A Zero Trust Framework to Secure IoT Devices

Aya Issa El-Zughaid[a], Zuhayr A. Funoush[a], Younis A. Younis[a*], Mohammed Yahya Alghamdi[b*]

[a]Department of Communication and Computer Networks, Faculty of Information Technolgy, University of Benghazi,Benghazi, Libya
[b]Department of Computer Science Faculty of Computing and Information, Al-Baha University, Al-Baha, Saudi Arabia

[*] Corresponding author; E-mail: Younis.Younis@uob.edu.ly, myahya@bu.edu.sa

Abstract:

This new age of cybersecurity has emerged due to the proliferation of Internet of Things (IoT) devices. Traditionally, institutions relied on security models that focused on well-defined boundaries around organizational resources. However, this approach has proven increasingly inadequate when addressing the challenges posed by IoT devices. The rapid expansion of IoT devices has rendered traditional perimeter-based security paradigms obsolete, requiring the development of new strategies for IoT cybersecurity. This research proposes a Zero Trust (ZT) security model, emphasizing the "Nil Trust, Always Verify" principle, tailored to IoT environments. The framework incorporates Multi-Factor Authentication (MFA), Single Sign-On (SSO), and core Zero Trust architecture components—Policy Engines, Administrators, and Enforcement Points—to establish a robust and adaptable security system. Key technologies like Software-Defined Perimeter (SDP) enhance secure remote access, while measures such as traffic filtering, segmentation, and encryption safeguard data privacy. Comparative analysis with traditional architectures demonstrates the framework's superior capability to address diverse IoT security challenges.

Key words*: IoT, Cybersecurity, Authentication and Authorization, and Zero Trust Framework.*

INTRODUCTION

In 2020 the coronavirus began to spread and IT teams had the great challenge of providing millions of employees with the ability to remotely connect to the corporate networks. This led to the use of VPNs in many organizations, which, as has been seen, while meeting organizational needs, increased the threat vector, impacted productivity, and broke locally installed applications. VPNs though had their flaws, a user who had the right of access to certain resources was in a position to access the whole network. Let me take to the year 2023 for a moment and see what it looks like. Approximately 80% of new digital business applications, IoT application included, are now accessed through the safe Zero Trust Network Access (ZTNA). Therefore, more than 60% of enterprises have stopped using traditional VPNs in their networks and ZTNA, while around 40% have also adopted it for various other uses

According to the research conducted by (Rose et al. 2020). In addition, IoT devices and services are rapidly emerging and are penetrating many homes at an unprecedented pace, as the recent report of the committed Gartner shows. IoT is a global network of interconnected devices whether fixed wired over the Internet or with wireless that have identities, are capable of data processing, either on their own or in coordination with human intervention. Moreover, IoT uptake is increasing more and more within all areas, with Western Europe, North America, and China in the forefront of IoT adoption Gartner (2020). A growing trend was identified in the IoT ecosystem and, in particular, in the number of M2M connections which are predicted to reach 5.6 billion in 2016 and will grow up to 27 billion in 2024 (Gartner, 2020). The opportunity of the Internet of Things market can be seen from its expected revenues which is expected to grow from $892 billion in 2018 to $4 trillion in 2025. Several applications exist with M2M connections such as smart city, smart environment, smart grid, smart retail, and smart agriculture (Fernández-Caramés et al., 2018).

This expansion in the IoT sector is therefore catalyzed by the enhanced usage of intelligent devices that utilize several important wireless technologies for example RFID, telecommunication data providers, Bluetooth, Wi-Fi, embedded actuators, and sensor nodes. In the past few years, the IoT has developed from being in its infancy to a more mature future internet (Tan & Wang, 2010). This has made it possible for there to be extensive and very fast connectivity of the various entities thereby allowing for very large-scale creation of intelligent environments. This network of connected devices presents tremendous opportunity for reinvention of and improvement to industries and lives through smart applications and integration. As the number of IoT applications grow at a very fast rate, there are issues of security and privacy (Azad et al., 2024). An unstable and insecure IoT network can hinder the full potential of new applications, subsequently reducing the demand for IoT technology. Apart from the issues accompanying the use of the internet, cellular networks and WSNs the IoT brings in new problems like privacy, authentication, management and data storage. Mitigating these challenges is critical in setting up IoT system which ensures data security and promote user confidence.

Since, the numbers of IoT devices continue to grow, management and security of such devices becomes difficult. For this reason, these devices have limited capability to perform general computation which makes it difficult for them to employ effective security and privacy solutions (Fernández-Caramés et al., 2018). The use of complex cryptographic algorithms is particularly challenging due to the resource constraints of IoT devices. Other considerations include tracking of the device, protection of the device, its general upkeep and the protection of the data which is transmitted. The main challenging requirement is the need for building a secure and reliable environment for these devices (Fernández-Caramés et al., 2018; Lo et al., 2019). These questions are not trivial and need new approaches finding efficient answers balancing the device utility and security measures to bring IoT devices across various spheres seamlessly while keeping data and users' privacy intact. In addition, the access rights with facilities related to the extension of remote connections, as well as the integration of several networks, add to these weaknesses in security. The approaches used in perimeter-based security strategies do not effectively secure this typically further developed and much more diversified virtual reality. Such models fail to provide such a shield reliably in situations where access is not limited to a specific place but is distributed in multiple devices and networks. This leads to the situation where security measures are uncoordinated, and organizational exposure to security threats enhances (Ashraf et al.,2024).

These changes emphasize the relevance of the integrated security concept that follows the Zero Trust (ZT) model. Zero trust strategy which implies no trust inside or outside a network is necessary to protect IoT devices that do not have strong security measures. This approach is also crucial for combating the challenges of remote work since security should penetrate all the endpoints. Thus, the specific conditions of IoT devices' usage and the existing difficulties of the contemporary working-from-home model prove that there must be a stringent and supple security concept built on the foundation of the Zero trust approach. The major contributions of this study include the development of the Secure IoT-ZT Framework, a comprehensive Zero Trust-based architecture designed to enhance the security posture of IoT systems. The framework is evaluated through a comparative analysis with traditional perimeter-based models, demonstrating the superiority of Zero Trust principles in addressing IoT security challenges. Additionally, a scenario-based evaluation is conducted, applying the framework within a smart healthcare system to illustrate its practicality and effectiveness in real-world IoT environments.

This paper concentrates on the practicality and utilize of a Zero Trust (ZT) security model in the organization of IoT cyber security. The investigation is designed in a way that will provide a quantitative evaluation of the applicability of ZT principles in enhancing the security posture of IoT. networks in various sectors such as healthcare. This is done in consideration of features of the Zero Trust architecture, such as its foundation, types of authentications, policies, and encryption, and segmentation as means of protecting IoT systems. The paper also layout the Zero trust management (Secure IoT-ZT) for IoT whereby every Infrastructure Resource is authenticated and checked for credentials and settings on connection to a network to avoid trickery. It also helps verify all messages sent from one resource to the other and encrypt them in a manner that makes it hard to forge them. Therefore, the framework validates the transactions before executing the transaction, and thus eliminates the abnormal or suspected transactions. In this way, with the help of the described Zero trust model, Safe IoT-ZT framework, IoT environment can improve the security situation and prevent threats and unauthorized actions.

Despite offering an extensive approach to covering the ZT framework, the present investigation does not examine the financial costs of utilizing ZT within IoT structures when integrated into the latter. In the same way, although the study acknowledges the impact of user behavior and the trends in remote access on the security issues of IoT, it does not examine the psychological motivators of user compliance with security measures or the practical change management processes that may be required to implement Zero trust security models. These are intentional to keep the study squarely on the agreed research questions, and to avoid a replication or a fragmented study of the issues at hand. Had this paper strictly observed its scope of investigation, then the following conclusion can be made making a valuable contribution on the ongoing debate on the importance of adopting Zero trust architecture in enhancing the resilience of IoT's against current and emerging threat landscapes. It presents a structured model that practitioners can readily adopt while setting distinct limits for the research's investigative scope. The remainder of the paper is organized as follows: Section II offers a synopsis of IoT, Zero trust, and Zero trust in IoT. Section III will express related work to cover several studies and articles regarding IoT security requirements and zero trust. Section IV will present the proposed Secure IoT-ZT Framework. Section V compares the traditional perimeter-based architecture and the Zero trust framework solution in meeting the evolving security requirements of IoT environments. This section illustrates a scenario-based evaluation of the Secure IoT-ZT framework in a smart healthcare system. Lastly, Section VI will wrap up the paper.

