A Review on Zero Trust for Implementing Authentication and Access Security in IoT

JAN EDGAR E. TUPAS

Mapua University School of Information Technology, jeetupas@mymail.mapua.edu.ph

MIGUEL T. SONIEL

Mapua University School of Information Technology, mtsoniel@mymail.mapua.edu.ph

CHRISTIAN HENRY MIGUEL E. CARUZ

Mapua University School of Information Technology, chmecaruz@mymail.mapua.edu.ph

Abstract

The rapid escalation of the Internet of Things (IoT) has brought various unprecedented security challenges, necessitating robust authentication and access control measures. This review explores the critical role of Zero Trust (ZT) in strengthening IoT authentication and access security. By examining recent advancements in ZT-based frameworks, protocols, and access controls, this paper emphasizes the significance of continuous monitoring, behavior analysis, and attribute-based encryption in safeguarding interconnected IoT systems' integrity, confidentiality, and resilience. Furthermore, these frameworks, protocols, and access controls allow data within IoT systems to be secured by implementing real-time network security, fine-grained access control, and continuous authentication in the architecture. The review also highlights the integration of ZT in different access control approaches, offering a comprehensive defense mechanism against malicious attacks. Through an analysis of ZT's potency in addressing IoT security challenges, this review provides valuable insights into evolving the environment of IoT authentication and access security, preparing for cutting-edge solutions to safeguard IoT systems.

Additional Keywords and Phrases: IoT, Zero Trust, Authentication Security, Authentication Protocol, Access Control

1 INTRODUCTION

1.1 Introduction

The rapid expansion of digitalization all around the world remains prevalent in contemporary times. There is immense effort focused on innovation and creating novel technologies necessary for the advancement and improvement of human lives, advancing and improving existing technologies, and formulating technological solutions to numerous existing problems that humans continuously face. These developments in technology and digitalization are the fuel that drives technological economies worldwide. In the Philippines, the Internet economy alone was estimated to be valued at USD 7.5 billion in 2020 with an expected increase of 30 percent for each of the following years [16]. Among these technological developments is the rapid expansion and adoption of the Internet of Things (IoT) which is a network of interconnected devices that share data. As IoT develops in the Philippines, some business sectors are utilizing it to run their operations more profitably and productively [14]. Large-scale communication is utilized in IoT environments which in turn demands fool-proof security. Any IoT entity handling data could potentially be the source of a security breach that jeopardizes human lives or compromises the resources of the entity, rendering them unavailable [8]. The effective authentication of IoT devices must be prioritized to prevent security threats especially with perimeter-based security. Here, all entities located in the internal network are trusted while those in the external network can only be trusted after successful authentication [13]. Identifying and utilizing effective security methods and technologies for IoT is necessary to ensure the security of all shared information, and the protection of humans that utilize these devices. The Zero Trust (ZT) security model was introduced to address the limitations of perimeter-based security. ZT characterizes cybersecurity solutions that prioritized assessing trust for each transaction rather than relying solely on implicit trust based on network location [17]. It posits the presence of a potential threat within the system and that an enterprise's environment should not be trusted similar to any third-party environment [4]. Authentication and access control are the fundamental ideas behind achieving ZTA [12]. Zero-trust authentication solutions can monitor and evaluate all authentication attempts where each request for access to resources needs to be reauthenticated and reauthorized, preventing potential unauthorized access to resources [6]. With the continuous development of ZT based technologies and solutions, implementing proper authentication schemes and access controls based on ZTA holds the potential in safeguarding security vulnerabilities in IoT.

The objective of this study is to review recent literature associated with the development of ZT-based technology for enforcing and improving IoT authentication and access security. The specific objectives of the study are the following:

1. To define and discuss IoT and IoT security issues based on existing literature.

2. To define and discuss ZT and ZTA based on existing literature.

3. To review and discuss recent advancements in ZT-based IoT authentication and access security measures.

The scope of the study encompasses IoT, security in IoT, issues in IoT security. It also includes ZT and ZTA, the ZT framework and its core components. The study also discusses the recent advancements in ZT-based frameworks, authentication protocols and access controls for enforcing IoT authentication and access security based on literature.

1.2 Relevance

IoT connections continue to surge in the current digital age. A report from IoT Analytics indicate a 16% growth of IoT connected devices in 2023 translating to 16.7 billion endpoints [18]. In the Philippines, smart cities are being developed such as the New Manila Bay – City of Pearl and the New Clark City which aim to be self-sufficient and include smart transportation and buildings [14]. The significance of IoT in the present digital age and the security concerns that revolve around IoT underscore the critical need for robust and innovative solutions to ensure the integrity, confidentiality, and resilience of interconnected systems and prevent attacks that threaten the safety of all. On par with the growth of IoT is the rising popularity of ZT. In a report from Okta, 61% of surveyed organizations have implemented ZT initiatives in 2023 and 35% plan to adopt ZT in the near future [19]. In securing IoT, authentication is the primary defender that ensures no threat actors or malicious activity breaches the IoT environment. With the integration of ZT, numerous researches are continuously published in current times proposing methods, strategies, frameworks, and protocols for ZT-based authorization and access control in IoT.

