Weinberg *et al*. *Complex Eng Syst* 2024;4:16
DOI: 10.20517/ces.2024.41

Complex Engineering Systems

Research Article

Open Access

Zero trust implementation in the emerging technologies era: a survey

Abraham Itzhak Weinberg[1], Kelly Cohen[2]

[1]AI-WEINBERG, AI Experts, Tel-Aviv 90850, Israel.
[2]Department of Aerospace Engineering, University of Cincinnati, Cincinnati, OH 45231, USA.

Correspondence to: Dr. Abraham Itzhak Weinberg, AI-WEINBERG, AI Experts, Tel-Aviv 90850, Israel. E-mail: aviw2010@gmail.com; ORCID: 0000-0002-2505-9653

How to cite this article: Weinberg AI, Cohen K. Zero trust implementation in the emerging technologies era: a survey. *Complex Eng Syst* 2024;4:16. http://dx.doi.org/10.20517/ces.2024.41

Received: 3 Jul 2024 **First Decision:** 22 Aug 2024 **Revised:** 1 Sep 2024 **Accepted:** 19 Sep 2024 **Published:** 26 Sep 2024

Academic Editors: Shuping He, Hamid Reza Karimi **Copy Editor:** Fangling Lan **Production Editor:** Fangling Lan

Abstract

This paper presents a comprehensive analysis of the shift from the traditional perimeter model of security to the Zero Trust (ZT) framework, emphasizing the key points in the transition and the practical application of ZT. It outlines the differences between ZT policies and legacy security policies, along with the significant events that have impacted the evolution of ZT. Additionally, the paper explores the potential impacts of emerging technologies, such as Artificial Intelligence and quantum computing, on the policy and implementation of ZT. The study thoroughly examines how Artificial Intelligence can enhance ZT by utilizing Machine Learning algorithms to analyze patterns, detect anomalies, and predict threats, thereby improving real-time decision-making processes. Furthermore, the paper demonstrates how a chaos theory-based approach, in conjunction with other technologies such as eXtended Detection and Response, can effectively mitigate cyberattacks. As quantum computing presents new challenges to ZT and cybersecurity as a whole, the paper delves into the intricacies of ZT migration, automation, and orchestration, addressing the complexities associated with these aspects. Finally, the paper provides a best practice approach for the seamless implementation of ZT in organizations, laying out the proposed guidelines to facilitate organizations in their transition towards a more secure ZT model. The study aims to support organizations in successfully implementing ZT and enhancing their cybersecurity measures.

Keywords: Zero trust, policy, eXtended detection and response (XDR), artificial intelligence (AI), quantum computing, chaos theory

1. INTRODUCTION

In recent years, several phenomena have been observed in which their interactions lead to the proliferation of the Zero Trust (ZT) approach. The first is an increase in the number of devices connected to the network, such as Internet of Things (IoTs)[1]. The second is poised emerging technologies, such as Artificial Intelligence (AI), Generative AI (GenAI), and quantum computing. The third is the rapid growth of cyberattacks, attack surfaces, and sophistication levels of attacks[2]. In addition, the COVID-19 pandemic has accelerated the adoption of cloud-based technologies and technologies that enable workers to work from anywhere they would like to. In addition, the White House Executive Order (WHEO) published definitions and migration steps for ZT to agencies[3].

In this paper, we focus on recent technological developments in ZT. The paper will focus on the influences of emerging technologies such as AI, and quantum computing on ZT implementation, elucidating their effects on the formulation of tailored ZT strategies. Additionally, we elaborate on their impact on ZT automation orchestration and migration in the context of new emerging technologies. To the best of our knowledge, only a few ZT survey papers relate to this aspect[4] and this is the first time that the combination between them has been surveyed.

This paper presents the challenges, approaches, and implementation of ZT for Detection and Response (DR) layers, such as Endpoint DR (EDR), eXtended DR (XDR), and Network DR (NDR) also known as Network Traffic Analysis (NTA). As can be learned from its name, DR has two purposes: detecting and responding to security incidents that aim to bypass the End Point Protection Platforms (EPP). ZT is a crucial framework for EDR as it is one of the most exposed points to cyberspace.

The paper is organized as follows: First, we introduce ZT, discussing its history and evolution over the years. Next, we elaborate on the ZT policy and its principles. In the subsequent section, we explore the challenges that ZT faces. Following that, we delve into discussions on ZT implementation methods. Subsequently, we address the integration of ZT with cutting-edge technologies such as AI, chaos theory, and quantum computing, as well as cybersecurity. We also discuss approaches for evaluating ZT. Finally, we conclude by summarizing the main issues and outlining future directions.

While dealing with defense approaches, it is important to bear in mind that while the attack can be considered a success story, even after many failures, the defense must always be successful. Hence, defense capabilities must be better than potential attacks. Cybersecurity experts claim that an attack will eventually occur, and practically, the chances of 100% are only theoretical[5]. Risk can be mitigated by early detection and response to an attack when it occurs. ZT is expected to solve this gap. Since ZT plays a practical role in many organizations, we find in the literature design principles such as designing architecture from the inside out, determination of the access needs at a preliminary stage, focusing on the required organizational outcomes, and using the EDR as a source for inspecting the log traffic[6].

The ZT can help protect against Operational Technology (OT) attacks. OT attacks are designed to exploit systems that are directly on the plant floor[7]. ZT can be applied to Industrial Control Systems (ICS) to ensure that only authorized devices and users can access the system[8,9]. For example, in the case of the 2017 NotPetya attack[10], which caused millions of dollars in damage to industrial sites, ZT principles could have prevented the spread of malware by limiting lateral movement between systems. In addition, ZT can improve Remote Access Security (RAS) by enforcing strict authentication and access control policies[11,12]. ZT can help protect against supply chain attacks by limiting third-party vendors' access to critical systems and data. It can also help protect against IoT-based attacks by ensuring that only authorized devices can access the network[13,14].

Finally, OT attacks using open Application Programming Interface (API) can pose a serious threat to industrial control systems, allowing attackers to gain unauthorized access to OT systems and data[15]. ZT model includes strict access control and authentication policies, network segmentation, and security measures that specifically target open APIs, such as using API gateways to enforce authentication and access control policies. The implementation of a ZT can effectively complement Digital Twin (DT) configurations. DTs create a virtual representation of a physical system, facilitating various purposes such as monitoring, optimization, planning, and decision-making[16,17].

By replicating key aspects of physical objects or systems using sensors and real-time data, DT enables modeling, analysis, and testing of changes prior to real-world implementation. To ensure the protection and segmentation of DT, the application of ZT principles is essential, encompassing strong authentication, authorization, microsegmentation of sensitive data, and centralized monitoring of logs and events[18]. Using DT can increase integration of real-time data and, as a result, ensure robust security measures. This can lead to mitigation of the risks associated with tampering and cyberattacks. ZT principles guarantee that only authorized access is granted, enhancing the security, resilience, and effectiveness of information technology (IT) and operational systems by integrating virtual models with granular, context-aware access controls and monitoring mechanisms[19]. The integration between the two can serve as a valuable test bed for simulating cyberattacks and evaluating the effectiveness of ZT in handling such threats.

1.1. Zero trust history and evolution

The phrase ”Zero Trust” was coined by Stephen Paul Marsh in 1994[20]. The next step occurred approximately a decade later in 2003. The Jericho Forum consortium defined de-perimeterization[21]. They claimed that ZT can be used as a security strategy for de-perimeterization. De-perimeterization is practically the removal of a boundary between an organization and the outside world. Only six years later, in 2009, Google implemented ZT architecture BeyondCorp and published it in 2014[22]. BeyondCorp uses an authentication-based combination of the device and the user. Thus, it eliminates the need for privileged corporate networks.

In 2010, Kindervag *et al.*from Forrester used ZT for access control[23,24]. In their report, Forrester claimed that firewalls are not sufficient in the endeavor effort to cope with cyber attacks[24]. In addition, they coined one of the main premise principles of ZT: “never trust, always verify”[24]. In 2015, ZT analysts reported augmentation in the adaptation of ZT by technology vendors[25,26].

In 2017, Forrester and Gartner published the ZT frameworks: Zero Trust eXtended (ZTX) ecosystem[27] and Continuous Adaptive Risk and Trust Assessment (CARTA)[28] respectively. ZTX is a framework that maps ZT to organizational applications. CARTA is considered a strategic framework that enables organizations to continuously assess their risk of cyberattacks. CARTA also enables the assessment of the trust level of organizational systems. In 2018, the National Institute of Standards and Technology (NIST) and National Cybersecurity Center of Excellence (NCCoE) published the cornerstone paper SP800-207. It defines cybersecurity metrics with a focus on ZT components and principles. In this way, it helps abstractly design the organizational network architecture in the light of ZT without drilling into a specific implementation[29]. In 2019, Gartner introduced the terms Zero-Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) to describe new defenses considered part of the emerging ZT framework[30]. These new models added available layers of protection beyond the traditional network perimeter.

In 2020, the COVID-19 pandemic accelerated widespread adoption of remote work, increasing the need for ZT approaches to secure hybrid workforces[30]. NIST published updated guidance on applying ZT principles in Federal networks in Special Publication 800-207.

