are used in cloud computing. Numerous operating system collaboration groups and server classifications in intra- and inter-networks have led to a number of security problems.

5.2. Webpages Dataset: Importance and Relevance

Building machine learning models to perform a variety of webpage analyses is made easier with the help of the Webpages dataset. Both supervised and unsupervised learning models can be developed. However, it is important to keep in mind that there isn't yet a large enough dataset in the public domain to facilitate research in this field.

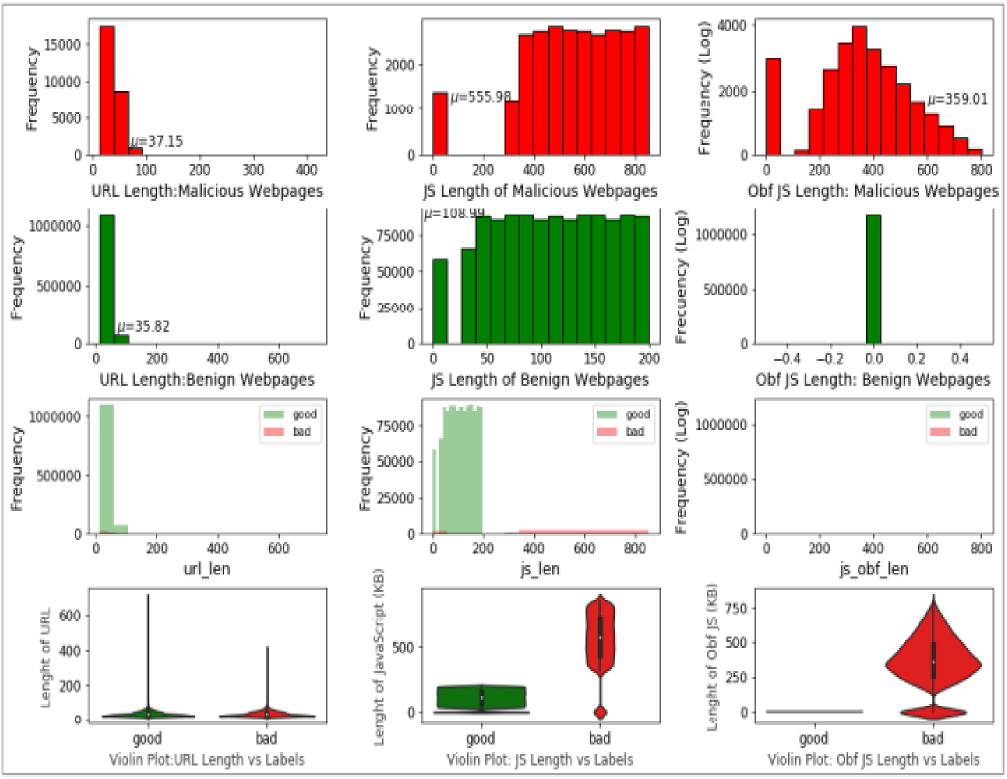

Figure 3: Plots of Univariate

All researchers working in the field of online security will gain from it. Additionally, cyber security and anti-virus organizations might utilize this data to model their security products. It has enough qualities to provide more understanding. In order to support future study, Additionally, this data contains processed raw web content, including JavaScript code, which can be used to extract additional attributes if needed. It is helpful for the Internet security research community, cyber security firms, and Cyber Law Enforcement agencies when they are creating policies. The dataset was created with the downstream purpose of classifying webpages as benign or harmful in mind.

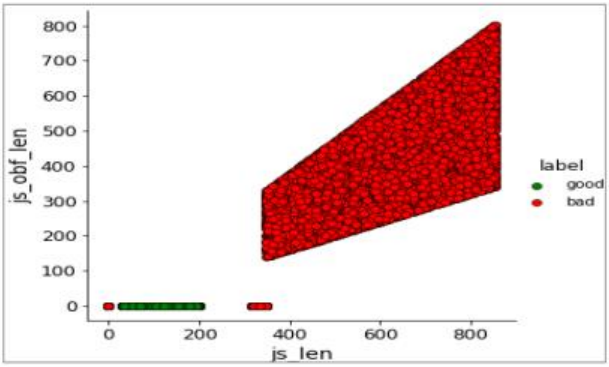

Figure 4: Bivariate Pairwise Plot

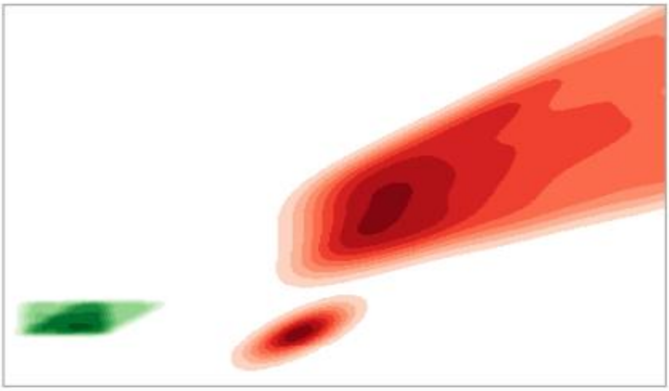

Figure 5: Bivariate Density Plot

Nonetheless, this dataset has enough data to be applied to any machine learning application involving webpage analysis. A webpages dataset is essential to Zero