1.3 Research

The literature review conducted is centered on the implementations of ZT and ZTA on ensuring authentication and access security in the IoT. The of the review is to describe the current advancements of ZT for authentication and access security in IoT and provide an analysis on the reviewed works. The structure of the review begins with an overview of IoT, the security approaches in IoT, and the challenges and vulnerabilities in IoT security. The review then details ZT and ZTA as described by NIST. Recent researches on ZT-based authentication and access controls will be reviewed.

2 DISCUSSION

2.1 Internet of Things

IoT is referred to as a network of interconnected devices that share information with each other. Dissecting the term "Internet of Things" results in the first word "Internet" which is a system of interconnected networks, and "Things" which in this context refers to smart devices. IoT smart devices are embedded with technologies, such as sensors, that allow them to acknowledge, connect, and transfer data with other devices. IoT devices deliver services without requiring manual assistance and the application of IoT spans from smart homes to smart cities and factories [15]. Various organizations and research groups propose definitions for IoT. For the Institute of Electrical and Electronic Engineers, IoT is a "collection of items with sensors that form a network connected to the Internet" [20]. According to International Telecommunication Union (ITU), IoT is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" [21]. The Electrotechnical Commission (IEC) define IoT as "An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react" [22]. According to the National Institute of Standards and Technology (NIST), IoT is "The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information" [23].

The common characteristics that the mentioned organizations specify regarding IoT are the following: IoT is an infrastructure meaning it is made up of hardware and software components; IoT manifests interconnectedness among devices and objects; IoT embodies the processing and sharing of information, reaction, and interaction. Therefore, IoT can be defined as an infrastructure of interconnected objects that process and share information and as a result enables objects to interact with each other and enable services that contribute to human life. Figure 1 shows the basic building blocks of IoT [29]. Sensors are the gadgets that collect and give out information. Information is sent to the processors which handle and refine them. Then the information is sent to respective areas through the gateways. The information is properly utilized in applications that are controlled by clients for specific purposes.

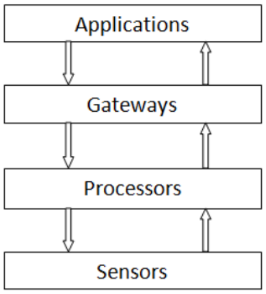

Figure 1: Basic Building Blocks of IoT. Diagram by Kumal, via Researchgate (https://www.researchgate.net/publication/345154367)

2.2 IoT Security Issues

In an IoT infrastructure, components are secured by implementing measures that meet the requirements of the CIA triad, namely confidentiality, integrity, and availability. According to the authors of [25], achieving the CIA triad in an IoT environment requires the implementation of verification, authorization, and encryption. Verification and authorization measures must be strong and of high quality to prevent malicious actors from compromising IoT systems. Advancing and implementing verification and authorization strategies is critical to counter the advancing tools and methods used by threat actors. Currently there is a variety of techniques used for user authentication. The common user authentication techniques used are identified in [26] and encompass the following: One Time Password Authentication, ECC-Based Mutual Authentication, ID and Password-based Authentication, Certificate-Based Authentication, and Blockchain. In [15], device authentication techniques were segmented into User-Gateway-Device approach, User-Device-Gateway approach, Device-to-Device approach, and Chaotic-map approach. User authentication techniques follow perimeter-based security, allowing authenticated users to operate freely, with no additional authentication procedures to identify or prevent threat actors who may exploit vulnerabilities through lateral movement. This weakness is prone to exploitation from threat actors.

The IoT architecture describes how IoT components are arranged, communicated, interact, and function together. It is essential in guaranteeing the smooth and disruption-free overall flow of data, communication, and functionality. IoT architectures are made up of layers that have unique functions necessary for the overall operation of the IoT system. Figure 2 shows the layered architectures of IoT [30]. Security vulnerabilities exist within each IoT architecture layer are usually exploited by threat actors to gain access to resources such as sensitive data. The common layers and attacks are shown in Table 1 [24][30].

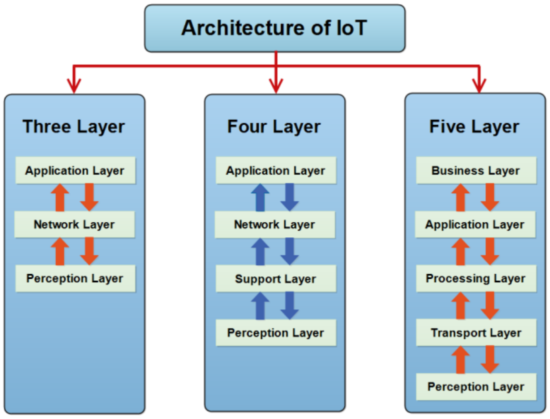

Figure 2: IoT Architectures. Diagram by Burhan et al., via MDPI (https://doi.org/10.3390/s18092796)