In 2021, a Microsoft report found 96% of organizations saw ZT as critical to success due to security and compliance needs[30]. Meanwhile, federal orders and strategies laid the groundwork for public sector adoption to

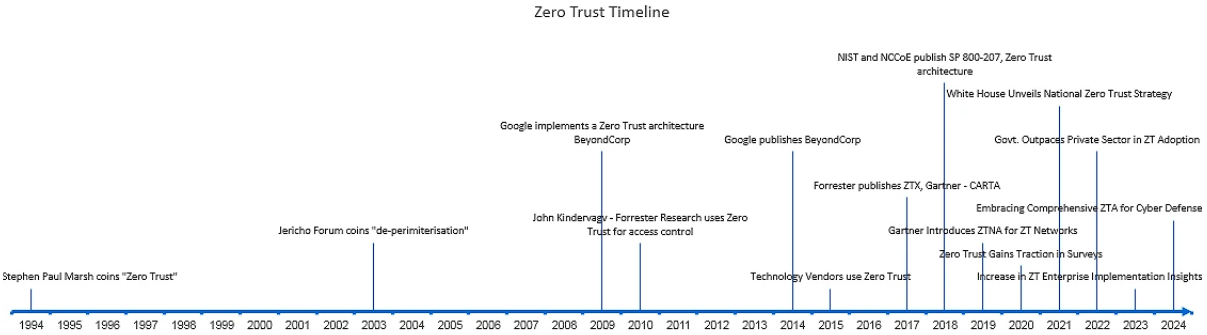
Zero Trust Timeline
NIST and NCCoE publish SP 800-207, Zero Trust architecture
White House Unveils National Zero Trust Strategy
Google implements a Zero Trust architecture BeyondCorp
Google publishes BeyondCorp
Govt. Outpaces Private Sector in ZT Adoption
Forrester publishes ZTX, Gartner - CARTA
Embracing Comprehensive ZTA for Cyber Defense
John Kindervagv - Forrester Research uses Zero Trust for access control
Jericho Forum coins "de-perimiterisation"
Gartner Introduces ZTNA for ZT Networks
Zero Trust Gains Traction in Surveys
Stephen Paul Marsh coins "Zero Trust"
Technology Vendors use Zero Trust
Increase in ZT Enterprise Implementation Insights
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024

Figure 1. Zero trust timeline.

strengthen national cyber defenses and transition to ZT.

In early 2022, the U.S. government accelerated its adoption of ZT frameworks[30]. United States Office of Management and Budget (OMB) released details of the federal ZT strategy and set requirements for agencies to meet five security goals by September 2024. Acting Director Young issued a memorandum stressing defenses against evolving threats. Additionally, Cybersecurity and Infrastructure Security Agency (CISA) published an expanded Cloud Security Technical Reference Architecture in June 2022, co-authored with two other agencies to guide adoption of ZT in cloud environments. Such proactive government efforts, combined with initiatives worldwide, indicated public sector leaders in ZT according to an Okta (company) report. It found that 72% of surveyed government organizations had active or planned ZT programs compared to 55% of private companies.

By 2023, OKTA reported ZT had gone mainstream[31], with adoption more than doubling in two years and 61% of organizations reporting a defined initiative. Another 35% planned to implement one soon, showing over 90% recognized its importance. The swift rise underscored how ZT strategies delivered stronger security as hybrid work became standard.

By 2024, ZT security reached a critical stage[32]. Adopting comprehensive Zero Trust Architecture (ZTA) became recommended to align defenses with evolving threats. ZT transformed from isolated tools to a foundational change, moving beyond legacy perimeter views. Full ZTA verified all users, assets and applications continuously, strengthening protections while boosting productivity as risks grew distributed and dynamic.

In Figure 1, we present the history and evolution of ZT.

Currently, ZT is widespread and has growing market potential. It is implemented in organizations worldwide that use different architectures and systems on both premise and cloud architectures. It has a prospect of 60.7 billion dollars by 2027, with an annual growth of 17.3%[33]. This is evident in the growth of ZT implementation and usage - horizontally all over the world and vertically - in many market segments and technologies. We can observe the invasion of ZT into 5G networks for healthcare devices[34].

2. ZERO TRUST POLICY AND PRINCIPLES

The ZT policy is a security framework that aims to protect organizations from cyberattacks. As a result, it encompasses all the organizational systems' users, regardless of their physical location. ZT continually validates the system security configuration, as well as authentication and authorization processes[35,36].

ZT changed the architecture of separation between different levels of security zones such as the Internet, De-

Militarized Zone (DMZ), and Trusted and Privileged zones to a controlled architecture[37,38]. ZT employs a Control Plane (CP) to effectively classify and distinguish between trusted and untrusted clients. When the CP acknowledges the client, it accepts the traffic. Typically, ZT uses an encrypted tunnel based on temporary one-time credentials to communicate with a trusted client. ZT transferred the traditional perimeter model and removed the borders between the different zones while maintaining secured communication only with trusted clients.

The CISA proposed the ZT Maturity Model[39] which divides ZT into eight pillars: users, infrastructure, devices, data, applications, networks, visibility and analytics, and orchestration and automation. The model relates to human factors, devices, and data usage. Each pillar indicates an identification process implemented before accessing the data or required services. ZT relates to both the static aspect of security that resides as data in devices and infrastructure, and to the dynamic aspect of data streams in networks and applications.

To achieve the ZT policy, the organization must relate to the security and authentication aspects of each pillar. Missing one of the pillars' security aspects might influence the ZT policy and, hence, breach the organizational security level. The first and most fundamental stage of ZT is user identification. This stage is critical because most breaches use compromised identities, which are difficult to detect[40].

This stage is implemented before accessing organizational resources. ZT defines a ZTNA policy that defines which of the remote workers are eligible to connect to specific resources. In recent years, the commonly used technique for identification has been based on Multi-Factor Authentication (MFA), such as Passkey. MFA is based on asking the user for two or more pieces of evidence for authentication.

ZT defines authorized devices and infrastructure only after going through a compliance process that stands under the Compliance Management (CM) spec. Thus, ZT ensures that the organization aligns with the required industrial cybersecurity regulations. To protect organizational data from exfiltration threats, ZT usually recommends encrypting data and using access control regulation policies, such as least privilege. ZT policy applies to applications in several ways such as legitimacy of the application, authorized user access to the application, and the environment in which the application can run. NIST defines the regulations for the ZT Application workload. Workload is a resource that supports application capability. ZT obligates organizations to define which resources are essential for each application and how they work in the most secure way.

To protect the network, ZT uses techniques such as explicit policies or variable trust. The variable trust uses a score to define the trust of the transferred data when an action is required. An additional ZT pillar involves visibility and analytics[36]. Visibility and analytics focuses on users and network traffic. To enable analytics and visibility, ZT guides organizations to enable network traffic inspection and store the history of logged users, asset logs, and actions. NIST ZT regulations advise the division of on-premise data centers and cloud, as well as workloads to traffic segments. Thus, ZT prevents lateral movement. In this way, the organization can investigate attacks and detect them online.

The eighth pillar of ZT in our list is orchestration and automation[41]. Automation and orchestration are the upper levels of ZT. They aim to deploy and apply ZT security policy. Automation focuses on making a process run without human intervention. It usually includes pipelines and scheduling parts, such as coordinating endpoint security. Orchestration adds optimization to automation. Orchestration usually includes AI components for each pillar. It helps in detecting attacks, identifying users, and responding to cyberattacks. To the best of our knowledge, orchestration has the highest level of ZT technology.

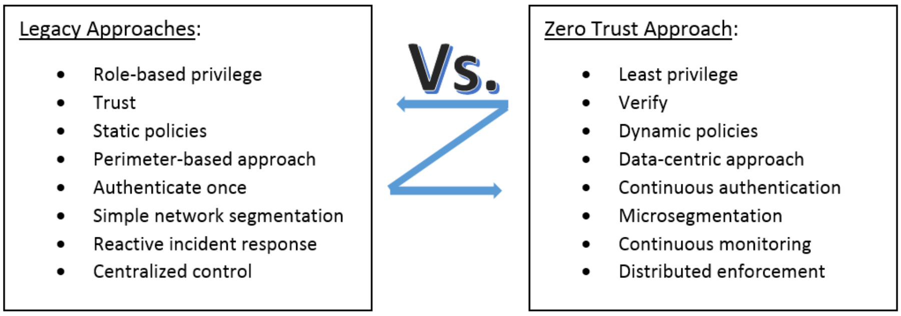

Figure 2. Legacy *vs.* Zero trust approaches.

2.1 From legacy policies and models to zero trust

ZT is considered a new approach compared to other policies and models that have been used for many years in the industry. This section discusses the relationship between them and ZT. One of the main characteristics of the ZT is its trustworthiness. To achieve this, ZT uses the Forrester's paradigm "never trust, always verify"[42]. The journey for achieving trustworthiness from security systems started many years ago by enforcing policies and access control. Access control techniques can be divided into Attribute Based Access Control (ABAC), Role Based Access Control (RBAC), and Fine Grained Access Control (FGAC)[43]. The main difference between the first approaches is whether the access control depends on the access user's attributes or organizational roles. Typically, RBAC is more popular because the same user can have several organizational roles. On the other hand, FGAC uses conditions or entitlements for user access confirmation.