2. BACKGROUND

2.1. Internet of Things (IoT)

The IoT is an integration of numerous objects and/or objects which are reality real Wi-Fi enabled Things that are generating, sensing and sharing new values through electronics, software, sensors and/or connectivity. IoT aims for constructing a system in which the devices are interlinked and exchange data with improved accuracy, and, in the process, may result in economic gains. The IoT is made up of ordinary consumer appliances like voice assistants and surveillance cameras and big mechanical systems like aviation turbines and construction equipment. Both of these devices use sensors to collect information and then send this information to the cloud where it is monitored and controlled.

According to Lin, H., & Bergmann, N. W. (2016), IoT technology has revolutionized many areas of our lives. Besides, it has provided opportunities for the creation of innovative business models and revenue opportunities. through the collection and analysis of data for product usage, leading to improved services and offerings by decreasing the reliance on human intervention, such as a smart thermostat adjusting the temperature in a home or an intelligent factory monitoring and controlling its machines to minimize downtime and enhance efficiency. However, in a thoughtful environment, IoT and non-IoT devices and services are often blended to enhance individuals' quality of life.

Although IoT is expected to impact many areas of our lives significantly in the future, persistent security and privacy issues need to be tackled. Due to the dynamic and diverse nature of IoT-based innovative environments, addressing these security and privacy issues can be complex. Major challenges for the widespread adoption of IoT systems include constrained storage and processing capacities, concerns about performance reliability, availability of communication channels, accessibility at any time and from any location, interoperability within diverse environments, data management efficiency, and security and privacy issues (Zorzi et al., 2010; Radanliev et al., 2020).

2.1.1. IoT Architecture

While many research studies have proposed different architectural layers for the IoT, to date there is no standard IoT reference model. One common proposed design used in these proposals is that of the three-tier application, network, and perception layers as highlighted by both Khan et al. (2012) and Siegel et al. (2018). However, there has been some architectures that have proposed putting the six-layer model into a four-layer model where the six layers are structured as the sensing layer, the network layer, the services layer and the application interface layer as proposed by Li et al. (2016). Unlike the current common three and four layers, we are in harmony with the argument that multiple layers are required to address the IoT intricacies. This study presents the IoT security necessities with a security structure that has five working layers as stated by Pal et al., (2020) the five layers include user interface layer, application layer, services layer, network layer, and device layer.

All levels comprise architectural elements required for acquiring information, storing them, performing computing, and sharing data between layers and elements. In addition to the layers themselves, there are basic security needs for the system which are key management, trust management, identity management, authorization and authentication. As stressed in section 3, there are clearly many other security requirements that organizations may need to implement; yet, the present list might have to be updated at some point as the threat environment evolves. As a result, the suggested security architecture is not centralized at a certain layer or level of the IoT system. However, the proposed metrics are provided as a horizontal model that can be applied at any system level. This approach guarantees the achievement of the security objectives at every level of functionality and in the vertical plane of the IoT system.

2.1.2. IoT Security Requirements

As more people have connected IoT devices and systems across various sectors and purposes, there is a high demand for supervisory mechanisms to safeguard the IoT devices, as well as the data they gather and/or relay. Unfortunately, security is a huge concern for IoT devices because of their limited resources and distributed platform. Thus, a set of IoT security requirements has been derived to meet these challenges and assist in the design, implementation, and management of IoT security. These requirements include enforcing the privacy of the data to be stored, the data integrity and more importantly locking down the data in a way that only certain people or equipment can get access to it. These prior works involving the security of the IoT failed to highlight security requirements as a prime concern as many of them just attribute the problem to a secondary element. Yang and Fang (2011) proposed an architecture for IoT security addressing key issues that include; Authentication, access control and identity concerns in communication, control and computation. Other similar studies for instance the studies conducted by Tourani et al. (2017) and Asiri (2018) also outline basic security concerns for IoT including; authorization, authentication, confidentiality, access control, trust and identity management. Additionally, the study by Jerald, Raj & Vijayadass (2016) covers quite a number of security issues at the network, the applications, layers, bootstrapping, configuration management, data integrity, firewalls, antivirus and even encryption functions and routing. In this section, we consider these requirements to be generic and necessary for most IoT systems:

- Confidentiality: This requirement makes it mandatory that any Sensitive data sent by IoT devices and systems must not be made available to every Tom, Dick and Harry. Data encryption is possible for data in motion and data at rest; access control is also possible to implement for read and write privileges.
- Integrity: This requirement also means that information received from IoT devices as well as the systems will not be changed or modified in any way without consent. Some of the we approach that can be used include data hashing, digital signatures, and integrity checks, all which will enable one come up with the right checks that can prove that data did not change during the time it took in transit or even when it was stored.
- Availability: To meet this requirement, IoT devices and systems must be online when required and available to not be taken down for DoS attacks or other issues. For availability of the IoT systems load balancing, redundancy and failover solutions can be implemented in order to guarantee that IoT systems would be able to function despite the fact that one or several components halt to work.
- Authentication: This requirement makes certain that IoT devices or Systems can validate the identity of a permitted user or device. Secure authentication can be provided by means of a combining strong password, two factor authentication, biometric solutions etc.
- Authorization: This requirement ensures that specific resources or data in the system are only available to specific user or device. RBAC or ABAC can be used to enable this; it helps to enable information availability throughout the business organization.
- Accountability: This requirement ensures that whatever action is taken by the IoT device or the users it is recorded and monitored. Automated logging facilities are used to capture all the activities of IoT devices and the users, and such records can be utilized to solve security problems and breaches.
- Non-Repudiation: This requirement ensures that an action carried out by an IoT device or a user cannot be refuted in the future. There are some measures, for example, digital signatures that can be applied to guarantee that actions being taken are not falsified because they can be easily rejected after some time.
- Resilience: This requirement makes sure that IoT device and systems can be operational in the event that there are incidents such as attacks or others. Redundancy can be realized through duplicity of IoT systems as well as having plans in case of disruptions to provide a solution on how the systems can get up and running again.
- Scalability: This is a critical necessity on IoT security since most IoT systems are complex involving many devices and users Hassija et al. (2019). For a security solution to be applicable at scale, it has to be fast and robust along with being secure in order to handle large volume of connections and requests.

2.1.3. IoT Threats and Attacks

Due to the nature of IoT devices being constrained in resources, many of the security approaches which might need many resources are not suitable for implementation in IoT devices hence the vulnerability to attacks. There have been a lot of published research focusing on security of IoT and in these research papers the various threats and attacks that could happen have been identified by Ahmad et al. (2019) among others, Yang et al. (2017). There are some works that, for instance, Ko et al. (2017), have tried to categorize threats and attacks based on the different layers of an IoT system. Some other work, Sfar et al. (2017) have also proposed the threats and attacks in light of the confirmed security issues such as identity, access control, trust, middleware, and mobility. A few works like Alaba et al. (2017) have grouped threats and attacks based on specific application and use cases. Further, based on the kind of structure used within the IoT, Roman et al. (2013) classify different security challenges: centralized IoT, collaborative IoT, connected IoT and distributed IoT. Briefly, some common threats and attacks that can affect the security of IoT devices and systems include:

- Malware: A type of virus targeting IoT devices and systems for attacker's remote control over them.
- Denial of Service (DoS) / Distributed Denial of Service (DDoS): An attack that floods an IoT device or system with to high traffic volumes to the point where it becomes inaccessible.
- Man-in-the-Middle (MitM): An attacker eavesdrops and alters messages sent between IoT devices, it also can receive some information it is not supposed to get.
- Physical Attacks: Real-time threats that target the physical vulnerabilities inherent to IoT, for instance, breaking into a house by cracking the smart lock controlling the entry.
- Botnets: A large number of malicious IoT end-points within the hands of a single attacker to coordinate a massive attack.
- Credential Stuffing: Cybercriminals use stolen password or user account details to gain unlawful access to IoT gadgets as well as networks.

2.2. Zero Trust Concept

Zero Trust is a security model that itself is assumed that all individuals, computers, and networks are inherently hostile and any access to the resources require approval. This approach is quite different from traditional security models that merely focus on securing the boundaries and taking the internal users and connected devices at their word Xiangshuai, Y., & Huijuan, W. (2020) reified and authenticated. This approach contrasts with conventional security models that rely on perimeter defense and trust users and devices on the internal network Xiangshuai, Y., & Huijuan, W. (2020). This reflects the Zero trust concept by branding it as the "never trust, always verify" philosophy. Any request made by either a user or the device whether is internal or an external resource is first checked through this method. This entails; This user authentication, Checking on the security of the device in use and Whether the access request relates to the user's profile Xiangshuai, Y., & Huijuan, W (2020) Originally, the zero-trust model stemmed from a rarity was when a group of IT security specialists came together in 2004 to form what was known as The Jericho Forum The Open Group (2024) field and authenticated. This approach contrasts with conventional security models that rely on perimeter defense and trust users and devices on the internal network Xiangshuai, Y., & Huijuan, W. (2020).