Table 1: Attacks on IoT Architecture Layers

IoT Architecture Layer	Common Attacks
Perception Layer	Jamming, Tampering, Collision, Exhaustion, Relay Attacks, Eavesdropping, Node Capture, Fake Node, Replay Attack, And Timing Attack, Spoofing
Network Layer	Denial-Of-Service (DoS), Distributed Denial-Of-Service (DDoS) Attacks, Spoofing Attack, IoT Botnet, Man-In-The-Middle (MITM) Attack, Storage Attack, Exploit Attack, Malicious Code Injection, Sinkhole Attack, Sybil Attack, Denial of Sleep Attack
Application Layer	Cross Site Scripting, Malicious Code Attack, Sniffing Attack, Spear-Phishing Attack
Support Layer	Dos Attack, Malicious Insider Attack
Processing Layer	Exhaustion, Malware
Business Layer	Business Logic Attack, Zero-Day Attack

2.3 Zero Trust

The term zero trust was first used by John Kindervag and was used to characterize solutions that assessed trust per transaction rather than relying on implicit trust based on network location [17]. ZT moves away from perimeter-based security and is based on the premise that "trust is never granted but must be continually evaluated". NIST [17] specifies the difference between ZT and Zero Trust Architecture (ZTA). ZT offers a range of notions aimed at reducing uncertainty in the enforcement of precise and least privilege per-request access decisions in information systems. ZT prioritizes authentication, authorization, and minimizing trust zones. ZTA is a ZT-based plan specified and implemented by an enterprise. Both ZT and ZTA focus on resource access where only authorized entities can utilize resources but with least privilege. Authentication and access control determine a user's identity and grant them the necessary privileges to perform various operations on protected resources [12]. Authentication is the procedure or action of confirming a user's or process's identity. Access control is a security method that controls what or who is allowed to access or use resources in a computer environment. ZT authenticates users and devices, restricts access and permissions, and is adaptive in terms of setting context-based policies [13].

The conceptual framework model of ZTA according to NIST [17] is shown in Figure 3. A subject uses the system to attempt to access a resource. The model shows how components of a ZTA interact with each other. The untrusted subject undergoes authentication and is managed by the Policy Enforcement Point (PEP). The PEP communicates with the Policy Decision Point (PDP) which includes the Policy Engine (PE) and Policy Administrator (PA) to determine what action will be done. Information from multiple local and external data sources are used to conduct access decisions. Access to the resource is granted once the subject is verified as trustable but will continuously be monitored throughout the session. The PE, PA and PEP are the three core logical components of ZTA and are shown in Figure 4. Granting resource access to an entity is decided by the PE. Here a trust algorithm that is fed with external input determines whether access to a resource is allowed, rejected, or terminated. It enforces access policies based on dynamic contextual information. The PA closely works with the PE in creating or ending the subject and resource transmission. It enforces access policies based on dynamic contextual information. A subject is granted access to a resource via the credential provided by the PA. When a subject is authenticated or untrusted, the PA signals the PEP to start or end the transmission. The PEP starts, monitors, and ends the transmission between the subject and resource. It enforces the policies at various points within the network.

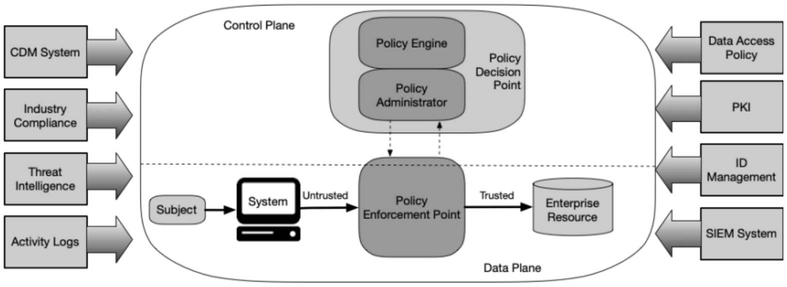

Figure 3: ZT Conceptual Framework Model. Diagram by NIST, via NIST (https://doi.org/10.6028/NIST.SP.800-207)

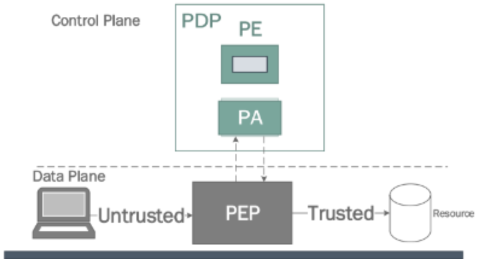

Figure 4: Core Logical Components of ZT. Diagram by NIST, via NIST (https://doi.org/10.6028/NIST.SP.800-207)

2.4 Review on Zero Trust Authentication and Access Control for IoT

The characteristics of IoT make ZT an appropriate solution for generating IoT systems [4]. IoT devices are diverse in terms of size, functionality, and communication protocols. They may operate in various physical locations and expand quickly. Threat actors have multiple points they exploit to breach the ecosystem which means extensive monitoring of all devices is needed. ZT seeks to improve the security posture of IoT networks through strict authentication and monitoring. Table 1 shows an overview of the reviewed literature. ZT authentication models, frameworks and protocols are discussed in this section.