The most popular and well-known models for enforcing access control in industry are the Bell-LaPadula (BLP) and Biba. Both Biba and BLP relate to the Confidentiality, Integrity and Availability (CIA) model. CIA is designed to guide policies for information security within an organization. Biba's main strength is to ensure the integrity of data in an organization, where BLP ensures confidentiality. In order to achieve it, Biba enforces two main rules: "no write up, no read down"[44] while BLP enforces "write up, read down" (WURD) or "no read up, no write down". In this way, Biba's principles prevent data modification by unauthorized objects, while the BLP's rules prevent the leakage of information. To enforce the required results, both models must be implemented as Mandatory Access Control (MAC) or Mandatory Integrity Control (MIC). However, in practice, it is a challenging task to enforce the models because many situations are considered grey zones. To solve these issues, Tidjon *et al.* proposed a ZT model that relied on and combined Biba and BLP[42]. The authors attached trust scores to each object (such as servers, files, and data channels). The scores use weights for each object based on Biba's integrity and BLP's confidentiality levels. ZT can rely on old models and can be implemented as a top layer in organizations that have already used these approaches.

2.1.1 Zero Trust in comparison to legacy policies and models

As mentioned before, ZT is based on solid grounds of legacy policies. The adoption of ZT dictates changes in the concepts and cybersecurity worldviews. Some of the main changes are summarized in Figure 2. The main differences are based on the following points: role-based *vs.* least privilege, trust *vs.* verification, static policies *vs.* dynamic policies, perimeter-based *vs.* data-centric, authenticate once *vs.* continuous authentication, simple network segmentation *vs.* microsegmentation, reactive incident response *vs.* continuous monitoring, and centralized control *vs.* distributed enforcement[4,45,46].

Legacy access control systems often rely on static roles and groups, implementing a role-based approach rather than a least-privileged one. ZT follows the principle of "least privilege", granting only the minimum access required for a specific task or context. Legacy models typically adopt an initial "trust but verify" approach, where devices and users are granted trust by default within the perimeter. ZT starts with "never trust, always verify" and requires continuous validation.

Legacy policies are typically static and undergo infrequent updates, in contrast to dynamic policies that adapt and evolve more frequently. On the other hand, ZT policies are more dynamic and situation-aware, changing based on context, such as location, task, and risk level. Legacy models primarily prioritize securing the network perimeter, in contrast to data-centric approaches that emphasize safeguarding the data itself. Instead, ZT focuses on securing individual data assets and granting only the necessary access on a per-request basis.

In legacy models, users are typically authenticated once and remain trusted until they log out, as opposed to continuous authentication methods that maintain ongoing verification throughout user sessions. ZT requires the continuous authentication and re-validation of access rights. Legacy network approaches often exhibit coarse segmentation, with simple network segmentation practices in place, as opposed to the more granular and precise microsegmentation methods. ZT leverages fine-grained microsegmentation-based methods, for example, on data, applications, users, and tasks.

Legacy security practices typically rely on reactive incident response strategies that address threats after they have been detected, in contrast to the proactive and continuous monitoring approaches that provide real-time threat awareness and prevention. ZT enables proactive threat detection and containment through continuous monitoring. Legacy security models typically depend on centralized control for policy enforcement, as opposed to distributed enforcement mechanisms that distribute policy enforcement throughout the network. ZT distributes enforcement points, such as EDR, across the full technology stack for increased resilience.

3. ZERO TRUST CHALLENGES

ZT challenges stem from continual changes in the organizational environment. These changes can be endogenous or exogenous. Organizational management decides on internal changes and reacts to environmental changes.

These decisions and other factors cause organizations to constantly change workers' positions and, as a result, their roles in the computational systems are changed. Worker status also changed on a frequent basis. New workers join organizations where others leave. In addition, each worker usually uses more than one device for his work and connects it to the organizational network. Moreover, in each device, several installed applications were used by their owners. The overall number of applications and devices is growing. An additional trend that has been evident in recent decades is data and service distributions. Organizational data and services are distributed in a wide variety of places. Some of them are located in the cloud, whereas others are on-premise.

The implementation of ZT in organizations is a phased project. Each phase depends on the previous phase, and the final prospective results can be achieved only after years[47]. During the implementation of the ZT project, the environment constantly changes. New technologies are added, and source allocation is changed. In addition, there are many changes in budget allocations in the organization, as well as in projects and ZT levels.

An additional aspect of project implementation is its impact on organizational policy. As ZT is a cornerstone in organizational security, it is supposed to influence its security policy. Consequently, it can cause a domino effect on other computational and security systems, as well as attack surfaces. ZT also influences organizational standards and procedures. It is necessary to close the gap between the pre and post-implementation stages of ZT. One of the main approaches for closing this gap requires integration between departments, teams of workers, products, and legacy systems. This is usually supported by new standards and procedures. A common solution for such an integration is the creation of an organizational repository that integrates the relevant information and helps coordinate between ZT project users and leaders.

The ZT project requires inspecting both inside and outside the perimeter of an organization. Since ZT is based on the continual inspection of organizational security, continual inspection of the relevant network components is required. It requires defining tools and metrics to monitor the security status. It also has an impact on organizational risk management. Last but not least, it requires a thorough inspection of network edges such as EDR, Internet Service Provider (ISP) components, organizational IoTs, and employees' applications and devices under the Bring Your Own Device (BYOD) policy. The challenges of ZT require not only an overall inspection of the current organizational systems but also looking outside the perimeter of an organization. It involves not only systems but also organizational workers and management, as well as every entity that works with the organization.

Emerging network attack techniques present key challenges to current ZT frameworks. Side-channel attacks exploit implementation vulnerabilities, bypassing authentication and encryption safeguards, undermining the principle of verifying every request[48]. Addressing novel side-channel risks is crucial. Password guessing attacks, stemming from compromised credentials, necessitate robust credential policies and passwordless authentication for mitigation[49,50].

There is a unique solution for authentication that provides a strong defense against account compromise such as Attribute-Based Password Authenticated Key Exchange (AB-PAKE) protocol, ensuring that only two legitimate users with desired attributes and correct passwords can establish a shared session key. However, ZT may not fully resolve issues in initial credential management. Techniques such as deepfakes pose detection challenges for existing methods such as behavioral analytics, requiring ZT strategies to identify manipulated requests. Distributed and encrypted threats obscure network visibility, demanding enhanced endpoint data for accurate risk identification. To combat the rapid pace of new attacks, ZT must blend segmentation for resilience with rapid threat containment strategies based on user behaviors.

Blockchain technology can serve several vital roles in supporting ZT architectures[51]. It excels in identity management by offering a decentralized approach to handling digital identities and credentials, mitigating single points of failure and enabling identity verification without central authority reliance. Through smart contracts, blockchain can enforce detailed, dynamic access control policies, including context-based rules and trust attestations. The immutable ledger of blockchain ensures data integrity, aiding in detecting unauthorized changes and anomalies within a ZT framework.

Moreover, blockchain facilitates trust establishment through transparent cryptographic verification, aligning with ZT's principle of verifying access trust without internal system visibility. By encoding ownership and lifecycle details on blockchain, asset management gains enhanced visibility into device identities, postures, and authorization levels for informed access decisions. Smart contracts also streamline policy enforcement, automating complex access policies in alignment with business rules stored on blockchain, ensuring consistent policy application in decentralized business environments.

The impact of ZT on operational overhead varies based on organizational implementation[52]. Initial setup and policy configuration may demand substantial effort initially, but ongoing operations typically do not impose significant overhead once established. While granular access controls and asset visibility add processing and storage requirements, these costs are balanced by long-term breach mitigation and enhanced access management efficiency.

Leveraging existing infrastructure minimizes additional hardware/software expenses, and automation through APIs and policy engines reduces manual workload. Workload segmentation and least privilege access optimize resource usage, while enhancing organizational agility and enabling secure cloud/remote access. Although there are upfront costs, a well-designed ZT approach focused on automation and efficient access management generally does not result in intolerable ongoing operational burdens at scale, emphasizing the importance of strategic resource planning.

In the next subsections, we divide the most fundamental ZT challenges into migration, automation, and orchestration. For each challenge, we will explain how emerging technologies, such as AI, can help organizations fulfill the challenge.

3.1 The role of AI in zero trust security

The AI revolution is already in place, with wide use in many fields, including cybersecurity. The AI is a double-edged sword. This is evident in malware generation using generative pre-trained transformer (GPT) tools[53]. The endless race between attackers and defenders relies on advances in AI technologies and solutions. In this section, we identify the way in which AI can integrate with ZT and elevate it to a higher level.

Usage in the ZT field can be classified into four main categories: CP, identity verification, attack detection, and monitoring[41]. The CP is the ZT brain responsible for decision making regarding whether to grant object access[35].