The "never trust, always verify" philosophy illustrates the Zero trust concept. Whether the user or device is internal to the network or external, every resource access is validated using this method. This involves verifying the user's identity, the device's security, and the applicability of the access request Xiangshuai, Y., & Huijuan, W. (2020). Zero trust has its roots in the "Jericho Forum," a group of IT security professionals who came together in 2004 to develop a new approach to network security The

Open Group (2024). The Jericho Forum also understood the status of restricting security solely with firewalls and several other network appliances mounted around the organization's perimeter as insufficient to address the continually evolving nature of computing architecture. In response, the Jericho Forum introduced the concept of de-parameterization as the new security model that states: Trust nothing, verify everything. This model understood that threats could be internal or external and that the need to have access controls where they are required is at every system level as opposed to only at the outer fringes of the network. The Zero Trust concept gained broader attention in 2010 when Forrester Research published " No More Chewy Centers: This paper started by presenting one of the most recent models of Information Security, known as the Zero Trust Model of Information Security (Kindervag, J., 2010). The report contended that conventional security paradigms were unable to cope with emerging threats like APTS and Insider Threats and proposed an identity-based security model which was a continuous process.

In February 2013, the United States issued a Presidential Executive Order on Cyber security in response to cybersecurity threats' increased quantity and sophistication U.S. Presidential Executive Order. (2013, February 12). This order said cyber-attacks are a clear and present danger, making Cyber Defense a national priority for agencies including the Department of Homeland Security and the National Science Foundation. This Executive Order featured a call to action. After that Year, the Zero trust became more popular as the security concept and many organizations use it as the approach to security. The NIST also has produced a Zero trust architecture framework through which the Zero trust security model is being implemented at the National Institute of Standards and Technology a Zero trust architecture framework, which guides the implementation of a Zero trust security model at the National Institute of Standards and Technology (2013). Zero trust has the concept of creating a security structure as infrastructure that can be utilized by many enterprises.

This paper defines them as follows: A fundamental tenet of Zero Trust is the ability to provide safe access to all resources regardless of their location as well as the ability to treat all network traffic as a security risk in the absence of authorization, inspection or encryption as detailed by National Institute of Standards and Technology (2013). In Zero trust, the word "zero" means it's not about having "zero" trust in the literal sense but about having "zero" trust in the sense of inherent or implicit trust. Zero trust is all about methodically laying a foundation of trust and then expanding that trust to allow the correct level of access at the right time. A few companies have implemented zero trust network security (Townsend, K. (2015)—for example, the Cisco Application Centric Infrastructure (ACI) (Cisco. (a2014) Whitelist-Based Policy Model Supports Zero Trust Security Architecture Cisco. (b2014). By default, Cisco ACI does not trust new endpoints but checks for connectivity against an allow list policy. Traffic between two endpoints can be allowed, denied, logged, redirected, or instantiated using these policies (contracts).

2.2.1. Zero Trust Architectures

It is essential to recognize that different architectures and commercial products can support this philosophy. As a result, there is no universal solution that fits all scenarios., and each organization should evaluate its unique requirements to determine the best path toward implementing Zero trust.

- NIST Architecture: NIST has published a particular SP 800-207 National Institute of Standards and Technology publication. (2013) outlines the Zero trust architecture as "an enterprise cyber security strategy that removes any implicit trust in individual elements, nodes, or services, necessitating ongoing verification of the operational landscape through real-time data from multiple sources to assess access and inform other system responses," as outlined in the NIST Zero Trust Architecture has three core components: the Data Component, the People/Identity Component, and the Infrastructure/Network Component.

- Gartner Architecture: On the other hand, Gartner has proposed its own Zero trust architecture Gartner (2020), called the Continuous Adaptive Risk and Trust Assessment (CARTA) model. The CARTA model aims to continuously assess and adapt to the risk of every user and device in an organization's network rather than simply trusting those inside the perimeter and distrusting those outside it. The CARTA model consists of four main components: Continuous assessment, Adaptive access, Risk-based policies, and Continuous monitoring. Furthermore, as Gartner put it, ZTNA refers to the removal of the over reliance on employees and partners who access apps and data, through traditional technologies such as VPNs. ZTNA employs the 'never trust, always verify' model, which means that trust in any zone is constantly being verified in real time because of the changing standing of the user. Furthermore, there is the software-defined perimeter (SDP), which provide contextual user access and defends services from hackers and malware. There are two main approaches to implementing ZTNA: it is divided into two categories namely endpoint initiated and service initiated.
- CISA Zero trust Maturity Model: In more recent or the current year the Cyber Security and Infrastructure Security Agency (CISA) has helped organizations move to the right Zero trust Maturity Model. The model establishes a foundation and framework for organizations to understand how they fare on their path to the Adoption of a more robust Zero Trust paradigm CISA. Zero Trust Maturity Model is made up of various levels or phases, each of which defines specific maturity of Zero Trust principles.
- Palo Alto Architecture: Another Zero trust architecture approach is Palo Alto Networks Zero trust Reference Architecture Palo Alto Networks (2024) and uses the identification and verification of all users and devices approach and continuous monitoring and risk assessment. It includes four components: SASE which stands for Secure Access Service Edge, Identity management, Network security and Data security. This component is responsible for encrypting data that is still and data in transit. They are technologies that include, but are not limited to Data Lose Prevention (DLP), data encryption, and data classification to guard data against loss or leakages.
- These are some of the current implementations of Zero trust architecture and our Zero trust architecture or framework, as will be revealed later.ps and data using traditional technologies like VPNs. ZTNA operates under a "never trust, always verify" approach, continuously reassessing trust validation in real time based on the user's context. Moreover, the software-defined perimeter (SDP) offers contextual user access that shields services from hackers and malware. There are two main approaches to implementing ZTNA: of which include the endpoint-initiated and a service-initiated types.
- CISA Zero trust Maturity Model: CISA has developed a Zero Trust Maturity Model to help to put into practice the Zero trust Model for entities. The model offers a framework, and best practices for organizations to evaluate the state of their security and their journey towards the implementation of the zero-trust Zero trust architecture CISA. The Zero Trust Maturity Model is divided into stages or levels which we are going to discuss in detail in the following subsections, with each level of the model indicating a specific level of Zero Trust strategy implementation.
- Palo Alto Architecture: Another Zero trust architecture approach is Palo Alto Networks Zero trust Reference Architecture Palo Alto Networks (2024), and according to it, all users and devices should be authenticated and authorized continuously, and the system should monitor the risk level persistently. It includes four components: SASE, Identity, Network security, Data security. This component safeguard data that is stored on the system as well as data being transmitted from one point to another. As implemented solutions it has features like DLP, encryption and data categorization as means of preventing access or leakage of critical information.

These are just a few examples of existing Zero trust architectures and our Zero trust architecture or framework, which will be discussed later.

2.3. Adopting Zero Trust in IoT: Understanding the Relationship Between IoT and Zero Trust

An anatomic structure that restricts organization, users, proxies, networks, or devices in access to resources and where these subjects are considered untrusted by default requiring validation. This approach deviates from the conventional approaches of security models that focus on the borders and trusting users and devices within the internal network Xiangshuali, Y, & W Huijuan (2020). This approach differs from traditional security models that rely on perimeter defense and trust users and devices on the internal network Xiangshuai, Y., & Huijuan, W. (2020). Consequently, applying principles of zero trust improves IoT devices' security arrangements. The above- mentioned devices can easily be compromised since most are not designed with adequate inherent security and are intended to connect to a network without first authenticating it. A Zero trust approach to IoT security means that no device is to be trusted initially and if a device and the user of that device want to access sensitive data or systems of an organization then it has to prove its identity as well as the identity of user of the device. For this reason, there is the following challenge of integrating Zero trust security in IoT devices: Here are some of the critical difficulties of Palo Alto Networks (2024):

- Lack of standardization: An IoT device is something that has connectivity built into it, thus the devices are of diverse forms, sizes, and packets functionality and there is as yet no standard procedure for protecting an IoT device. It has been found that the zero trust security architecture is not easy to execute across various types of devices.
- Limited computing power: Some connected objects have limited processing capacity and storage space, and it is difficult to implement high levels of security. Thus, security solutions, which are to operate on low-power devices, have to be necessarily designed accounting for these restrictions.
- Firmware updates: As a rule, IoT devices have a long-life cycle and may not be updated to new firmware versions, or it is impossible. This can make devices open to the commonly known security bugs for a longer period of time.
- Resource constraints: Most IoT devices are characterized with restricted network and storage capacities, and low compute power which presents a problem when trying to incorporate security solutions that would demand a lot of resources.
- Distributed nature: IoT devices are typically deployed in many places, and hence centralized management and control can be complex. This could sometimes cause some areas to be left unnoticed and other areas having no security at all.