Table 2: Overview of Related Literature

Ref	Authors	Year	Title	Contribution
[1]	Dimitrakos et al.	2020	Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things	Trust-aware continuous authorization model that applies ZTA to consumer IoT environments
[2]	Chen et al.	2021	A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture	ZTA-based four-dimensional security framework for 5G intelligent medical systems.
[3]	Shah et al.	2021	LCDA: Lightweight Continuous Device-to-Device Authentication for a Zero Trust Architecture (ZTA)	Device-to-device authentication protocol that depends on a dynamic function to guarantee continuous authentication and CSI for frequent key updates
[4]	Ameer et al.	2022	BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems	ZT authorization policy model design using the ZT authorization requirements framework (ZT-ARF)
[5]	Ge and Zhu	2022	GAZETA: GAme-Theoretic ZEro-Trust Authentication for Defense Against Lateral Movement in 5G IoT Networks	GAZETA, A formal zero-trust security framework based on Markov games
[6]	Alshomrani and Li	2022	PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol	Device continuous authentication in the Internet of Things ecosystem using a physical unclonable function (PUFDCA)
[7]	Garcia-Tedoro et al.	2022	A Novel Zero-Trust Network Access Control Scheme based on the Security Profile of Devices and Users	Security Attribute-based Dynamic Access Control (SADAC)
[8]	Awan et al.	2023	A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT	Zero-Trust and ABAC for IoT using Blockchain (ZAIB)
[9]	Ali et al.	2021	Uplifting Healthcare Cyber Resilience with a Multi-access Edge Computing Zero-Trust Security Model	ZT-based multi-layered security model to confirm the credentials of User Equipment (UE)
[10]	Yao et al.	2020	Dynamic Access Control and Authorization System based on Zero-trust architecture	ZT-based dynamic and fine-grained access control and authorization system model
[11]	Tian et al.	2022	A Terminal Security Authentication Protocol for Zero-Trust Satellite IoT	ZT authentication protocol for S-IoT terminal security
[27]	Ejiyeh	2023	Real-Time Lightweight Cloud-Based Access Control for Wearable IoT Devices: A Zero Trust Protocol	ZT real-time lightweight data access control protocol for cloud-centric IoT sensor networks
[28]	Huang et al.	2023	ZT-Access: Combining Zero Trust Access Control with Attribute-based Encryption Scheme against Compromised Devices in Power IoT Environments	ZT access control and attribute-based encryption scheme against compromised devices in Power IoT environments

An architecture for trust aware continuous authorization based on ZT is proposed in [1] by by Dimitrakos et al. in 2020. The architecture builds on an Attribute-Based Access Control (ABAC) foundation, utilizing attribute abstraction and extensibility to handle resource heterogeneity. In 2021, Chen et al. [2] proposed a four-dimensional security framework using Zero Trust Architecture (ZTA) for 5G smart medical systems. Subjects request access and have varying trust levels computed in real-time from diverse sources. Objects have security levels computed based on their own value, environment, and real-time threats. Environment considers situational security during access requests, adapting trust levels based on changing environments. Behavior involves real-time security analysis and evaluation. This framework serves as the basis for a ZT security awareness and protection system for 5G smart healthcare through continuous authentication and dynamic trust evaluation. A novel lightweight continuous authentication protocol for securing device-to-device communication is proposed in [3] by Shah et al. in 20201. The protocol uses a dynamic secret key refreshment mechanism involving modification to channel state information (CSI). A ZT-based authorization requirements framework (ZT-ARF) for IoT smart systems is presented in [4] by Ameer et al. in 2022. The framework focuses on score-based authorization and is composed of the following: actors, sessions, context states, targets, actions, action-target, predefined policies authorization engine, score engine, score calculation, threshold calculation, access decision enforcement engine (ADE). In 2022, Ge and Zhu [5] proposed GAZETA, a ZT framework based on Markov games. A strategic PE is designed to prevent lateral movement and Bayesian updates are used for trust evaluation. A quantitative trust evaluation mechanism continuously updates the trust score based on observations using dynamic Bayesian updates with multiple footprint analyses. A continuous authentication protocol based on physical unclonable function is proposed in [6] by Alshomrani and Li in 2022 for device authentication in an IoT ecosystem. The physical unclonable function-based device continuous authentication (PUFDCA) utilizes ZT static authentication, where the identity of an IoT device is verified and only allows access per session, and continuous authentication. In 2021, Ali et al. [9] proposed a ZT security model that provides security using continuous validation of user equipment (UE). The model utilizes a lightweight authentication algorithm that ensures the continuous validation of UE credentials. Identity and location are the two credentials that are utilized during the authentication process. The suggested model reduces cyber risks related to the increasingly complex threat environment. A security authentication protocol for Satellite-IoT terminals is proposed in [11] by Tian et al. in 2022. The protocol addresses security objectives, which are fundamental to ZTA and include unforgeability, data integrity, data confidentiality, resistance to replay attacks, and forward security. A ZT real-time lightweight access control protocol is proposed in [27] by Ejiyeh in 2023. The protocol is used for cloud-centric dynamic IoT sensor networks. The protocol uses a ZT approach as trustworthiness is evaluated using a criterion-based access control and multi-dimensional score-based approach. In 2023, Huang et al. [28] proposed a zero-trust access control which is an attribute-based encryption scheme referred as ZT-Access. The model integrates zero trust access control with attribute-based encryption with the intent of continuously monitoring and analyzing the access entities of behavior. In 2020 Yao et al. [10] proposed a ZT dynamic access control that establishes a dynamic control system which aims to authenticate continuously based on the identity of the object and the access subject. The model used for the proposed access control is a Trust-Based Access Control (TBAC) model for dynamic and fine-grained access control. A zero-trust network access control that is based on the devices and users' security profile is proposed in [7] by Garcia-Teodoro et al. in 2022. Security Attribute-based Dynamic Access Control (SADAC) accumulates variety of security-related attributes regarding communications, installed applications, consumption of resources and protection mechanism of the device. A blockchain-inspired and attribute based zero-trust access control model for IoT is proposed in [8] by Awan et al. in 2023. The model is blockchain-inspired providing decentralized mechanism for storing and sharing data, hence the proposal of the model called Zero-Trust and ABAC for IoT using Blockchain (ZAIB).