ZT goes hand-in-hand with the AI technology. AI can help in the implementation of ZT, as described before, and the symmetrical implementation of ZT intensifies the need for AI. The adoption of ZT policies enhances the need to use AI based on security ecosystems. Implementing ZT in an organization creates more data that stream from more objects and sources. This also affects the microsegmentation process and intensifies the need to analyze the data at a more granular level. By implementing ZT, there is a strict need to enforce policies. AI and automation can be leveraged to dynamically define and enforce fine-grained, context-aware access policies required for a ZT model. In addition, AI can be used to continuously analyze the risk levels associated with different entities, such as users, devices, events, and processes. AI dynamically adjusts ZT policies and responses in real-time.

The continuous verification requirements of ZT make it a natural fit for AI technologies that can monitor user and device behavior in real-time and detect anomalies. This includes behavioral analytics. Rapid changes in ZT environments require fast responses to security incidents. Fast responses to security incidents can be achieved by AI-driven automation, for instance. The implementation of ZT increases the number of system alerts. Only a small portion of alerts are relevant and must be handled. AI system reduces alert fatigue by reducing false alarms and highlighting and forwarding important issues. The nature of ZT increases the operational costs. AI enables automation of the tedious and routine operation of the ZT system and, as a result, can decrease operational costs.

3.2 Common AI algorithms for supporting zero trust cybersecurity

ZT classification and clustering are important techniques used in cybersecurity to identify potential security threats and protect against cyberattacks. These algorithms can be divided into supervised and unsupervised algorithms, which are also known as classification and clustering.

Classification algorithms can be used in ZT security models for purposes such as user and entity classification, anomaly classification, network traffic classification, file classification, and email classification. Machine Learning (ML) algorithms can classify users, devices, workloads, and applications into risk categories (such as high, medium, and low risk) based on their attributes and behaviors. This aids in access control and segmentation decisions. Anomaly classification can be trained based on normal behavior and activity patterns to classify new observations as normal or anomalous. This enabled the detection of threats and policy violations. Network traffic analysis can classify traffic into known categories, such as web, email, and Voice over Internet Protocol (VoIP), to enforce microsegmentation policies and detect abnormal traffic. File classification algorithms can classify files as malicious or benign to detect malware and block harmful files from entering a network. Email classifications can be used to detect phishing emails. The ML algorithms can be used to detect and filter threats before they reach the users.

The common classification algorithms used for ZT include Support Vector Machines (SVM)[54], Decision Trees (DT)[55], Linear Discriminant Analysis (LDA)[56], Artificial Neural Networks (ANN)[55], Convolutional Neural Networks (CNN)[57], Recurrent Neural Networks (RNN)[58], AutoEncoders (AE)[59] and Bidirectional Encoder Representations from Transformers (BERT)[60].

Clustering algorithms can be used in ZT security models in several ways, such as device and user grouping (where the groups are unknown in advance), application workload clustering, anomaly detection, threat hunting, and segmentation optimization. Clustering algorithms can group users and devices with no prior knowledge of relevant groups. These algorithms use similar attributes, access needs, and risk profiles. This can be used to assign them to roles and enforce the least privileged access controls. In addition, the algorithms can be used for clustering workloads based on their communication patterns, and dependencies can help optimize network microsegmentation and isolate workloads with different security requirements. Similar to classification algorithms, clustering algorithms can be used for anomaly detection where the groups are not explicit in advance. These algorithms can detect deviations in clustering patterns over time. For instance, if a node suddenly changes in a cluster, it can indicate anomalies and potentially suspicious behaviors. Threat hunting can be performed by clustering entities based on their network behaviors, and threats that exhibit different patterns can be identified and flagged for further investigation. An additional method to use clustering algorithms in the context of ZT is segmentation optimization. Network traffic patterns can be clustered to identify natural segmentation boundaries within the network, thereby aiding the design of the microsegments.

The commonly used algorithms for ZT clustering tasks are Affinity Propagation (AP)[61], Density-Based Spatial Clustering of Applications with Noise (DBSCAN)[62], Hierarchical clustering[63], Gaussian mixture modeling (GMM)[64,65], Self Organizing Map (SOM)[66] and K-Means[67].

A combination of supervised and unsupervised learning, classification, clustering, and neural network algorithms can be leveraged to implement the core functions required for ZT security model tasks, such as anomaly detection, role-based access, and behavior analysis.

3.3 Combating GPT and AI-based attacks with zero trust cybersecurity framework

In recent years, there has been a breakthrough and profileration of AI models and GPT. Side by side, they enable novel attack vectors. ZT, as a cybersecurity framework, has to adapt itself to these types of attacks and provide policies and solutions for mitigating them. AI-generated attacks are a growing cybersecurity threat that can be used by malicious actors to bypass the traditional security measures. These attacks can be generated using ML models and can include a variety of tactics such as spear-phishing, malware, and social engineering. To protect against AI-generated attacks, organizations can implement a ZT model that limits access to critical systems and data, and continuously monitors potential threats. This can include strict access controls, such as MFA and role-based access controls, and the continuous monitoring of network traffic and user behavior.

Additionally, organizations can use security solutions that are specifically designed to detect and respond to AI-generated attacks, such as AI-based threat detection systems that use ML algorithms to analyze network traffic and identify suspicious activities. The chaos theory-based approach can also be used to handle AI- and

GPT-based attacks. GPT has many useful applications and can also be used maliciously by hackers to generate realistic-looking phishing emails, social engineering messages, and other types of attacks. Malware generation using GPT tools is already available in[53]. We dedicate the next section on how chaos theory techniques can be used to detect and respond to these attacks[68]. To protect against AI- and GPT-generated attacks, organizations can implement a ZT model that limits access to critical systems and data, and continuously monitors potential threats. Additionally, organizations can use security solutions specifically designed to detect and respond to GPT-generated attacks, such as anti-phishing solutions that use ML algorithms to analyze the content and context of emails to identify suspicious messages.

4. ZERO TRUST STRATEGY AND APPROACHES

In this section, we describe several common ZT approaches that organizations can adopt, including the strategies and technologies they employ as part of a comprehensive ZT approach. The first approach is identity-based access control[69,70], which grants access based on verified user or device identities rather than network location, using MFA and strong identity management systems.

The second method was microsegmentation[71,72], which isolates the systems, workloads, and data within the network to minimize lateral movement if one asset is compromised. This method enforces strict control of network traffic. Additionally, the least-privileged access approach ensures that users and services only have the minimal access rights necessary to perform their assigned tasks. Privileges are granted on a just-in-time and as-needed basis. An additional relevant access approach is adaptive access[73,74], which dynamically adjusts access privileges based on real-time factors such as location, device health, and authentication strength, applying more stringent access controls for high-risk situations.

While minimizing access to entities, it is necessary to continuously monitor organizational systems and networks. Continuous monitoring and analytics enables this feature[35], as it constantly monitors network traffic, assets, and user behavior for anomalies that could indicate threats. AI and ML were used to detect deviations from normal patterns. To continually monitor organizational data traffic, gateways and service edges must be secured and monitored. Secure service edges enable the strict control of access to APIs and other external touchpoints[34,35]. The identity, permissions, and context of each request should be verified. In addition to implementing continuous monitoring, the organization can implement User and Entity Behavior Analytics (UEBA)[29,75]. It plays an important role in continuous monitoring. UEBA solutions can detect anomalies and deviations in things, such as user login and access patterns, device usage and communication patterns, privileged account activity API, and application usage. The other security aspect is related to data.

ZT requires data encryption[4,76]. Encrypting data at rest and in transit to prevent unauthorized access, even if the system is compromised. Therefore, key management and robust policies are critical. In recent years, there has been a transformation from an on-premise infrastructure and services to the cloud. ZT strategy involves securing a cloud workload[35,38,77]. ZT principles are applied to Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), including verifying managed identities, encrypting data, and enabling activity monitoring.

The aforementioned common approaches and technologies are part of a comprehensive, general ZT strategy. It is important to implement multiple types of controls instead of relying on a single technique in isolation. An additional approach to ZT involves the training and education of teams and users. Training and education are crucial for creating ZT environments[78]. Users must understand why policies have changed and how their workflows may have been impacted. This could reduce friction and encourage adoption. From the perspective of implementation and project management, the organization must consider that ZT extends beyond technology. It also requires changes in processes, governance, and organizational culture. These include establishing a

ZT Center of Excellence (ZTX CoE) and creating a ZT roadmap and milestones[29,35]. This section described some of the common strategies and technologies that organizations employ as part of a comprehensive ZT approach. Implementing multiple types of control instead of relying on any single technique in isolation is crucial. Moreover, it is essential to remember that ZT is an ongoing journey rather than a final destination. Organizations must consistently evaluate and optimize their ZT posture in response to evolving threats and improving security maturity.

5. ZERO TRUST IMPLEMENTATION BEST PRACTICE

Earlier, we described the ZT migration. ZT implementation establishes a ZT posture from the start of a new environment. ZT migration transitions from an existing traditional security model to ZT architecture over time.