In addition, adaptation of Zero trust security for IoT devices requires a holistic approach that specifically considers the uniqueness of IoT devices and the difficulties associated with it. Maintaining awareness of new the IoT security standards and the best practices is always important in order to avoid being on the losing side.

3. RELATED WORK

Some work and papers have been published to address different issues in IoT technology. However, these contributions are still fragmented and are not adequate, and mostly cover only a few aspects of this field. However, academic and social forums and networks have not been substantially engaged as they should even though they are central to charting the future development of this field. In Whitmore et al. (2015), a research paper focuses on providing the details of IoT in terms of architecture, applications, security and privacy. The authors identify the primary directions and issues in IoT and estimate the impact of this technology on entities and societies. The survey also presents an overview of known IoT platforms and standards and indicate further studies are required. Indeed, this paper has a limitation in that it affords more concentration on the technological side of the IoT. It does not go into considerable detail about social, economic, and ethical implication of IoT, which are assuming more importance as IoT is inducted into various facets of life. In the same vein, the paper by Al-Fuqaha et al. (2015) gives background about the technologies, protocols, and applications of the IoT. It begins with an introduction to the IoT paradigm and proceeds to the enablers of IoT which are sensors and actuators, RFID and wireless technology. This paper also presents a use of communication in IoT and these include MQTT, CoAP and ZigBee. Further, it has reviewed the literatures on the various application areas like Health care, smart homes and transportation in IoT. The last section of the paper will present the future research directions and challenges of IoT. However, this paper have the following shortcomings. Many important publications are covered insufficiently or not covered at the all, and the nature of the survey does not allow paying attention to the methodological aspect of the problem. A critical discussion of the surveyed technologies and protocols is missing, as well as an indication of the disadvantages and difficulties of these technologies.

Moreover, Lin, H., & Bergmann, N. W. (2016) discuss the issues of privacy and security in smart home domain when the IoT becomes the part of smart home. The authors describe different security and privacy threats such as data safeguards, access control, device identification, and authorization in smart homes. Smart home applications are discussed concerning the problems of privacy and the paper provides a framework for privacy protection based on the access control and data encryption practices. Moreover, the authors present the predicted measures to address the security and privacy challenges of smart homes such as; block chain, IDS, MFA. This paper raises the importance of further studies and the enhancement of proper security and privacy frameworks for smart home with IoT solutions. The main limitation of this paper mainly lies in the fact that while presenting the privacy and security challenges in smart home applications, there is limited information on other applications and uses of the IoT. For example, it has no case studies to back up its assertions and suggestions. It largely depends on the opinions of the authors of the works used. Lin, H., & Bergmann, N. W. (2016) have covered all the aspects of security in the IoT and have described in detail in the given paper. This reflects on the special characteristics of IoT that provoke security concerns including the heterogeneity, the resource limitation and the distribution. The authors also give a clear and comprehensive analysis of security threats and attacks for IoT that is eavesdropping, spoofing, denial-of-service, data manipulation among others. The original security mechanisms and protocols in the IoT security area are also presented in the paper such as the access control, authentication, encryption, and key management. Last, the paper outlines the research avenues and limitations in the context of IoT security. The main weakness of this paper can be viewed in the limitation of the discussed security aspects of IoT which excludes other aspects like scalability and interoperability. Yang and Fang in their paper; Yang, J., & Fang, B. (2011) presented a concept of a security model and some key technologies for the IoT. According to the authors, the model, which has been designed with host and network security in mind, cannot be employed when it comes to IoT as there are numerous devices with low computing power as well as limited storage space. Instead, they propose a three-layer security model for the IoT: security at the perception level, security at the network level and security at the application level. The main goal of the perception layer security is to safeguard the sensor nodes as well as the information they convey with regards to the network layer security, it is principal role is to ensure secure communication among the nodes. Last but not the least, the security at application layer can make sure that only those persons who are legally permitted can manage or operate the IoT devices. The authors also examine some technologies useful for the realization of this security model, namely cryptography, authentication, and access control.

This paper also presents a secure IoT architecture developed by Jerald et al. (2016) for an integrated smart services environment. This architecture is designed to enable secure machine to machine communication, exchange of data between IoT devices, cloud services and the human end-users. It comprises several layers: As a result, four dimensions have been identified as perception, network, service and application. All of them proposed individual layers where safety measures such as authentication, encryption, and access control are to be implemented to provide secure communication and exchange of information. The performance of architecture is evaluated through an example that illustrates how it can be used to enhance security of communication and data exchange between different stakeholders in the IoT environment by Lo et. al. (2019). This paper has only one weakness because the authors suggested an architectural design that does not include the detailed strategies for implementing and the original approach has not been tested with an actual application to measure how beneficial it would be. It also remains ambiguous on how this proposed architecture meets some of unique challenges that face IoT including the issues of resource limited environment and scalability. Moreover, the paper does not also provide information on whether there are losses of security in an attempt to achieve improved performance in the recommended architecture. In their work, Rose et al. provided only an abstract description of what can be considered as Zero trust Architecture (ZTA). They painted a picture of how ZTA could especially be of benefit when it comes to improving the cyber security status of an enterprise. Also, they identified generic deployment scenarios and cases for ZTA and thereby enriched the extant knowledge on this subject Rose et al. (2020).

Continuing the line of thought, Embrey notes other reasons why ZTA has been implemented, including better protection, policy management for users and devices. Speaking to this, Embrey said that ZTA has a crucial role in handling such issues. The article by B. Embrey has no real case study and data analysis and discussion and filled with the author's opinions and industry observations. As a result, it might not have a clear view of the forces propelling the adoption of Zero trust. The article is quite short and does not explore the substantiality of the Zero trust concept in detail (Embrey, B. (2020). Mehraj and Banday presented a novel approach to implement Zero trust security model specifically for cloud platforms and underlined the trust-building phase and its difficulties in cloud computing. However, this paper does not contain a comprehensive discussion of the performance comparison of the proposed solution with other methods in real-world cloud computing systems. Additionally, the authors failed to discuss the prospects of the barriers and weaknesses of implementing Zero trust model in cloud computing Mehraj, S., & Banday, T. M. (2020). While working on the identification of separate components of the Zero trust architecture and the critical technologies necessary for its adoption Yan, Wang prehensive evaluation of the proposed framework and its effectiveness in real-world cloud computing environments. Further, the authors did not address the potential challenges and limitations of implementing a Zero trust model in cloud computing Mehraj, S., & Banday, T. M. (2020). Yan and Wang conducted a comprehensive investigation on the essential components of Zero trust architecture (ZTA) and the crucial technologies used in its implementation Xiangshuai, Y., & Huijuan, W. (2020). They also used some of these technologies in different cases as to demonstrate the advantages of ZTA in the different situations. However, one weakness of this paper is that it discusses the theoretical pointers of Zero trust without offering tangible directions for organizations intending to adopt the model. Furthermore, the paper provides only a short discussion on the possible drawbacks of implementing Zero Trust or its criticisms including, but not limited to the following: the model may be cumbersome; it may affect a user's experience.

The work done by Sood (2020) includes an analysis of the major problems that arise in the process of implementing block chain and ZTA, for example, the inability to work on a large scale and the lack of possibility to create a single unified block chain platform. Further, the authors present an overview of some of the most current research within the subject area together with different examples of usage and possible applications and present an evaluation of further research opportunities in this area. Nevertheless, the paper does not include extensive technical descriptions and does not compare the proposed strategy in practice either. Also, it is worth noting that the paper overlooks the possibility of the problems that can be experienced when trying to implement block chain in the ZT architecture at a larger scale. Atwal et al., R. P., & Chauhan, S. (2021) attempt to provide a comprehensive literature review on Zero Trust Network Architecture (ZTNA) concept that has emerged as one of the most popular models for network security. The authors explore the evolution of ZTNA, its foundation, and main features of an effective ZTNA. They also provide a brief state of the art of ZTNA: its difficulties and possibilities for future development. The survey serves as a useful reference for those who are engaged in research, or who are associated with implementing aspects of the ZTNA on the networks they manage. However, the paper lacks the depth by which new knowledge and contribution to the understanding of ZTNA can be derived from the paper. For that, the results found in the survey are only bound to the solutions available in the market. It fails to look at any research avenues or obstacles which have to be addressed in the advancement of ZTNA. Secure IoT-ZT Framework

4. THE PROPOSED ZERO TRUST FRAMEWORK

Figure 1 depicts the proposed framework for deploying the "full Zero trust" architecture. It encompasses most approaches, effectively addressing concerns and achieving the desired benefits. Let's delve into the details of how this approach is implemented:

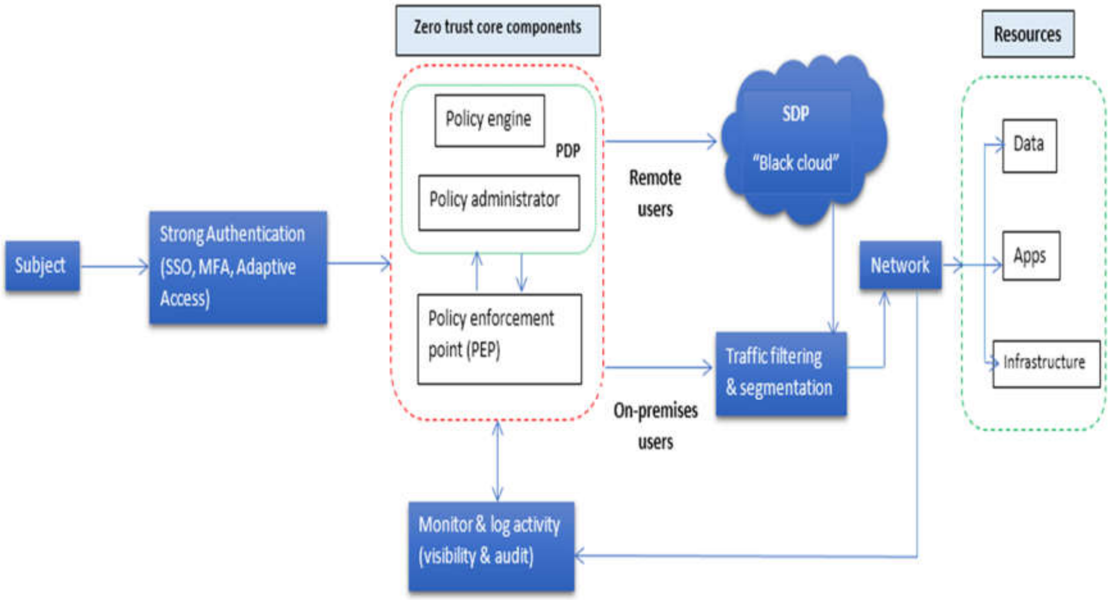
Zero trust core components
Resources
Policy engine
PDP
Policy administrator
Policy enforcement point (PEP)
SDP
"Black cloud"
Remote users
On-premises users
Subject
Strong Authentication (SSO, MFA, Adaptive Access)
Network
Traffic filtering & segmentation
Data
Apps
Infrastructure
Monitor & log activity (visibility & audit)

Figure 1. Secure IoT-ZT Framework.

4.1. Subject

As Gartner recognizes it, zero trust encompasses users, devices or services asking for permission to use resources within the internal network or systems of an organization. By contrast, NIST offers a conceptual definition of a subject and sees it as an entity capable of initiating actions or operations on objects of an information system and may encompass users, applications or devices interacting with the latter National Institute of Standards and Technology. Within an information system, including human users, applications, or devices that interact with the system National Institute of Standards and Technology. (2013). As such, subject means an entity, which can be a user, application or a device that communicates with an information system or a network whether through a remote or physical access.

4.2. Strong Authentication

The authentication methods enhance security by streamlining access, adding layers of verification, and dynamically adapting to the risk level of each authentication attempt. The authentication method can be:

- Multi-Factor Authentication (MFA): Customers must provide a number of factors, and the use of passwords is supplemented with other means of ensuring the identity of the site's visitors.
- Adaptive Access: The authentication is then dynamic and can confirm to a number of parameters including but not limited to the: user's activity, type of device in use, and geographical location of the device before forwarding it to undergo the required level of security that the access attempt calls for.
- Single Sign-On (SSO): The applications enable a single sign-on mechanism, which means the users can get access to different applications or systems using the same username and password as in a single application.

4.3. Zero Trust Core Components

The Subject is considered to be functioning within an untrusted environment, whether the access is remote or at an enterprise perimeter. To access the enterprise resources, the Subject must go through Zero trust core components, which are:

- Policy Engine: This engine defines and enforces access policies within the Zero trust environment. Based on the defined procedures, it evaluates the subject's request and determines whether it should be granted or denied.
- Policy Administrator/ Policy Decision Point (PDP): This position makes policy decisions. It takes input from various sources, such as user attributes, device information, network context, and security events, and evaluates it against the defined policies. The PDP determines whether the subject's request aligns with the security policies.
- Policy Enforcement Point (PEP): is accountable for enforcing the policies defined by the policy engine. So as per the guidelines usually it works as a mediator between the subject and the resources which subject wants to access. The PEP which stands for the protection of the subject's request checks whether the subject is allowed to gain permission and allows or denies access according to the security policies set.

The data plane is used to allow for the communication between the subject and the enterprise resource, while the control plane differentiates its operation. With respect to the control plane, the PDP and PEP exist as separate entities across a network that can be connected to no enterprise resources. On the other hand, the data plane is concerned with the application data plane traffic that is the actual data transfer. That way, there is no confusion between the implementation of access policies and the actual data exchange in a way that improves the ZT architecture's security and stability.

4.4. Advanced Secure Access Solution (ASAS)

Another approach in a Zero Trust environment is that any user more or less connecting from a remote location is able to request entry to the enterprise by utilizing a Software-Defined Perimeter (SDP). SDP is an open security model that is used to provide secured access to application and resources regardless of geographic location of a person and the type of network that the person is a part of. After the identity of the user is authenticated, SDP creates a secure tunnel through which all traffic is HTTPs with "Black Cloud" resource, which means the data is protected but only authorized devices can access the network. This method also gives users the principle of least privilege, giving users access only to those resources required for a given task.

4.5. Traffic filtering and traffic segmentation

In relation to the Zero Trust environment, traffic filtering means the process of choosing or rejecting network traffic based on certain principles and regulations. This process can assist in combating different threats including unauthorized access since the acts are simply filtered out. Since strict traffic filtering is being implemented, only relevant and approved traffic is only allowed hence reducing the possibility of data breaches. The means of traffic management and the principle of limiting threat movement across the network by splitting it into separate segments or zones is called segmentation. This strategy provides small perimeters around specific resources or asset in a Zero Trust environment. It also operates to restrict even subjects' access to the content based on their roles, privileges, or according to the principle of least privilege, to only segments or zones of the content as necessary.

4.6. Resources

Under Zero trust architecture, resources mean data, application, and systems that requires protection. Data means the data that is populated into the network and may contain confidential information; applications relate to the software systems and services; while infrastructure implies the network devices and units.

4.7. The third activity that needs to be implemented is Continuous Monitoring and Logging.

These are part of the Zero Trust architecture that offer continual monitoring, and real-time auditing, and threat identification. In this manner, it becomes possible to protect the valuable resources, which are available in the organization's network, and also assertively and actively counter the new and evolving threats which are inherent in cyberspace.

5. COMPLIANCE TO IOT ENVIRONMENT WITH ZERO TRUST ARCHITECTURE

A Zero Trust model is capable of being a very strategic approach for limiting access and use of an IoT ecosystem. Even within the network perimeter, zero trust does not trustee any device or user in the environment based on a standard set of default assumptions. However, in the proposed scheme, every device and user have to authenticate it and authorize the access of resources time and again. It is worth to note that there are different approaches of implanting Zero Trust, which can be elsewhere referred as Zero Trust Architectures. Another model is the CISA Zero Trust Maturity Model covering the same topic and designed to provide organizations with a framework for any maturity level to help implement Zero Trust (CISA, 2020). This model is based on five pillars: identity, equipment, software, information, and connections. The second well-known Zero Trust architecture is a model that has been created by the National Institute of Standards and Technology (2013). This model gives emphasis towards the aspect of constantly validating and providing permissions to the user, devices and services for accessing the resources. It also highlights how the technology of network segmentation, visibility, and monitoring to help network owners to identify a threat and handle it appropriately. Other even more comprehensive models which are have also been developed by research and advisory firm called Gartner in a form of Zero trust model with a key focus on CARTA. Contrary to earlier models, this model focuses on constant evaluation of risk and trust, and of security controls as events progress. Therefore it is possible for organizations to adopt several Zero trust models to enhance security of their systems as well as data security. While each model may have its main concern or special focus, it all has the zero trust prerequisite and revalidation of access to the resources in common.

Based on the above literature, some recommendations can be made to ensure that an IoT environment is driven towards the Zero Trust Model. Some measures are setting up access control measures, using network segmentation, enforcing data encryption measures, and monitoring and logging continual measures, and employing Software-Defined Perimeter (SDP). Thus, applying mentioned measures, the organizations achieve a high level of protection for IoT environments and exclude unauthorized access to their resources. Here, we will view the most critical steps for Zero trust architecture and how we can apply it in an IoT environment in detail:

5.1. Identity Assets

Identity assets are people, roles or objects that need to be identified and approved to gain access to resources. Such entitlements can directly involve the user, a device, an application, and even a network. These identity assets are assigned an identity to ensure that their credentials and authorization to CISA is valid identity asset. In this step, we are required to list all IoT devices, categorize data and determine applications, the system for their administration, and the network on which IoT operates – all as described in the background section.