2.5 Analysis of Reviewed Frameworks

ZT follows basic tenets that must be implemented in ZTA. The tenets should be the basis for creating and enforcing a ZT strategy. The four-dimensional framework [2] is based on ZTA for IoT smart healthcare. The dimensions include Subject, Object, Environment, and Behavior. Each dimension is essential for ensuring ZT security. The framework enables real-time assessment of security and trust levels through continuous monitoring and behavior analysis which makes the framework an effective blueprint for implementing ZT in IoT systems. It also allows for fine-grained control of access behavior, meaning it can precisely control access to resources based on attributes. The framework also evaluates trustworthiness based on multiple inputs which enhance the reliability of trust assessment and overall security. The benefits of the framework to IoT systems include identity verification, adaptive access control, dynamic authorization, enhanced security, and behavioral monitoring. These features all help to maintain the overall security and integrity of IoT devices in the healthcare setting and can be used as a basis for implementing ZT in other IoT settings. Another ZT-based framework, ZT-ARF [4] is designed to provide ZT-based authorization requirements. The components of the framework include Actor Characteristics, Target Characteristics, Action Characteristics, Action-Target Characteristics, Context Characteristics, Usage Check, and Behavioral Check, which are more specific compared to four-dimensional framework in [2]. It also promotes a score-based authorization for computing trust scores among access subjects, enhancing security through ZT. The framework goes in depth by mapping the requirements with the ZT basic tenets. The framework in IoT can be used as a basis for developing ZTA for IoT. The GAZETA framework for IoT networks [5] focuses on authentication defense against lateral movement using ZT. Dynamic trust updates using Bayesian correction and authentication policies are used by GAZETA. In assessing the framework, GAZETA provides a reliable trust evaluation that adapts to a changing environment which is essential for implementing security in IoT since a slight change in environment can already signify malicious activity. This framework can be expanded and applied to other ZT strategies for IoT defense. Table 3 shows an overview of the frameworks.

Table 3: Overview of Frameworks

Ref	Framework	Components	ZT Features	Environment
[2]	Four-Dimensional Framework	Subject, Object, Environment, Behavior	Identity verification, real-time security and trust assessment, continuous monitoring, dynamic authorization, fine-grained access control	5G Smart Healthcare
[4]	ZT-ARF	Actor Characteristics, Target Characteristics, Action Characteristics, Action-Target Characteristics, Context Characteristics, Usage Check, and Behavioral Check	Dynamic and fine-grained authorization, suitable for constrained smart devices, formal policy definition, scalability, privacy-preserving, continuous and score-based authorization	IoT Enabled Smart Systems
[5]	GAZETA	Defender, Agent	Dynamic trust update and evaluation, strategic authentication policies, constant monitoring, lateral movement mitigation	5G IoT Networks

2.6 Analysis of Reviewed Protocols

ZT focuses on robust authentication because when users or devices are given access to resources, authentication continues using trust evaluation based on contexts and behavior. This can safe guarded IoT from malicious users and devices because gaining initial access is already hardened from the robustness of ZT protocols, and if they do gain access, they are constantly being monitored and can be removed from the system immediately. The recent ZT protocols proposed for authentication and access security are proven to exhibit security properties and resistance to security attacks as shown in table 2. Based on the review, the LCDA protocol [3] resist the most types of attacks. Although the use of it in an IoT environment is not discussed, the protocol focuses on device-to-device authentication which could be implemented for IoT. The PUFDCA protocol [6] secures IoT devices by leveraging static and continuous authentication. PUF technology provides unique and unclonable identifiers for each device. The protocol successfully resists attacks, and is lightweight and can be used for low-energy IoT. However, the protocol relies on location for continuous authentication which might pose as a vulnerability. Another protocol for S-IoT [11] authenticates smart devices in an S-IoT environment and also uses PUF technology to enhance security. The protocol uses cryptographic primitives for bidirectional authentication, implements continuous authentication, and is proven to resists replay attacks. However, the protocol is yet to be used for other IoT environments. The lightweight cloud-based protocol for IoT sensors [27] implements ZT by continuously verifying the trustworthiness of subjects. The protocol ensures high availability and scalability which is appropriate for IoT systems as they constantly tend to increase. However, the protocol is cloud-based and may result in latency which affect real-time access. The protocol was also evaluated in a simulated environment and is yet to be tested in a real-world scenario. The ZT-Access protocol [28] uses a zero-trust access control and attribute-based encryption to secure data. It enforces dynamic authorization and continuous monitoring and makes it effective against compromised IoT devices. However, the protocol is only focused in a power IoT environment is yet to be expanded to other IoT environments. Table 4 shows an overview of the ZT protocols