Trust Architecture (ZTA) because it makes it possible to gather and examine a variety of web page features, content, and structures, which aids in the creation of strong cybersecurity defences. Researchers and developers can improve threat detection, prevention, and incident response capabilities by examining webpages to find trends, abnormalities, and possible vulnerabilities. Additionally, ZTA's defences can be strengthened and a culture of constant monitoring and trust verification can be fostered by using webpage datasets to train machine learning models to identify and categorize harmful web content, such as phishing sites or malware-infected pages.

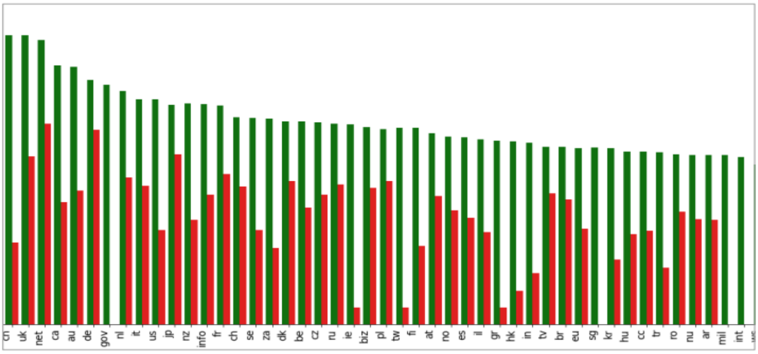

Figure 6: Plot of Top-Level Domain ('tld') Attribute

'tld', the seventh attribute, provides the webpage's Top Level Domain Name. Figure 7 shows a visualization of this property. This dataset includes webpages from a wide variety of domains, as the graph illustrates.

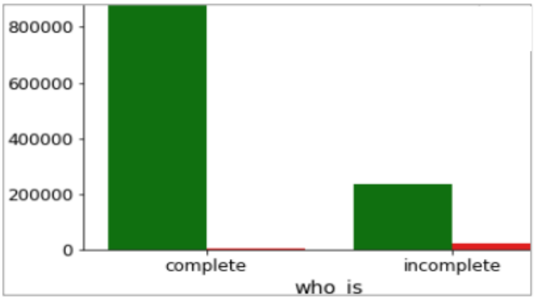

Figure 7: Registration Plot

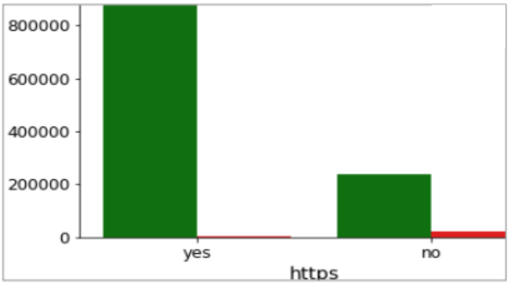

Figure 8: HTTPS Plot

'Who is' and 'https' are the eighth and ninth attributes in the collection, respectively, and they indicate if the webpage uses HTTPS and whether its WHOIS information is complete. Both of these attributes are categorical. The 'who is' property provides the completeness of domain registration information for websites hosted with domain registrars. The 'https' element indicates whether or not the web server delivers the webpage using the HTTP secure protocol. These two characteristics are shown in Figures 8 and 9.

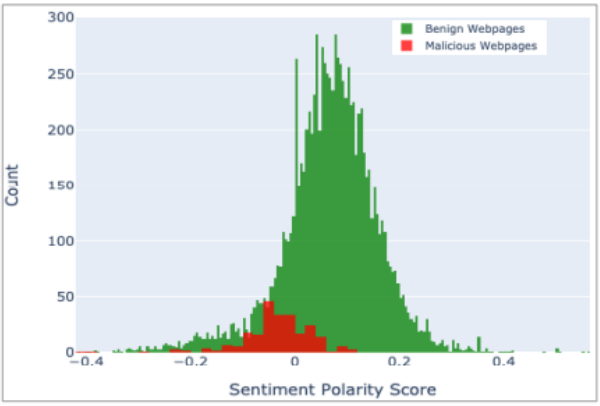

Figure 10: Web Content: Sentiment Score

'content' is the dataset's eleventh attribute. JavaScript code and other raw web content are contained in this property; they have been cleaned and filtered to minimize their size. This attribute was included in the dataset with the intention of facilitating more attribute extraction from the dataset, should that be needed in subsequent studies. Additionally, this unstructured web content can be used directly for experiments with some machine learning approaches, such as deep learning (see Chapter 6 for an example of this). Figures 10, 11, and 12 below display this raw content's vectorized plot.