5.2. Segregate your network

Isolation of the network in an IoT scenario simply refers to grouping of devices or applications with dissimilar or varying security levels into distinct networks Tan & Wang, 2010 Palo alto networks 2024. It means that sensitive or less significant device remains independent and in contact only with the devices needed for its operation. This way, you can sufficiently reduce the chances of invasion and hacking within the network since the dangers moving from one sector of the network to the next. Segregation can be achieved through:

- Define your trust boundaries: However, the prerequisite to adopting a Zero trust network model is defining the boundaries of trust. This entails determining the devices, apps and data that you rely on in the IoT setting and those which you cannot put your trust on.
- Network segmentation policies: The motive of the network segmentation policies is to divide your IoT environment into a number of segments to reduce the carefully of cyber-attacks. Network segmentation can be done by physical segmentation or by using Virtual Local Area Networks or Software Defined Networks. Other policies in place within a Network segmentation include the firewalls or the intrusion detection and prevention systems as well as Network Access controls that regulate traffic flow between segments of an IoT network.

5.3. No more than the amount of access that is necessary should a user be granted

The principle of least privilege is most often associated with access control. The concept is about constraint on the usage that is a security process that controls to whom or what is capable of accessing any resource within a computer system. It entails controlling use of the devices, systems, data or network through the use of mechanisms such as passwords, user IDs and firewalls that only permits allowed processes to gain access to systems of Palo Alto Networks by the year 2024Access control can be implemented through various methods, including:

- Role-Based Access Control (RBAC): This method manages or regulates the resources in line with the roles of the users. For instance, there are may be unique roles that can be created within an IoT system like an administrator, technician and or the end-users with varied privileges.
- Attribute-Based Access Control (ABAC): ABAC is a more flexible model that identifies multiple attributes of the user such as title, location and clearance, to grant access to certain resources.
- Context-Based Access Control (CBAC): This model works with information related to an access request, location of the user or the time of the request.
- Mandatory Access Control (MAC): MAC is a very stringent model of access control that uses a script for management of resources and user access to these resources. What it is: It is generally employed in such environments as governments and military bases.
- Discretionary Access Control (DAC): DAC gives consumers the power to manage who can access their resources. For instance, within the same framework, users might restrict the interaction with their IoTs to only specific personnel.

Since there are different types of IoT concerns, so, the kind of access control techniques that can be used depends on the need of a given IoT system. The choice of approach will therefore depend with factors including the type of your setup either small or complex, the devices and resources being managed, and the security/compliance levels you need to meet. Also, there are some tools that can help in the fulfilment of the principle of least privilege in your IoT setting. The tools selected will basically depend on your set-up and the extent to which you need access control. Some examples include:

- Privileged Access Management (PAM) Solutions: The above tools are derived for controlling and handling of privileged access towards the most sensitive systems and information. In an IoT context, PAM solutions make certain that only those people who should access certain devices and information do so.
- Identity and Access Management (IAM) Tools: IAM also means a centralized approach of controlling the user and the device identity as well as the permission's they are given. Therefore, IAM practices can make it possible to adhere to the feature of least privilege in which emissions and devices are only allowed access to privileges they need to complete their tasks. That is why I wanted to share these tools and solutions for managing access control and the principle of least privilege in IoT.

5.4. Encryption

In this step, you have to decide which data must be encrypted there are personal data for examples names and addresses, and the financial data for example credit card numbers and other type of information that ought to be protected from disclosure to unauthorized parties. Selecting the right algorithm is varying with the actual message to be protected and how secure is required to be (Hassija et al., 2019). One of them is to follow the practice of end-to-end communication encryption where encryption is done at source and decryption at the destination. This is particularly significant in an environment where data is transmitted through an IoT network that may not be secured. Possible tools for using end-to-end encryption include the Transport Layer Security (TLS) and the Datagram Transport

Layer Security (DTLS), which is TLS tailored for situations where information exchange occurs in small portions, for instance in Internet of Things devices Palo Alto Networks (2024). On the other hand, there is a need to use vital encryption keys when it comes to the protection of data. These are pretty straightforward and would be best to use complex passwords and MFA keys as well as to ensure that the keys are as often changed as possible. KMS is one of the tools used in managing encryption keys; some of the cloud services; HSMs-physical tools. These tools make provision of safety deposit for encryption keys and their manipulation more secure.

5.5. Monitor and log activity

Recording activity is a part of a Zero Trust model as it controls and logs all activity in an IoT environment to identify any malicious actions pointing to a security threat Palo Alto Networks (2024). Here are some steps you can take to deploy monitoring and logging activity in your IoT environment:

- Identify the key metrics to monitor: Identify those few things that you care about and want to monitor in your Internet of Things environment. These may include traffic flow within a network, the manner that the device is being used, users and how they conduct themselves, applications among others.
- Choose a monitoring tool: Choose one that can track and analyze all the metrics you will have identified. The five most commonly used monitoring tools for IoT environment are Prometheus, Grafana, Nagios, and Zabbix.
- Define alerting and notification policies: Also, come up with alerting and notification policies that will make notifications to be in place any time a metric reads out of the set acceptable range. This will enable you to close out any possible security breaches as and when they occur.
- Implement logging and auditing: Employ the use of logs and audited or audit friendly systems to track activity in your IoT setting. This means that you will be able to track back security occurrences and take the necessary measures of preventing the next occurrences.
- Use machine learning and AI: Integrate monitoring and logging tools and use machine learning as well as artificial intelligence in reading results. This shall help in the detection of trends and the peculiarities as may be depicted by a security threat.
- They are the following ones: Security Information and Event Management tools is another category of tools that can be used for monitoring and logging in IoT context. SIEM is developed to collect and process any form of data that is relevant to the security infrastructure of an organization such as IoT devices, networks and applications. Most of them depend on artificial intelligence and complex algorithms to identify and address as well dynamic cyber-attacks. These tools provide a common wall where the security staff can access and investigate cases. • Common SIEM tools include IBM QRadar, Splunk Enterprise Security, McAfee Enterprise Security Manager, LogRhythm and other that can flag and record activity in IoT domain. from an organization's IT infrastructure, including IoT devices, networks, and applications. They often leverage machine learning and advanced analytics to detect and respond to real-time security threats. These tools offer a centralized dashboard for security teams to monitor and investigate incidents.
- Some popular SIEM tools include IBM QRadar, Splunk Enterprise Security, McAfee Enterprise Security Manager, LogRhythm, and others that can effectively monitor and log activity in IoT environments.

5.6. Continuous Inspect, Patch Management

Continuous inspection and patch management are some of the crucial activities in the Zero trust model within IoT settings Hassija et al. (2019), and a successful approach thus requires a multifaceted and coordinated approach that involves people, processes, and technology. Here are some steps you can take to implement these measures:

- Inventory your IoT devices: That is why it is crucial to take an inventory of all IoT devices in your environment, including all the devices that were connected to your network such as sensors, cameras, and other smart devices.
- Prioritize devices: Sort them in a way that facilitates the ranking of their threat level to the surrounding. Operations critical or devices with known vulnerabilities should probably be placed in the highest priority list.
- Establish a patch management process: The next thing that needs to be developed is a strategy that allows for quick and effective application of patches and updates on your IoT devices. Some of these best practices may include scheduling patching according to frequency, evaluating patches prior to implementation and tracking metrics of patch management.
- Automate patch management: You may use an automated patch management tool so as to easily apply or fix some patches and updates to the devices. Popular patch management software for IoT settings is IoT Device Management Software some of which include Microsoft Azure IoT Hub, AWS IoT Device Management, and Google Cloud IoT Core.
- Conduct continuous vulnerability scanning: IoT devices should be checked for vulnerabilities and the results used to guide the process of fixing vulnerabilities. For example, for this purpose, you can use Nessus or Qualys for this purpose.
- Implement containerization: Employ Docker or Kubernetes to implement smart application and services of IoT. This approach contributes to the se Michel C. 2006 Isolation of applications and their ability to contain vulnerability or attacks ensures that their harm is limited.
- Monitor device behavior: Whenever there is a change, or suspicious activity from your IoT devices is noticed, it should be reported. Some of the technologies in use include IDS or SIEM technologies to watch devices and be alerted of potential threats.