Table 4: Overview of ZT Protocols

Ref	ZT Protocol	Security Property	Security Attacks Resisted
[3]	LCDA	Confidentiality, Freshness, Data integrity, Mutual authentication, Forward secrecy	Replay attack, Impersonation attack, MITM attack, Cloning attack, Relay attack, Sybil attack, Black-hole attack, DoS attack
[6]	PUFDCA	Confidentiality, Freshness, Forward secrecy	Impersonation attack, MITM attack, Physical attack, Replay attack,
[11]	Protocol for S-IoT	Unforgeability, Data integrity, Confidentiality, Forward security	Replay attack
[27]	Protocol for IoT Sensors	Mutual authentication, Secrecy of key agreement, Confidentiality, Data integrity, Privacy, Anonymity	
[28]	ZT-Access	Confidentiality, Data integrity, Privacy	Compromised devices, Leakage

2.7 Analysis of Reviewed Access Controls

Access control is essential in implementing ZT security. It is responsible for managing who can access what resources, under what conditions, and continuously adapting to the changing security landscape which is what ZT security aims to enforce. Table 5 shows the components of specific access controls. UCON+ [1] combines UCON, ABAC, and a trust level evaluation engine (TLEE) to enforce ZT consumer IoT. It upholds modular integration and flexibility while fostering an inherent connection between dynamic authorization and trust level assessment. The ZT dynamic access control [10] implements continuous authentication using the identity of the object and access subject. The access control improves from the role-based access control (RBAC) by enforcing a trust-based access control (TBAC). Here trust is evaluated using the current behavior and historical behavior of access subject. The trust threshold is also adjusted based on the security environment. Access permission is then based on the trust and trust threshold obtained enforcing dynamic access control and authorization. This access control can be implemented in an IoT environment to enforce security based on dynamic trust evaluation. The Security Attribute-based Dynamic Access Control (SADAC) [7] uses security-related attributes of users and devices for access control decisions. It enforces a dynamic supervision procedure, continuously evaluating the security profile of subjects and is used to implement access restrictions. When access is initially granted, it is periodically renewed using the subject and access object security level. This important for IoT security as threats are immediately restricted of access when identified. Expanding this fine-grained access control to an IoT framework can advance the integration of ZT in IoT security. The ZAIB access control model [8] for IoT integrates attribute-based access control (ABAC), ZT, and Blockchain to enforce resource access security. Unlike the access control of [10], ZAIB uses ABAC where it uses environmental and device behavior to create policies for authentication for dynamic access control. It uses blockchain to enhance security and privacy through anonymous device and user registration, immutable activity logs, protection of data and attributes, and smart contracts for access control. This is combined with continuous behavior analysis of subjects so that devices only remain authenticated if they are free from malicious behavior. The access control is an effective approach to securing IoT environments. However, it is a novel approach so improvements can still be made.

Table 5: Access Controls and Components

Ref	Access Control	Components	Basis for Assessing
[1]	UCON+	Context Handler, Message Bus, Session Manager, Policy Information Point, Attribute Table, Attribute Retriever, Device Inventory, Policy Decision Point	Trust level evaluation expressions
[8]	ZAIB-ABAC	Subject, Subject Attributes, Object, Object Attributes	Environmental and Device Behavior
[7]	SADAC	User, Security Profile	Security-related Attributes of Subject
[10]	TBAC	User, Role, Res (resources), Ope (operations), Perm (permissions)	Current and Historical Behavior of Subject