Organizations can make a smooth transition to ZT security over time by using several principles. To successfully adopt a ZT model, organizations should begin with small-scale pilots to gain experience, validate the value proposition, and troubleshoot any issues before gradually expanding[28,29,79,80]. The management and leading team should conduct a comprehensive inventory of all assets, including users, applications, devices, and data, to establish visibility and a baseline for the ZT model.

Several success stories illustrate the impact of ZT on the organization. Airbus[81], Capital One[82], and NASA[83] successfully implemented models for enhanced security and operational efficiency. Airbus witnessed that ZT was extended to corporate data across email, collaborative applications, and custom-built solutions while maintaining a balance between security and productivity. Mobile endpoints were securely protected from cyber threats through proactive visibility, detection, and remediation of potential issues from a cloud-based platform that enabled smooth, simple deployment to over 100,000 corporate devices. An easy-to-use, non-intrusive interface allowed field workers to remain productive while accessing resources with the confidence of robust protection everywhere.

Capital One's adoption of ZT reflects an IT security approach mandating thorough identity validation for all users and devices attempting to access network assets, irrespective of their location within or beyond the network perimeter, showcasing the importance of such measures in bolstering overall network security. Additionally, ZTNA serves as a critical facet within the SASE framework, emphasizing the significance of adaptive security protocols within contemporary network architectures.

NASA adopted ZT principles to securely enable hybrid workforces to collaborate from anywhere, using any device at any time as guided by its Future of Work strategy. Well-implemented ZT architectures streamlined cybersecurity efforts by providing consistent security controls and user experiences regardless of location. As a guiding principle for security architectures aimed at improving security posture and increasing cyber resilience, ZT both reduced risks from malware infections and minimized potential impacts of attacks. Partial ZT deployments within NASA nonetheless yielded dramatic security enhancements by guiding more secure cloud computing through identity-based adaptive controls and demonstrating that perfect implementations should not preclude considerable improvements from good progress toward a ZT model.

While success stories illuminate the path for some ZT projects, a different narrative emerges when considering the potential pitfalls that could lead to failure in US federal agencies, as predicted by Gartner[84]. Gartner Predicts 75% of U.S. Federal Agencies Will Fail to Implement ZT Security Policies Through 2026. These pitfalls include funding shortfalls causing implementation delays, a cybersecurity skills shortage impeding recruitment efforts, struggles to meet policy deadlines amidst budget constraints, limited progress reporting complicating transparency, and the looming risk of incomplete ZT adoption leaving agencies vulnerable to threats, potentially resulting in service disruptions or costly data breaches.

To achieve the desired end state, a clear vision and roadmap should be articulated and broken down into manageable phases and priorities. It is equally important to focus on changes in security policies, procedures, and people, as it is on technologies to ensure buy-in from all stakeholders. Automation should be used wherever possible to minimize manual effort and human error, starting with easy wins to build momentum and validate the concept[39].

Incorporating API-based access for applications can help minimize fragile and centralized components. A risk-based approach should be adopted, prioritizing high-risk users, assets, and access for initial ZT implementations to maximize the impact[85]. Careful planning and testing should be performed when integrating various zero-trust solutions to avoid these issues. A clear change management plan should be developed, communicating changes to employees, predicting impacts, and formulating a plan to minimize disruptions while providing adequate training[86,87].

A governance model should be created, defining roles, processes, policies, and guidelines around ZT to manage and maintain it in the long term. Regular progress measurement using metrics can help evaluate the effectiveness and identify areas for improvement, allowing for necessary adjustments. Finally, a multi-year roadmap should be developed to guide ZT implementation and achieve the desired end state over time[80].

In addition, it is always beneficial to follow the best practice guidelines that have already been tried in other organizations. The first principle is to start small but think big. It is recommended to begin with small-scale pilots to prove value and address any issues before gradually expanding to the entire organization. Conducting a full inventory of all assets, users, devices, applications, networks, and data provides visibility and a baseline for ZT models.

Creating a clear vision and roadmap for the desired end state, and breaking it down into actionable phases and priorities, helps organizations achieve their goals and minimizes risk and complexity.

6. AI AS A SUPPORTIVE SOLUTION FOR ZERO TRUST CHALLENGES

In this section, we will explore the primary ZT challenges of migration, automation, and orchestration. We will discuss and demonstrate how AI can enhance the solutions for these challenges.

6.1 Migration challenges and how AI can help

ZT migration refers to the transition of an existing traditional network security model to ZT architecture. We can identify several potential challenges that organizations face when transitioning to a ZT security model, including complexity[25,88], resistance to change[89], cost[90,91], visibility[92], compatibility of legacy systems[73], integration[72], technology immaturity[93], lack of skills and expertise[94] and implementation time[92]. Navigating the complexities of ZT implementation requires a holistic multilayered approach that encompasses numerous changes across networks, systems, applications, processes, and policies. This level of change is inherently complex to implement[25,88]. Furthermore, resistance to change can pose a challenge, as some organizations face pushback from employees who are comfortable with the status quo and are reluctant to adopt new security practices and policies. Effective communication and change management strategies are crucial[89]. AI plays a significant role in addressing these challenges. By automatically enforcing dynamic policies, AI is well suited for implementing fine-grained, context-aware, and continually adapting access policies at the core of ZT. Additionally, AI's scalability surpasses that of humans, reducing resistance to change.

Another aspect to consider is the cost of implementing a comprehensive ZT model. The inclusion of various components such as MFA, microsegmentation, and continuous monitoring can be financially demanding, particularly for large organizations[90,91]. Nevertheless, leveraging AI and ML to automate complex tasks can help lower the operational costs involved in establishing and maintaining a strict ZT architecture. Moreover, many organizations realize a lack of visibility in their existing networks, systems, and access rights during the planning stage of ZT implementation. This lack of visibility adds further complexity to the planning and implementation processes[92]. AI can contribute to improving visibility by utilizing ML techniques to analyze network traffic, endpoint data, log files, and other relevant data sources, thereby providing a clearer understanding of the existing environment.

In addition, the incompatibility of legacy systems with ZT features, such as continuous authentication and device posture checks, presents another challenge. Overcoming this requires the implementation of workarounds, replacements, or even the creation of air gaps to bridge the compatibility gap[73]. Furthermore, integrating ZT solutions and technologies can be a challenging task, particularly when dealing with multiple point products from various vendors. This requires careful planning and rigorous testing to ensure successful integration.

In addition to the challenges of integrating ZT solutions and technologies from multiple vendors, organizations may face the hurdle of dealing with relatively immature technologies. Technologies such as identity management, microsegmentation, and other related components may still be in the early stages of development, demanding that organizations consistently update and enhance their implementation. Therefore, careful planning, rigorous testing, and a proactive approach to technology updates are essential for overcoming these obstacles and ensuring successful ZT implementation[72].

In addition, the lack of skills and expertise in areas such as identity, access management, segmentation, and cryptography can pose a hurdle for organizations adopting ZT[94]. AI can alleviate this challenge by automating complex authentication, authorization, access control, and monitoring processes, thereby reducing the manual effort and training required by workers. Implementing a full ZT transformation across an entire organization is a time-consuming endeavor, often taking months or years. The scale and complexity involved necessitate careful planning, phased implementation, and creation of roadmaps to ensure a successful and efficient transition[92].

In addition to the aforementioned challenges, AI can significantly contribute to ZT in various areas such as continuous verification, risk-based decisions, reducing alert fatigue, and detecting anomalies. Continuous verification, a key tenet of ZT, can be achieved through AI technologies such as behavioral analytics and anomaly detection. These AI capabilities enable continuous monitoring of user and device activities, ensuring the ongoing verification of trustworthiness.

The role of AI in ZT extends to risk-based decisions as it can continuously analyze risk levels associated with different users, devices, applications, network segments, and events. By dynamically adjusting ZT policies and responses in real time based on this analysis, organizations can effectively manage and mitigate risks. AI-powered solutions have been developed to combat alert fatigue. These solutions can filter and prioritize ZT alerts, allowing human analysts to focus on critical issues. By reducing mental exhaustion and human error, organizations can maintain a high level of vigilance in their security operations. Furthermore, AI techniques such as ML and deep learning excel in detecting anomalies and outliers in large datasets. As ZT relies on continuous monitoring and verification, these AI capabilities are critical for identifying potential threats and security breaches.

By leveraging continuous verification, risk-based decisions, alert fatigue reduction, and anomaly detection enabled by AI, organizations can enhance the overall security of their ZT implementation, effectively mitigate risks, and ensure a robust security posture. In summary, AI should be leveraged wherever possible during ZT migration to provide better insight, automate processes, enforce dynamic policies, continuously verify trust, make risk-based decisions, accelerate remediation, reduce costs, and detect anomalies. AI can help address many of these challenges and streamline the transition to a ZT model.

6.2 Automation challenges and how AI can help

ZT automation uses automated technologies and processes to implement the principles of ZT architecture. Several automation challenges are associated with ZT security models. The main automation challenges revolve around integrating solutions, orchestrating policies and scaling operations, and gaining full visibility. ZT principles require the continuous verification of trust, but current technologies still rely heavily on human intervention for many tasks. Automation is an important goal; however, full autonomy remains elusive. For completeness, some of the points overlap with the migration section.