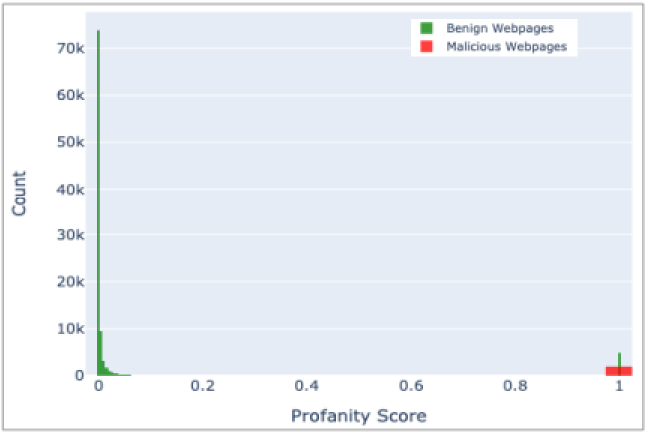

Figure 11: Web Content: Profanity Score

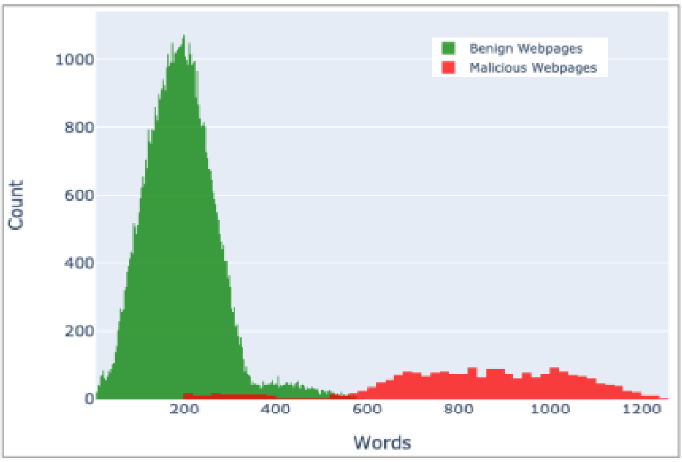

Figure 12: Web Content- Word Count

6. DISCUSSION

Every time a device wishes to connect to the network, it should be authenticated and granted only the minimal amount of access necessary to carry out its intended role. This is crucial given the evolving security landscape of today, particularly with regard to IoT networks. Imagine a situation where a conference room's smart TV serves as the display screen. It can end up being a bot that launches a DDoS attack or a spying gadget that compromises data or privacy. There is a great deal of risk because it is linked to the same network as the company that houses sensitive information like finances and human resources. Therefore, greater duty to prevent data misuse accompanies increased capabilities. Every effort is being made to minimize human involvement in order to improve the Quality-of-Experience (QoE) in a seamless manner. An exploit's risk surface grows as a result. When an attack targets medical, emergency, or mission-critical communication systems—where communication must be dependable—the casualties are devastating. The loss could be financial, private, or life-threatening. Therefore, fine-grained access control must be put in place and each device requesting access to a resource must first be authenticated. The emphasis is now on selectively protecting the data or resources depending on the potential harm they could do if lost or compromised, rather than protecting the network's perimeter. The information might be readings from various Internet of Things devices or each device's credentials, which are needed for access control. Due to their inherent resource limitations, IoT devices will need to rely on an external agent, such as cloud storage, in order to handle data on a big scale. Resource-constrained gadgets are those that have limited processing and storage power and frequently rely on batteries (poor energy budget) (Chokkanathan et al., 2024). However, there is always a chance of a privacy violation when you entrust sensitive information to an outside authority. Any leak of personally identifiable information, including a user's location or identity, is considered a privacy breach. It is necessary to handle the data such that it cannot be associated with the user. The IoT system becomes centralized when a single authority controls all network access control, which has an impact on the system's scalability. Additionally, it exposes the system to a single point of failure. In IoT networks, access control and authentication should ideally be limited to the objects from which they originate, making it impossible to steal their identity by removing the essential components. When nodes are engaging for the first time, this fosters trust, particularly in a foreign network.