3 CONCLUSIONS

Effective authentication and access security methods must be enforced in IoT systems to protect all shared data from malicious actors and threats. Because of the limitations of perimeter-based security, such as the inability to detect malicious actors within a network and prevent lateral movement, the concept of ZT has gained popularity. In ZT, all subjects are treated as untrusted and must constantly undergo authentication while being constantly monitored during resource access sessions. Authentication and access control are essential in ZTA and establish robust security especially in IoT systems. Literature regarding ZT-based authentication and access security for IoT is reviewed in this study. In the reviewed articles, three frameworks, namely the four-dimensional framework [2], ZT-ARF [4], and GAZETA [5] were discussed and each framework provided similar strengths for ensuring ZT-based security. The frameworks enforce dynamic access control models to determine trust levels of subjects to determine whether to provide access or not. Real-time network security, fine-grained access control, and continuous authentication is implemented in the frameworks to ensure security of data within IoT systems. In the reviewed literature, Five ZT protocols for authentication and access security were discussed namely LCDA [3], PUFDCA [6], Protocol for S-IoT [11], ZT-Access [28], and Protocol for IoT sensors [27]. The LCDA protocol combats the most types of security attacks but is yet to be implemented in an IoT environment. PUFDCA proves to be lightweight and resistant to multiple attacks, which is effective for IoT systems. However, it relies on device locations for authentication. The reviewed protocols are consistent in ensuring confidentiality and data integrity which are essential for safeguarding IoT systems. In the reviewed literature, four access controls, UCON+ [1], TBAC [10], SADAC [7], and ABAC [8] were discussed. The access controls varied based on the elements used for determining whether to trust the subject. UCON+ used trust level evaluation expressions. TBAC used the subject's current and historical behavior. The security-related attributes of the users and devices were used by SADAC. ABAC focuses on environmental and device behavior in creating policies. Overall, the reviewed frameworks, protocols, and access controls provide ZT-based security solutions that ensure all subjects requesting resources are robustly assessed and evaluated before granting access. Through these frameworks, protocols, and access controls, ZT ensures continuous authentication and monitoring in sessions, preventing security attacks that threaten IoT systems, resulting in data compromises and loss. This allows for the effective safeguarding of IoT systems.

4 REFERENCES

[1] Theo Dimitrakos, Tezcan Dilshener, Alexander Kravtsov, Antonio La Marra, Fabio Martinelli, Athanasios Rizos, Alessandro Rosetti, and Andrea Saracino. 2020. Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 1801-1812. DOI: https://doi.org/10.1109/TrustCom50675.2020.00247

[2] Baozhan Chen, Qiao Siyuan, Zhao Jie, Liu Dongqing, Shi Xiaobing, Lyu Minzhao, Haotian Chen, Lu Huimin, and Zhai Yunkai. 2021. A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture. IEEE Internet of Things Journal, 8, 13 (July 2021), 10248-10263. DOI: https://doi.org/10.1109/JIOT.2020.3047589

[3] Syed W. Shah, Naeem Firdous Syed, Arash Shaghaghi, Adnan Anwar, Zubair A. Baig, and Robin Doss. 2021. LCDA: Lightweight Continuous Device-to-Device Authentication for a Zero Trust Architecture (ZTA). Computers & Security, 108, (2021). DOI: https://doi.org/10.1016/J.COSE.2021.102351

[4] Safwa Ameer, Maanak Gupta, Smriti Bhatt, and Ravi Sandhu. 2022. BlueSky: Towards Convergence of Zero Trust Principles and Score-Based Authorization for IoT Enabled Smart Systems. In Proceedings of the 27th ACM Symposium on Access Control Models and Technologies (SACMAT) (SACMAT '22), June 8–10, 2022, New York, NY, USA. ACM, New York, NY, USA, 10 pages. DOI: https://doi.org/10.1145/3532105.3535020

[5] Yunfei Ge and Quanyan Zhu. 2023. GAZETA: A Game-Theoretic Zero-Trust Authentication Framework for 5G IoT Networks. IEEE Transactions on Information Forensics and Security. DOI: https://doi.org/10.1109/TIFS.2023.3326975

[6] Shrooq Alshomrani and Shan Cang Li. 2022. PUFDCA: A Zero-Trust-Based IoT Device Continuous Authentication Protocol. Wireless Communications and Mobile Computing, 2022, 9 pages. DOI: https://doi.org/10.1155/2022/6367579

[7] Pedro García-Teodoro, José Camacho, G. Maciá-Fernández, José-Antonio Gómez-Hernández, and V.J. López-Marín. 2022. A novel zero-trust network access control scheme based on the security profile of devices and users. Computer Networks, 212, (2022). DOI: https://doi.org/10.1016/j.comnet.2022.109068

[8] Samir Masood Awan, Muhammad Ajmal Azad, Junaid Arshad, Urooj Waheed, and Tahir Sharif. 2023. A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT. Information, 14, 129 (2023). DOI: https://doi.org/10.3390/info14020129

[9] Belal Ali, Mark A. Gregory, and Shuo Li. 2021. Uplifting Healthcare Cyber Resilience with a Multi-access Edge Computing Zero-Trust Security Model. In Proceedings of the 31st International Telecommunication Networks and Applications Conference (ITNAC), 192–197. DOI: https://doi.org/10.1109/ITNAC53136.2021.9652141

[10] Qigui Yao, Qi Wang, Xiaojian Zhang, and Jiaxuan Fei. 2020. Dynamic Access Control and Authorization System based on Zero-trust architecture. In Proceedings of 2020 International Conference on Control, Robotics and Intelligent System (CCRIS 2020), October 27–29, 2020, Xiamen, China. ACM, New York, NY, USA, 5 pages. DOI: https://doi.org/10.1145/3437802.3437824