As mentioned above, implementing ZT architecture involves addressing various challenges in different areas. Authentication and access requests, for instance, require the automation of these processes at scale, which can be complex. This entails the integration of identity management solutions with applications, APIs, and devices to establish a comprehensive and cohesive authentication framework[95,96].

Similarly, the continuous monitoring of trustworthiness is crucial in ZT; however, it poses a set of challenges. The continuous monitoring of users, devices, and applications in an automated manner requires the integration of various monitoring tools to gather and analyze relevant data[75]. On the other hand, incident response presents a challenge in fully automating the detection, containment, and remediation of security incidents, often requiring some degree of manual intervention[97,98].

Device onboarding in ZT networks involves automatic provisioning of devices and applications while enforcing security policies, which can be a complex process. This requires integration of identity management, configuration management, and network access control. AI can play a crucial role in automating the provisioning of devices and applications and ensuring the enforcement of necessary security policies, configurations, patches, and updates[99–101].

Automating the issuance, renewal, and revocation of credentials such as certificates and tokens at scale is notoriously challenging in ZT. Certificate management requires careful attention to obtain this right[75]. Privileged access management is another area where automation and control of privileged access for administrative activities while maintaining operational efficiency remains an ongoing struggle[102].

Data protection in ZT involves automatically encrypting data at rest and in transit according to security policies, which can be particularly challenging for big data and real-time systems[103]. In addition, automating the generation of audit reports and ensuring compliance with regulations is difficult and often relies on manual reporting, although AI can offer potential solutions in this area[104].

Finally, API management poses a complex endeavor, especially at an enterprise scale, as it requires the automatic management of the full lifecycle of APIs, including discovery, security, monitoring, and deprecation[105]. These challenges emphasize the need for careful consideration, integration, and automation in multiple areas of ZT implementation to achieve a robust and effective security framework.

AI and ML can significantly help with automation in ZT environments. They show great potential for automating many complex components of ZT environments, such as threat detection, dynamic policy management, risk-based access control, device onboarding, accelerated remediation, and verification of trust and compliance. This can streamline the operations and reduce costs.

AI systems can continuously analyze the risk levels associated with different users, devices, applications, locations, and other relevant factors to make automated access control and security decisions based on risk. These capabilities are already emerging today and will likely continue to improve and expand in the coming years to further enable AI-driven automation within ZT architectures.

6.3 Orchestration challenges and how AI can help

As mentioned above, ZT orchestration refers to the ability to automate and coordinate various systems and tools involved in organizational security. Orchestration involves integrating multiple automated systems and technologies involved in the security ecosystem, whereas automation focuses on automating individual ZT tasks and functions without direct human input. Similar to automation, the main orchestration challenges revolve around integrating point solutions, managing policies at scale, achieving visibility in operations, automating processes, and minimizing business disruptions. ZT requires coordinated actions across the full technology stack, and effective orchestration is key to success. Some of the key orchestration challenges for ZT security models include a range of crucial aspects, such as integrating solutions[106,107], management policies[108], scaling operations[109], achieving visibility[92], enforcing trust[110], automating responses[111], automated security workflows[47], checking posture[90], handling incidents[112], minimizing disruptions[113], and reducing costs[90].

Integrating solutions from multiple vendors for tasks such as identity management, access control, device management, network segmentation, and encryption can be difficult owing to the limited interoperability among these solutions[106,107].

In addition, managing various security policies across multiple systems, including access control, device configuration, encryption, and monitoring, requires complex orchestration to ensure dynamic enforcement[108]. Scaling ZT operations to support large-scale authentication, authorization, and monitoring of thousands or millions of users and devices poses further challenges that necessitate scalable solutions[109].

Achieving visibility by orchestrating data from various tools to obtain a unified view of users, devices, applications, networks, and threats is another challenge. Solutions often operate in silos, but AI techniques, such as ML, can analyze data from different ZT tools to provide a unified view of activities within the environment, enabling better orchestration[92]. Enforcing trust and continual verification across dynamic environments, with frequent additions and removals of users, devices, applications, and networks, adds complexity to the orchestration process[110].

Automating responses and coordinating solutions, such as Security Information and Event Management (SIEM), EDR, Network Access Control (NAC), and other relevant solutions in real time pose challenges, as most responses still require human input. However, AI models can be trained to autonomously integrate different ZT solutions from various vendors, minimize manual effort, and facilitate the correlation of data and alignment of policies[111].

Over time, AI may be able to orchestrate entire security workflows within ZT environments autonomously, from continuous monitoring to incident response, with minimal human intervention[47]. Another significant challenge involves effectively orchestrating security posture checks and trustworthiness assessments of devices and applications. This requires seamless coordination of operations across various solutions, including firewalls, antivirus programs, and configuration managers[90]. Furthermore, orchestrating end-to-end workflows to manage security incidents from detection to resolution requires centralized visibility, control, and coordination among teams, tools, and processes[112]. Minimizing disruptions to users and critical business processes during ZT operations requires central governance and policy enforcement for effective orchestration[113]. Finally, effectively orchestrating and automating ZT processes can optimize costs by reducing redundant tooling, streamlining purchases, and improving the overall efficiency[90].

AI and ML can be instrumental in orchestrating ZT environments and offer significant benefits in several key areas. First, AI is well suited for dynamic policy orchestration, as it can enforce and adapt fine-grained, context-aware access policies that form the foundation of ZT. By leveraging AI, policy changes can be orchestrated in real-time across multiple systems, enabling efficient and agile policy enforcement[111].

AI systems can also play a pivotal role in risk-aware orchestration. Through continuous analysis of the risk levels associated with users, devices, applications, locations, and other relevant factors, AI can dynamically adjust the orchestration and prioritize them based on risk. This proactive approach allows for adaptive and intelligent decision-making in managing security measures within ZT environments[114].

Furthermore, as ZT-related regulations continue to evolve, AI has the potential to automate compliance orchestration. Although this remains a challenge at present, in the future, AI systems may be capable of automatically orchestrating the necessary people, processes, and technologies to ensure compliance with ZT regulations. This would streamline compliance efforts and enhance the overall effectiveness of the ZT security frameworks[41]. The integration of AI and ML technologies into ZT environments empowers organizations with advanced capabilities to dynamically enforce policies, adapt to changing risk levels, and potentially automate compliance-related processes. The synergy between AI and ZT orchestration contributes to the overall efficacy and resilience of security measures in modern digital ecosystems.

AI and automation show great promise for orchestrating the complex components of ZT environments through techniques such as automated solution integration, dynamic policy management, enterprise-wide visibility, risk-aware decision-making, accelerated incident response, automated security workflows, and reduction of alert fatigue. AI can facilitate end-to-end coordination and synchronization within a ZT network.

7. ZERO TRUST AND CYBERSECURITY TECHNOLOGIES FOR DETECTION, PREVENTION, AND RESPONSE

In the previous sections, we mentioned algorithms and an AI approach for supporting the ZT response to attacks. In this section, we discuss the interaction between ZT and technologies, tools, and approaches that provide security solutions for detection, prevention, and response to cyber-attacks. ZT uses and dictates policy for tools and technologies that help organizations interact with the outside world. The definition of ZT provides a comprehensive approach to cybersecurity, helping organizations protect their critical systems and data from cyber threats. By implementing strict access controls, continuous monitoring, and risk-based authentication, organizations can reduce the attack surface and better protect themselves against potential threats. Additionally, the use of detection, prevention, and response tools can provide early warnings of potential threats and enable organizations to respond quickly and effectively to security incidents.

This section provides insight into the interaction between ZT and technologies and solutions such as XDR, EDR, NDR/NTA, Security Orchestration Automation and Response (SOAR) and SIEM[115,116]. The section explains why the aforementioned technologies can work synergistically with ZT and enhance the organizational security level.

The combination of XDR can countermeasure attacks, such as Living Off The Land (LOTL)[117]. XDR is a security approach that aims to integrate multiple security solutions, such as EDR, NDR/NTA, and SIEM, into a unified platform[116].

AI can be a meaningful tool for enhancing XDR and ZT. XDR is based on large volumes of backlogs. Even a small proportion of false alarms can cause tedious and intensive work for users. An ML-based system can decrease the human labor involved in analyzing a large amount of data. In addition, ML systems can increase the level of accuracy and, hence, decrease the number of false alarms. Combining the ZT policy with the XDR can practically decrease the number of logs by constantly verifying the endpoint online. However, constant verification can slow down the system response [118]. Practically, there is a need to determine the optimal point between the response time and the required threat level. This is a practical compromise between absolute never trust, ZT policy, and organizational needs.

Because there is a high probability that an organization will become a target for cyberattacks, one of the effective ways to handle it is detecting it as soon as possible [5]. Once an attack is detected, a rapid response is required. The effectiveness of an organization in handling an attack is one of the crucial parameters for its success in countermeasuring the attack. Detecting an attack at the endpoints usually indicates the early stage of the attack. Hence, implementing ZT in endpoint devices helps the organization cope with severe stages of attack.