7. CONCLUSION

Traditional architectures are fundamentally different from zero trust. It secures direct access to IT resources rather than networks. It controls access according to context and risk rather than identification, which is susceptible to theft. The architecture is delivered as a service and at the edge by a dedicated cloud, which serves as an intelligent switchboard that permits safe, one-to-one connections between users, devices, workloads, branches, and applications, regardless of where they are located. To put it another way, zero trust separates network connectivity and security. It enables businesses to use the internet as their corporate network in an efficient manner. In order to replicate these actions, the Zero Trust Security Model takes stringent steps to verify the identity and intent of users, devices, and the interdependent factors in the system environment. These rules are considered economical and effective since they outperform the latency in the conventional security model. The perimeter-based deployment of the old security framework has led to ransomware, malware, intrusion, and data theft. As a result, the ZTA meets this goal; nevertheless, because to the lack of knowledge on this design, its adoption is restricted. We offer a literature-based assessment of the ZTA architecture's effectiveness and efficiency along with a conceptual overview of it. ZTA, therefore, removes the trust vulnerability in an organization's information system, and the model may be combined with various security frameworks and put into practice. From the standpoint of policy, the architecture is founded on the principle of "never trust" and attempts to identify and verify individuals and devices prior to granting them access to infrastructure and resources. The rapid pace of digital transformation requires a security architecture that can keep up. Traditional perimeter-based tactics are no longer sufficient due to their inherent shortcomings. Today's cybersecurity problems can be solved with zero trust architecture's emphasis on dynamic, context-based laws and secure, any-to-any connections.

REFERENCES

[1] Rebouças Filho, W. L. (2025). The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. *Brazilian Journal of Development*, *11*(1), e76836-e76836.

[2] Hubbard, T., Klimavicz, J. F., Wong, S., & Steinhoff, J. C. (2021). Zero trust in a virtual cybersecurity world. *The Journal of Government Financial Management*, *70*(2), 12-19.

[3] Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, *156*, 103414. https://doi.org/10.1016/j.adhoc.2024.103414

[4] Roy, A., Dhar, A., & Tinny, S. S. (2024). Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review. *Journal of Computer Science and Information Technology*, *1*(1), 25-50.

[5] Stafford, V. (2020). Zero trust architecture. *NIST special publication*, *800*(207), 800-207.

[6] Sharma, H. (2022). Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security. *ESP Journal of Engineering & Technology Advancements (ESP-JETA)*, *2*(2), 78-91.

[7] Ogendi, E. G. Leveraging Advanced Cybersecurity Analytics to Reinforce Zero-Trust Architectures within Adaptive Security Frameworks.

[8] Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116.

[9] Chokkanathan, K., Karpagavalli, S. M., Priyanka, G., Vanitha, K., Anitha, K., & Shenbagavalli, P. (2024, November). AI-Driven Zero Trust Architecture: Enhancing Cyber-Security Resilience. In *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE.

[10] Kim, Y., Sohn, S. G., Jeon, H. S., Lee, S. M., Lee, Y., & Kim, J. (2024). Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. *KSII Transactions on Internet and Information Systems (TIIS)*, *18*(9), 2665-2691.

[11] Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating Artificial Intelligence with Zero Trust Architecture: Enhancing Adaptive Security in Modern Cyber

Threat Landscape. *International Journal of Research and Analytical Reviews*, *9*, 712-728.

[12] Manda, J. K. (2022). Zero Trust Architecture in Telecom: Implementing Zero Trust Architecture Principles to Enhance Network Security and Mitigate Insider Threats in Telecom Operations. *Journal of Innovative Technologies*, *5*(1).

[13] Bashir, T. (2024). Zero Trust Architecture: Enhancing cybersecurity in enterprise networks. *Journal of Computer Science and Technology Studies*, *6*(4), 54-59.

[14] Abbas, G., & Gul, S. (2025). Zero Trust Architecture: Revolutionizing Cybersecurity in the Era of Advanced Threats.

[15] Patel, R., Müller, K., Kvirkvelia, G., Smith, J., & Wilson, E. (2024). Zero trust security architecture raises the future paradigm in information systems. *Informatica and Digital Insight Journal*, *1*(1), 24-34.

[16] Alagappan, A., Venkatachary, S. K., & Andrews, L. J. B. (2022). Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. *Energy Reports*, *8*, 1309-1320.

[17] Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero trust: Applications, challenges, and opportunities.

[18] Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports*, *26*(2), 215-228.

[19] Rhoads, J., & Smith, A. (2024). Effectiveness of Continuous Verification and Micro-Segmentation in Enhancing Cybersecurity through Zero Trust Architecture.

[20] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, 57143-57179.