5.7. Software-defined perimeter or also commonly known as Software Defined Perimeter is a security feature (SDP)

SDP can be defined as an approach of security that establishes a dynamic context of required set and time-bound network security connection for end user resources Gartner (2020). In a conventional network security posture, access control is often governed by a network perimeter and presumed trust levels. Nevertheless, With the increase of using cloud services, working from home, and smart devices, the utilization of the traditional perimeter-centric security model is no longer efficient in guarding important data and assets Alsheikh et al. (2021). To overcome these risks, SDP put into practice the Zero-trust model because the model considers all users and devices as untrusted. It uses strong access control measures in order to only allow certain parties to gain access to certain resources. According to Jewel, SDP works based on the fact that the best way to hide a layer is to make it completely black so no one can see it, just like the cloud around Schloshberg in the movie Dark. This is done using access policies that change their properties by depend on contextual properties such as user identity, device integrity, and location. SDP solutions employ encryption, micro-segmentation and tunneling to create several safe channels between user and resource.

As one of the major benefits of the Software-Defined Perimeter principle can be considered the fact that it differs from VPN which, after the identification of the user or the device, provides him with the possibility to obtain broad network access; in the situation when the SDP provides access only in accordance with the clearly defined role-based permissions and with reference to the context. After a user or device logs on to the SDP controller, the user is only permitted to access certain resources or application where he or she is permitted to access based on his or her role, location, and many other factors. This opens new security features that are more rigorous to enhance the security as compared to the others. Using tools are as follows: some of the tools that can be used to enforce SDP in IoT environment are AppGate SDP, Perimeter 81, Pulse secure, and many more. The above tools offer different functionalities like; Policy-Based Access Control; Multi-factor Authentication (MFA); and Integrations with Identity and Access Management (IAM).

6. RESULTS AND DISCUSSION

Table 1 also presents a revolutionary change in the network security approach. It presents the analysis of the conventional approach to perimeter protection and the zero trust framework solution to address the new safety needs of the IoT infrastructure. Thus, the comparison of these two strategies will provide important information about the framework for distinguishing between and improving the effectiveness of the zero-trust model. The identified issues highlight the necessity of a robust and optimized structure, such as the Zero Trust model, for securing IoT environments. The deployment of the Secure IoT-ZT framework in real-world IoT environments faces several challenges. Resource constraints of IoT devices, such as limited computational power and energy, make implementing robust security measures difficult. Integration complexity arises from the heterogeneous nature of IoT devices and communication protocols, while scalability and interoperability with legacy systems add further complications. User compliance with strict authentication protocols and the financial costs of infrastructure upgrades and training also present barriers. Additionally, adapting to an evolving threat landscape requires continuous updates and monitoring, which may strain existing resources. Addressing these challenges through lightweight cryptographic algorithms, automated policy enforcement, and enhanced user training could improve the framework's practical applicability.

6.1. Evaluation of Secure IoT-ZT framework

In protecting IoT environments there has been discussed several models that can address the IoT's dynamic security threats in relation to privacy, trust, and data security. There are two models that have received interest; the ones tied to block chain technology and the model that was developed together with the framework of the Palo Alto securities. In the following we propose, the Secure IoT-ZT framework tailored to protect IoT devices with a Zero trust model. We hope that our work will be possible to compare with these models with regards to such factors as complexity, scalability, energy consumption and other factors that are considered relevant in the field. Through this comparison, the pros and cons of each approach shall be discussed, and Secure IoT-ZT major strengths in enabling security requirements of IoT environments exposed. The findings aim to guide organizations and researchers in designing effective security solutions for IoT contexts.

6.2. Scenario-based Evaluation of Secure IoT-ZT Framework in a Smart Healthcare System

The risks are not limited because the contemporary hospital environment is rather diverse, and IoT invention contributes to the patient's treatment through many devices, including monitors, pumps, wearables, etc. These challenges are not limited to protecting patients' information but also to provide and maintain dependability and serviceability of virtually any IoT devices. In-patient monitors and treatment critical, require a reliable and dynamic security structure.

Table 1. Comparison between the Traditional perimeter-based architecture and the Secure IoT-ZT framework.

IoT security requirements	Traditional perimeter-based architecture	Secure IoT-ZT framework solution						
		Identity assets	Monitor & log activity	Continues inspection & patch management	Access control (least privilege)	Network segmentation	Encryption	SDP
Confidentiality	Lack of end-to-end encryption for data.				√	√	√	√
Integrity	Lack of granular control.		√	√	√	√	√	√
Availability	It does not provide sufficient protection because it relies on the assumption that all devices within a network are trustworthy and secure.		√	√				
Authentication	Determined by network location or IP address (This would be spoofed or compromised).	√			√	√		√
Authorization	Relies heavily on network-level access control.	√			√	√		√
Accountability	Lacks fine-grained control and insight into the activities and behavior of devices on the network.	√	√	√	√	√		√
Non-Repudiation	It requires the use of digital signatures and secure communication protocols, which are not supported by traditional methods.	√	√	√	√	√	√	√
Resilience	A single point of failure, which reduces the network's resilience to attacks.					√		√
Scalability	Focus on securing the perimeter, which becomes a bottleneck.					√		√

6.2.1. Strong Authentication

- MFA and SSO: In this case the framework applies MFA and SSO at each point of access of the hospital's network. This strong layer of safety helps to guarantee that every interaction made with the IoT structure is authenticated and constant.
- Scenario Application: For example, before a nurse or a doctor can view patients' records or manage connected devices, he or she must enter an identification number – an employee code – together with a second form of verification – perhaps fingerprint recognition or a safe mobile application. Such a two-factor approach minimizes the possibility of illegitimate entry into the system.

6.2.2. Zero Trust Core Components

- Policy Engines: These engines are the dynamic core of the entire Secure IoT-ZT framework as they are constantly performing the access validation. They evaluate every application and make conscious decisions based on the constantly evolving threat profile.
- Scenario Application: Suppose a doctor has to control patient monitors but is unable to reach the monitoring room. This request is well understood by the policy engine, which applies the latest security policies to scrutinize it and ensure that the doctor who is asking for the access has every right to do so.

6.2.3. Traffic Filtering and Segmentation

- Network Segmentation: In this context critical IoT devices are placed in specific segments of the network depending on their importance and function. This segmentation is very important in reducing chances of large-scale network losses.
- Scenario Application: A practical example is the continued practice of dividing the infusion pumps into a different network domain altogether. This means that only certain authorized medical personnel only have access to these sensitive devices which greatly reduce the vulnerability of one network getting infected with the virus from the other.

6.2.4. Continuous Monitoring and Logging

- Real-time Monitoring: Being an integrated part of Secure IoT-ZT this proves the monitoring and the login of all the activities taken in the network. This is critical to improve the chance of an early identification of an insecure state or condition.
- Scenario Application: For instance, a log in attempt at odd hours of the day is flagged off as a special pattern. It is faster to have a quick assessment of a situation, something that may help prevent a security threat.

6.2.5. Benefits in the Scenario

- The main benefits stem from the development of the Secure IoT-ZT framework in an IoT setting of a hospital. Patient's data privacy is as well enhanced since access to patient information is made stricter by applying methods like TLS (Transport Layer Security) and AES (Advanced Encryption Standard), which are fundamental ingredients of current data security programs, on the data integrity of patient's information. A lot of benefits come from l's IoT environment; IoT devices' security is significantly improved. More detailed patient information security can be obtained by using authorized access to electronic medical records, and uses security measures of TLS and AES for data encryption.

- The security of IoT devices is significantly improved. The framework ensures regular firmware updates and incorporates advanced anomaly detection mechanisms. This proactive approach is essential in identifying and mitigating potential device tampering or malfunctions.
- Compliance with healthcare regulations such as HIPAA is meticulously addressed. The framework facilitates comprehensive audit trails and logging protocols that facilitate compliance reporting and ensure regulatory adherence.
- Policy engines form the framework's backbone, incessantly validating access requests. These engines use protocols like XACML (<span aria-drop level="2″ class=" G.
- The following modern security access engines use or enhance protocols like XACML, to assess risks and context in decisions: For example, the ability of a doctor to access patient monitors remotely goes through thorough check against the current applicable policies and credential enabled by these protocols.
- Network Security: VLAN & MPLS are used for Network segmentation. Standardized data security features like TLS and AES (Advanced Encryption Standard) which are to meet the goal of protecting patient's data confidentiality and data integrity.
- Continuous monitoring and logging are mentioned as key components of the framework; the protocols used for network activity are Syslog and SNMP's framework emphasizes Continuous Monitoring and Logging, leveraging protocols such as Syslog and SNMP (Simple Network Management Protocol) for real-time network activity tracking. Abnormality, such as the above login patterns, are immediately recognized and call for alarms raising, leading to inquiries.

Therefore, it can be suggested that the Secure IoT-ZT framework is a major evolution on the way to guarantee the security of healthcare IoT systems. With comprehensive, continuous and context-sensitive security management to the mix, the solution is more resilient and flexible compared to traditional security paradigms. The fact that it works in a highly important and, at the same time, vulnerable hospital environment proves that it can be a rather powerful tool in combating IoT threat actors for all healthcare and other essential industries.