XDR tools are currently attempting to bring together all the relevant security solutions. These are intended to unify multiple security capabilities into a single solution that offers automated analysis, remediation, monitoring, and detection. The organization aims to maximize the detection accuracy while increasing the security operations and remediation efficiency [119]. The benefits of XDR are deemed to be so broad that Gartner called XDR the top security trend to emerge out of 2020. XDR plays a central role in advancing ZT architecture when used together with more targeted Identity and Access Management (IAM) [80]. XDR solutions offer in-depth security monitoring via flexible as-a-service delivery, which addresses identity and data monitoring [119].

As part of XDR, NDR/NTA technologies play a crucial role in monitoring and analyzing network traffic, providing insights into potential threats, and enabling rapid responses within a ZT framework. Another important technology on which XDR relies is EDR. This refers to a category of cybersecurity solutions designed to detect, investigate, and respond to threats at the endpoint level. As part of the ZT architecture, EDR can significantly enhance the security of endpoints and strengthen the overall effectiveness of the ZT model.

An additional solution that enhances the ZT functionality is SOAR. SOAR is a security solution that uses automation and orchestration to streamline security operations and improve the incident response times [115,116]. In the previous section, we elaborated on the relation between ZT and automation and orchestration. By combining ZT and SOAR, organizations can implement a more effective and efficient cybersecurity strategy. ZT provides a strong security foundation by limiting access to critical systems and data and continuously monitoring potential threats. SOAR then builds on this foundation by automating security operations and incident responses, enabling faster and more effective responses to security incidents. For example, a ZT model may limit access to a critical system to only authorized users and devices, and continuously monitor the system for potential threats. If a threat is detected, SOAR can automatically trigger a response, such as isolating the system or blocking access until the threat is resolved. This automated response can significantly reduce incident response times and minimize the impact of potential security breaches.

An additional solution commonly used in the organizational security suitcase is the SIEM. The SIEM is a security solution that collects and analyzes security events from the IT environment to identify potential threats. By combining ZT and SIEM, organizations can implement a more effective and efficient cybersecurity strategy [120]. ZT establishes a robust security foundation by restricting access to critical systems and data while continuously tracking potential threats [115]. SIEM then builds on this foundation by collecting and analyzing security events across the IT environment, providing early warnings of potential threats. For example, a ZT model may limit access to a critical system to only authorized users and devices, and continuously monitor that system for potential threats. If a threat is detected, the SIEM can alert the security teams and provide detailed information about the threat, enabling faster and more effective responses to security incidents.

8. ZERO TRUST AND CHAOS THEORY

Chaos theory has been used in cybersecurity applications to detect cyberattacks. It is a branch of mathematics that studies the behavior of dynamic systems that are highly sensitive to initial conditions, meaning that small changes in the initial conditions can lead to vastly different outcomes.

In the context of cybersecurity, chaos theory can be used similarly to AI to analyze network traffic and detect anomalous patterns that may indicate the presence of a cyberattack[121]. By analyzing the behavior of network traffic over time, chaos theory-based algorithms can detect patterns that deviate from the expected behavior of the system, indicating that cyberattacks may be in progress[122]. An additional approach is to use chaos theory-based algorithms to analyze the behavior of individual network packets and detect anomalous patterns that may indicate the presence of a cyberattack[123].

Moreover, chaos theory can be used to compare the different states of an organization's systems and transferred data. The analysis can indicate a deviation from the normal behavior of the system, and might indicate a cyber-attack[124]. The analyzed data can be obtained from various sources, such as logs, EDRs, networks, computers, and every device that is connected to the organization systems.

While chaos theory-based approaches to cyberattack detection are still in the early stages of development and are not widely used in practice, they have shown promise in detecting certain types of cyberattacks such as Distributed Denial-of-Service (DDoS) attacks. However, these approaches also have limitations such as the potential for false positives and the need for extensive training data to develop accurate models. ZT and chaos theory can be used to enhance an organization's security posture. By combining ZT and chaos theory, organizations can implement a more effective and efficient cybersecurity strategy. As explained, by enforcing access control to critical systems and data and maintaining continuous monitoring for potential threats, the ZT approach offers a solid security foundation. Chaos theory analysis can be used to analyze network traffic and detect anomalous patterns that may indicate the presence of a cyberattack, providing an early warning of potential threats.

9. HOW DOES QUANTUM COMPUTING AFFECT ZERO TRUST

Akin to AI, which took many years from its inception to its ubiquitous presence, quantum technology is taking its first steps in general and in the cybersecurity world and has the potential to impact ZT[125]. Although several quantum algorithms, such as Shor's algorithm for integer factorization[126], Grover's algorithm for database search[127–129], Quantum Fourier transform[130,131] and quantum counting algorithms[132], offer promising exponential or quadratic speedups in asymptotic terms, achieving practical speedup on physical quantum computers still encounters significant technological challenges. However, these algorithms do give us a glimpse of the possibilities of overcoming these challenges. As mentioned above, quantum computing remains a speculative technology.

Despite this, it has the potential to revolutionize cybersecurity in several ways. For example, it can strengthen and enable future ZT security models by providing quantum-safe cryptography, scalable policy enforcement, enhanced visibility, accelerated automation, new sensing capabilities, and more resilient network properties that are more difficult to compromise[133]. However, it will likely be many years before these potentials are fully realized. The following are ways in which quantum computing could help strengthen and enable ZT security models in the future.

A quantum can contribute to safe cryptography. Quantum-resistant algorithms are essential for ZT solutions to withstand future attacks by quantum computers[134]. Technologies, such as quantum key distributions, can also enhance trust.

A quantum can enable the detection of anomalies. The pattern-matching and optimization capabilities of quantum computers may accelerate the detection of anomalies within ZT environments. This could help with continuous trust evaluation. Additionally, quantum computing can enhance the visibility of organizational security systems. The massively parallel processing power of quantum computers could potentially provide unprecedented levels of visibility in ZT networks, users, devices, applications, and data. Moreover, quantum technology has the potential to scale policy enforcement. In theory, quantum machines may be able to enforce fine-grained access policies required by ZT at a scale that classical computers cannot match. However, this was impossible for many years.

Existing access control strategies must adapt to the emerging threats and challenges posed by quantum computing[135]. Encryption algorithms such as RSA, built on the complexity of factoring large numbers, face vulnerability to Shor's algorithm on quantum computers, necessitating the evaluation and deployment of post-quantum encryption schemes[136]. Similarly, hash-based signatures such as Elliptic Curve Digital Signature Algorithm (ECDSA) are at risk of being compromised, prompting the adoption of quantum-resistant signature schemes. While symmetric cryptography offers more resilience compared to asymmetric methods, future quantum computers could potentially breach these defenses, underscoring the importance of larger key sizes for enhanced protection.

Access control policies that hinge solely on confidentiality of secrets may require reevaluation to anticipate decryption capabilities, urging the integration of multiple authenticators for fortified security measures. The adequacy of authentication factors, such as passwords and cryptographic one-time passwords, is called into question, urging the adoption of multifactor authentication incorporating physical and behavioral elements for heightened resistance.

Key management strategies must prepare for potential compromise of current keys, necessitating secure transitions as post-quantum alternatives come into play. Vigilance in monitoring for attacks is paramount, with a focus on identifying anomalies and unusual access patterns that could signify early cryptanalysis attempts in the landscape of quantum computing.

An important aspect of quantum technology is its ability to accelerate automation. The futuristic ability of quantum computers to rapidly process vast amounts of data could potentially be leveraged to automate complex ZT tasks such as continuous monitoring, threat detection, and response. When focusing on the EDR, quantum technology can be leveraged to develop sensors. New types of quantum sensors may be able to continuously monitor parameters, such as magnetic fields, vibrations, and temperatures, to help detect threats and anomalies within ZT environments.

Quantum has the potential to strengthen layered defenses. Quantum technologies could augment existing layers of ZT defenses, such as physical security and network segmentation, to make the overall model more resilient against threats. Finally, quantum systems are more difficult to compromise. The quantum properties of superposition and entanglement render quantum systems inherently harder to wiretap or eavesdrop on, potentially enhancing trust within ZT networks.

The advent of quantum computing necessitates fundamental adjustments to access control strategies within a ZT framework[137,138]. Quantum computers pose a threat to current encryption algorithms, demanding the adoption of post-quantum cryptography for secure data protection in transit and at rest. Upgrading cryptographic protocols, deploying quantum-resistant algorithms, and exploring new authentication methods are crucial steps to safeguard against potential quantum threats. Ensuring the integrity of blockchain-based access control systems also requires quantum-resistant cryptographic foundations. Companies must consider the risk of encrypted data compromise in the future and implement preemptive measures to mitigate quantum computing vulnerabilities.

Exploring quantum components and advanced quantum communication protocols within Zero Trust for Wireless Networks (ZTWN) represents a proactive approach to fortify security against potential cryptographic vulnerabilities posed by quantum computing advancements[137]. These quantum solutions, including Quantum Machine Learning (QML) algorithms and identity authentication techniques, enhance the long-term security objectives of ZTWN by leveraging quantum properties to ensure secure communication and thwart potential attacks.