[11] Minqiu Tian, Zifu Li, Fenghua Li, Jinzhang Cao, and Chao Guo. 2022. A Terminal Security Authentication Protocol for Zero-Trust Satellite IoT. In Proceedings of IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 299-306. DOI: https://doi.org/10.1109/TrustCom56396.2022.00049

[12] Naeem Firdous Syed, Syed Wali Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig, and Robin Doss. 2022. Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access, 10, 57143-57179. DOI: https://doi.org/10.1109/ACCESS.2022.3174679

[13] Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, and Xiangjie Ma. 2022. A Survey on Zero Trust Architecture: Challenges and Future Trends. Wireless Communications and Mobile Computing, 2022, 13 pages. DOI: https://doi.org/10.1155/2022/6476274

[14] Ana Antoniette C. Illahi, Alvin B. Culaba, and Elmer P. Dadios. 2019. Internet of Things in the Philippines: A Review. In Proceedings of IEEE 11th International Conference on HumanoidNanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM), 6 pages. DOI: https://doi.org/10.1109/HNICEM48295.2019.9072882

[15] Rudra Krishnasrija, Amit Kr Mandal, and Agostino Cortesi. 2023. Lightweight Mutual and Transitive Authentication Mechanism for IoT Networks. Ad Hoc Networks 138 (2023) 103003. DOI: https://doi.org/10.1016

[16] Maya Derrick. 2023. Philippines' digital economy set for exponential growth. https://datacentremagazine.com/articles/philippines-digital-economy-set-for-exponential-growth

[17] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Conelly. 2020. Zero Trust Architecture. NIST. https://doi.org/10.6028/NIST.SP.800-207

[18] Satyajit Sinha. 2023. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/?fbclid=IwAR1DBd97N2D0xmgIEoc_PcvG-JT2yE3Dp_KoUCYU--Fr3VLidKjjm-6M1tQ#:~:text=In%202022%2C%20the%20market%20for

[19] David Bradbury. 2023. It's official: Zero Trust now favored by 96% of organizations. Okta. https://www.okta.com/blog/2023/10/its-official-zero-trust-now-favored-by-96-of-organizations/?fbclid=IwAR10KI4owjIe-rk0j3DTY05cMLCbZdTnIRHxg6r1aBskgoFZ9_A0AecURp0#:~:text=Zero%20Trust%20began%20as%20an,of%20Zero%20Trust%20Security%202023

[20] Roberto Minerva, Abyi Biru, Domenico Rotondi. 2015. Towards a definition of the Internet of Things (IoT). IEEE Transactions on Computers. DOI: https://doi.org/10.1109/

[21] Phillippa Biggs, John Garrity, Connie LaSalle, and Anna Polomska. 2016. Harnessing the Internet of Things for Global Development. Geneva: International Telecommunication Union.

[22] ISO/IEC JTC 1. 2015. Preliminary Report 2014 Internet of Things (IoT), 1-11. https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf

[23] Ron Ross, Victoria Piliterri, and Kelly Dempsey. 2022. Assessing Enhanced Security Requirements for Controlled Unclassified Information. NIST Special Publication 800-172A. DOI: https://doi.org/10.6028/NIST.SP.800-172A

[24] Kassab, W., & Darabkh, K. A. (2020). A-Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. Journal of Network and Computer Applications, 163, 102663. DOI: https://doi.org/10.1016/j.jnca.2020.102663

[25] Debabrata Singh, Bibudhendu Pati, Chhabi Rani Panigrahi, and Shrabanee Swagatika. 2020. Security Issues in IoT and their Countermeasures in Smart City Applications. In Advanced Computing and Intelligent Engineering (Advances in Intelligent Systems and Computing 1089), B. Pati et al. (Eds.). Springer Nature Singapore Pte Ltd., Singapore, 301-313. DOI: https://doi.org/10.1007/978-981-15-1483-8_26

[26] Mourade Azrour, Jamal Mabrouki, Azidine Guezzaz, and Ambrina Kanwal. 2021. Internet of Things Security: Challenges and Key Issues. Journal of Ambient Intelligence and Humanized Computing, 1-19. DOI: https://doi.org/10.1007/s12652-021-03289-7

[27] Atefeh Mohseni Ejiyeh. 2023. Real-Time Lightweight Cloud-Based Access Control for Wearable IoT Devices: A Zero Trust Protocol. In First International Workshop on Security and Privacy of Sensing Systems (SensorsS&P), November 12–17, 2023, Istanbul, Turkiye. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3628356.3630118

[28] Wenhua Huang, et al. 2023. ZT-Access: A Zero Trust Access Control Scheme for Compromised Devices in Power IoT Environments. Ad Hoc Networks 145 (March 2023), 103161. DOI: https://doi.org/10.1016/j.adhoc.2022.103161.

[29] B Satyanarayana Reddy, M Ankamma Rao, K.Kranthi Kumar. 2020. A Survey on Internet of Things (IoT). International Journal of Advances in Arts, Sciences and Engineering, Volume 5 Issue. 2017 2320-6144 (Online), 98-106.

[30] M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," Sensors, vol. 18, no. 9, p. 2796, Aug. 2018. [Online]. DOI https://www.mdpi.com/1424-8220/18/9/2796.