7. CONCLUSION

In the context of this paper, securing IoT devices with the creation of a Zero trust framework known as Secure IoT-ZT has been considered. The first step in the journey involved the introduction to the subject under consideration, the problem statement and the aim and objectives of the study. The following sections gave the reader a clear appreciation of IoT as it encompassed the definition, characteristics, architecture, security needs, threat and attack prospective. With this IoT groundwork laid, the paper extended the discussion on Zero Trust, sharing its architectural frameworks established by NIST, Gartner, CISA, and Palo Alto. These frameworks laid the foundation for beginning to prosecute a security paradigm shift, which overcame the conceptual deficiencies of a perimeter security model. The main focus of this paper is to design and explain the Secure IoT-ZT framework that includes multiple features essential for IoT devices' safeguarding. The components are; subject, Strong Authentication mechanisms (SSO, MFA, Adaptive Access), Zero trust Core Components (Policy Engine, PDP, PEP), SDP, Traffic Filtering n Segmentation, Resources, and Continuous Monitoring and logging. The presented Secure IoT-ZT framework provides an in-depth and manifold solution to mitigate the threats IoT faces and avoid unauthorized invasions and leakage of information. After the analysis, the proposed Secure IoT-ZT model has been compared with the traditional security approach based on the perimeters, as well as other existing models of the security architecture, and those based on block chain and the approaches derived from the Palo Alto model. The evaluation was more inclined towards basic characteristics that were Energy Consumption, Advanced Hardware Requirement, Scalability and Complexity. The analysis showed that the Secure IoT-ZT framework provides the highest indices on all measures highlighted, which points to the efficiency and adaptation of this model for protection IoT environments. Therefore, this paper has highlighted on the relevance of Zero trust architecture in maintaining the security of IoT devices. Creating the Secure IoT-ZT framework has provided a foundation for improving the different modifications that IoT systems require in terms of security. To build the first circle of trust the organizations need to adopt Zero trust norms; they should improve the ways of identity verification; they have to apply strict access controls, analyze all the IoT activities, and log them for security purposes.

References

Ahmad, M., Younis, T., Habib, M.A., Ashraf, R., & Ahmed, S.H. (2019). A Review of Current Security Issues in Internet of Things. In Recent Trends and Advances in Wireless and IoT-enabled Networks. Springer. https://doi.org/10.1007/978-3-030-11292-0_2

Alaba, F.A., Othman, M., Hashem, I.A.T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Ashraf, U., Al-Naeem, M., Bhutta, M. N. M., & Yuen, C. (2024). ZFort: A scalable zero-trust approach for trust management and traffic engineering in SDN based IoTs. Internet of Things, 28, 101419.

Alsheikh, M. A., Abdalla, S. M., Abdalla, S. M., Abdou, A. M., & Ali, A. M. (2021). Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A State-of-The-Art Review. IEEE Access, 9, 16517-16531. https://doi.org/10.1109/ACCESS.2021.3058351

Asiri, S. A. (2018). A Blockchain-Based IoT Trust Model [Master's thesis, Ryerson University]. Toronto, ON, Canada.

Atwal, R. P., & Chauhan, S. (2021). Zero Trust Network Architecture: A Survey. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). https://doi.org/10.1109/CCWC51732.2021.9375994

Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. Internet of Things, 27, 101227.

Cisco. (2014). Cisco ACI security: A new approach to secure the next-generation data center.

Cisco. (2014). Cisco Application Policy Infrastructure Controller data center policy model.

Cybersecurity and Infrastructure Security Agency (CISA). (2020). Zero Trust Maturity Model. https://www.cisa.gov/publication/zero-trust-maturity-model

Embrey, B. (2020). The top three factors driving zero trust adoption. Computer Fraud & Security, 2020(9), 13-15. https://doi.org/10.1016/S1361-3723(20)30076-7

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the Internet of Things. IEEE Access, 6, 3279–33001. https://doi.org/10.1109/ACCESS.2018.2870644

Gartner. (2020). Zero trust architecture and solutions. Qi An Xin Group. https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-in-1-1OKONUN2.pdf

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). Security and Privacy Issues in Internet of Things (IoT): A Review. In 2019 International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1289-1294). IEEE. https://doi.org/10.1109/ICICCS.2019.8722912

Jerald, A.V., Rabara, S.A., & Bai, D.P. (2016). Secure IoT architecture for integrated innovative services environment. In Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). Palladam, India.

Khan, R., Khan, S.U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology. Islamabad, India. https://doi.org/10.1109/FIT.2012.53

Kindervag, J. (2010). No more chewy centers: Introducing the zero trust model of information security (pp. 1–15).

Ko, E., Kim, T., & Kim, H. (2017). Management platform of threats information in IoT environment. Journal of Ambient Intelligence and Humanized Computing, 9(4), 1167–1176. https://doi.org/10.1007/s12652-017-0550-6

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: A security point of view. Internet Research, 26(2), 337–359. https://doi.org/10.1108/IntR-07-2014-0178

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. Information, 7(3), 44. https://doi.org/10.3390/info7030044

Lo, S. K., et al. (2019). Analysis of Blockchain Solutions for IoT: A Systematic Literature Review. IEEE Access, 7, 58822-58835. https://doi.org/10.1109/ACCESS.2019.2912200

Mehraj, S., & Banday, T. M. (2020). Establishing a Zero Trust Strategy in Cloud Computing Environment. In 2020 International Conference on Computer Communication and Informatics (ICCCI). Coimbatore, India. https://doi.org/10.1109/ICCCI48352.2020.9104111

National Institute of Standards and Technology. (2013, April). Developing a framework to improve critical infrastructure cybersecurity. Forrester Group.

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security Requirements for the Internet of Things: A Systematic Approach. Sensors, 20(20), 5897. https://doi.org/10.3390/s20205897

Palo Alto Networks. (n.d.). The Right Approach to Zero Trust for IoT Devices. Retrieved from https://www.paloaltonetworks.com/resources/whitepapers/the-right-approach-to-zero-trust-for-iot-devices

Radanliev, P., De Roure, D., Page, K., Nurse, J.R., Mantilla Montalvo, R., Santos, O., & Maddox, L. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial Internet of things and industry 4.0 supply chains. Cybersecurity, 3(1), 1–21. https://doi.org/10.1186/s42400-020-00052-6

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 20). Zero trust architecture. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Rose, S., et al. (2020). Zero trust architecture. National Institute of Standards and Technology. Draft (2nd) NIST SP 800-207.

Sfar, A.R., Natalizio, E., Challal, Y., & Chtourou, Z. (2017). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118–137. https://doi.org/10.1016/j.dcan.2017.09.001

Siegel, J.E., Erb, D.C., & Sarma, S.E. (2018). A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, and Development Areas. IEEE Transactions on Intelligent Transportation Systems, 19(8), 2391–2406. https://doi.org/10.1109/TITS.2017.2778749

Sood, D., Sood, S., & Dhurandher, S. K. (2020). Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A State-of-The-Art Review. In 2020 12th International Conference on Communication Systems & Networks (COMSNETS). Bangalore, India. https://doi.org/10.1109/COMSNETS48256.2020.9027395

Tan, L., & Wang, N. (2010). Future Internet: The Internet of Things. In 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu, China.

The Open Group. (n.d.). Retrieved from https://publications.opengroup.org/c166

Tourani, R., Misra, S., Mick, T., & Panwar, G. (2017). Security, Privacy, and Access Control in Information-Centric Networking: A Survey. IEEE Communications Surveys & Tutorials, 20(4), 566–600. https://doi.org/10.1109/COMST.2017.2749501

Townsend, K. (2015, March 11). Don't implement zero-trust security in a virtualized network without reading this overview. TechRepublic. https://www.techrepublic.com

U.S. Presidential Executive Order. (2013, February 12). Improving critical infrastructure cybersecurity.

Whitmore, A., Agarwal, A., & Xu, L. D. (2015). The Internet of Things—A survey of topics and trends. Information Systems Frontiers, 17(2). https://doi.org/10.1007/s10796-014-9489-2

Xiangshuai, Y., & Huijuan, W. (2020). Survey on Zero-Trust Network Security. In Artificial Intelligence and Security. ICAIS 2020. Communications in Computer and Information Science. Singapore.

Yang, J., & Fang, B. (2011). Security model and key technologies for the Internet of Things. Journal of China University of Posts and Telecommunications, 18(2), 109–112. https://doi.org/10.1016/S1005-8885(10)60022-3

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of Things. IEEE Internet Things Journal, 4(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2703172

Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's INTRAnet of things to a future INTERnet of things: A wireless- and mobility-related view. IEEE Wireless Communications, 17(6), 44–51. https://doi.org/10.1109/MWC.2010.5675776