Quantum computing has the potential to transform cybersecurity through quantum-safe cryptography, scalable policy enforcement, enhanced visibility, accelerated automation, new sensing capabilities, and harder-to-compromise network properties.

10. ZERO TRUST EVALUATION

A crucial aspect of implementing ZT is to compare the organization's security state prior to and after the adoption of ZT principles. Moreover, any change in the ZT policy or architecture affects the organization. An evaluation process is required to assess the impact of these changes. The evaluation process uses metrics as a compass that enables management to understand the changes and progress while using the ZT. In this section, we present several approaches and metrics to evaluate the effectiveness of the organizational ZT security model.

ZT consists of several components and their integration leads to a holistic solution. As shown in Figure 3, the main components are policy enforcement, authentication, authorization, segmentation, monitoring, and response to threats[73,139]. Policy enforcement plays a pivotal role in defining, distributing, and enforcing access policies. It is crucial to strive for consistency across identity management, authorization, and policy control points. In addition, it is important to evaluate how the ZT system enforces a least-privileged access policy for different users. Moreover, ZT uses posture checks to evaluate and continuously verify the health of the devices accessing the network and its applications[35]. These checks also fall into the category of XDR tools.

An important way for ZT to enforce its policy is to use an optimal authentication process. The evaluation of authentication must relate to all entities, such as users, devices, and applications[35,86]. Relevant metrics, such as MFA adoption, can be obtained by investigating the number of users utilizing the MFA. An additional metric relevant for authentication is privileged access usage, which can be calculated by the number of access attempts with elevated privileges. Access policy coverage can be used to identify the roles of defined access policies. In addition, access policy violations can be used to calculate violations of defined access policies. An example of a metric is policy coverage, which measures the number of assets with defined access to configuration policies. The policy compliance metric measures assets compliant with defined access and configuration policies. An additional metric that falls in the policy category is Posture, which checks the failure rate and assesses the number of posture checks that failed to indicate non-compliance.

The next step in the evaluation process is authorization. One of the foundation stones is continuous authorization. The evaluation has to relate to authorization aspects such as continuity and revalidating access permissions over time. This evaluation can predict the ability of ZT to catch privilege escalations and changes.

An additional evaluation aspect of ZT focuses on network segmentation. This evaluation indicates how the network is segmented to restrict lateral movement[140]. Microsegmentation techniques based on application, roles, and environmental configurations can be considered. The relevant metrics for this category include microsegmentation adoption as an indication of the number of applications using microsegmentation and its complementary metric, unmanaged devices, which indicates the number of devices connected without proper

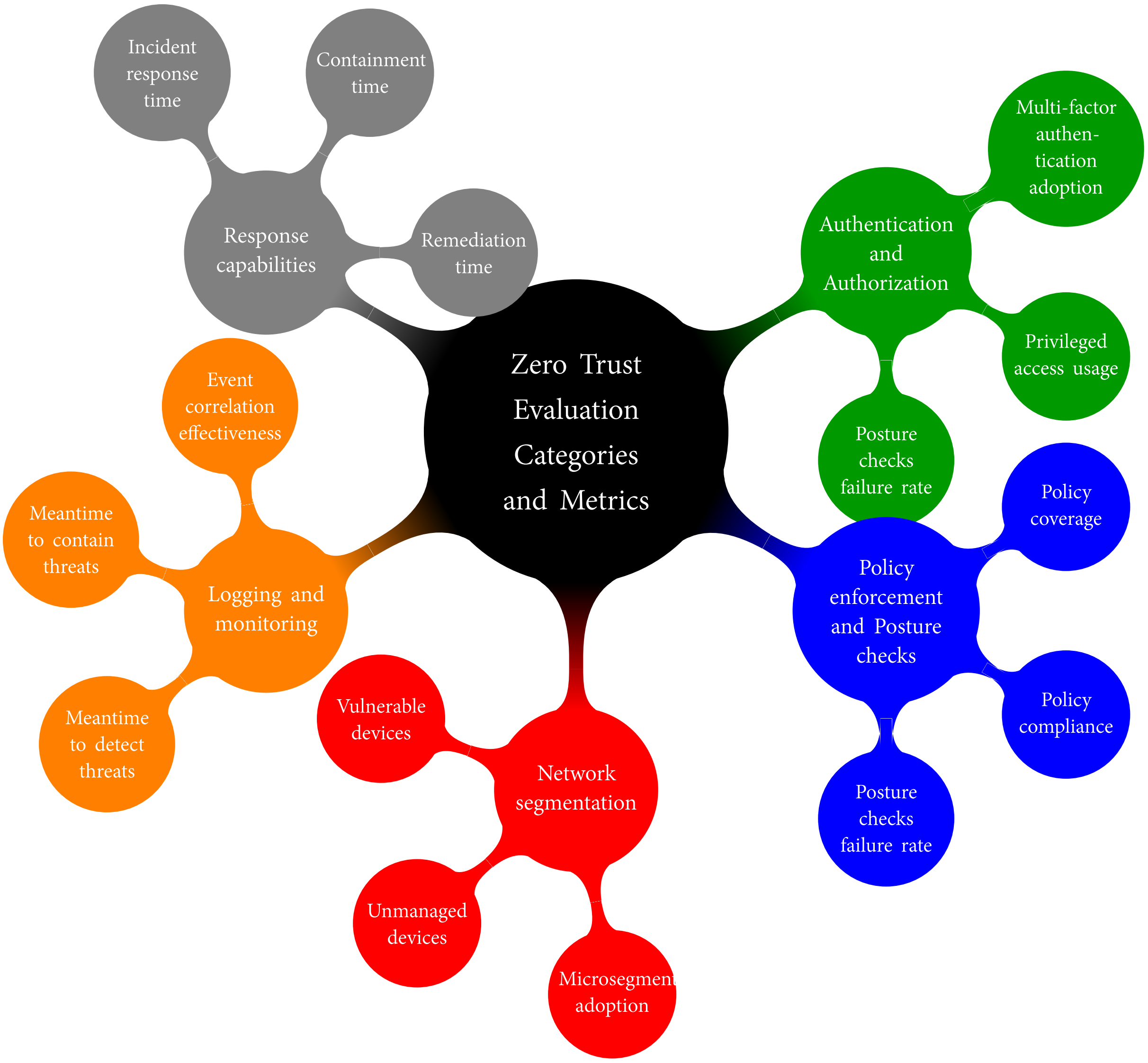
Zero Trust Evaluation Categories and Metrics
Response capabilities
Incident response time
Containment time
Remediation time
Authentication and Authorization
Multi-factor authen-tication adoption
Privileged access usage
Posture checks failure rate
Logging and monitoring
Event correlation effectiveness
Meantime to contain threats
Meantime to detect threats
Network segmentation
Vulnerable devices
Unmanaged devices
Microsegment adoption
Policy enforcement and Posture checks
Policy coverage
Policy compliance
Posture checks failure rate

Figure 3. Example for zero trust evaluation approaches and metrics.

registration. An additional metric is a vulnerable device that assesses the number of devices with vulnerabilities identified through the posture checks mentioned above.

Furthermore, the ZT evaluation category relates to the logging and monitoring of organizational systems. This evaluation consists of assessing organizational logs, event monitoring, and SIEM solutions. A high level of performance in this category ensures quick detection of anomalous behaviors. The metrics that can be used for evaluating the logging and monitoring categories are the mean time to detect threats and the average time to detect security incidents. The additional proposed metric is the mean time to contain threats, that is, the average time to isolate and contain security incidents. Another useful metric is event correlation effectiveness, which calculates the percentage of correlated events out of the total events.

The last category in our ZT evaluation process is response capabilities. It measures how quickly an organization responds to threats, revoke access, and remediate incidents. It also evaluates tabletop and red team penetration tests. Incident response metrics include the incident response time, which calculates the average time to begin the incident response after detection[141]. Another relevant metric is the containment time, which calculates the average time required to contain security incidents after detection. Finally, the remediation time metric calculates the average time required to fully remediate the security incidents after containment.

Additional qualitative metrics such as stakeholder satisfaction surveys, security assessments, and red team penetration test results can also provide valuable insights into the effectiveness of ZT initiatives. This section provides an overview of the main ZT evaluation categories and their metrics. By evaluating these key ZT capabilities, an organization can identify gaps, weaknesses, and areas for improvement to strengthen its overall security posture. Over time, it can track progress and measure the maturity and efficacy of the ZT model.

11. CONCLUSIONS AND FUTURE DIRECTIONS

This paper presents the main ZT issues relevant to the current era of evolving technologies. It also provides an overview of the main events that affect the ZT evolution. This study also compares the traditional ZT approaches with the current ones. In addition, it shows how organizations can implement emerging technologies and algorithms such as AI, quantum computation, and chaos theory, and how they affect the ZT strategy and implementation. Moreover, this study discusses the best practices and main issues in ZT challenges, such as migration, automation, and orchestration. Finally, this paper provides evaluation metrics and approaches for measuring the impact of ZT security on business operations, user experience, and overall security posture.

Future challenges and development directions for ZT architectures include extending policies to edge computing and IoT devices, advancing identity verification with blockchain and passive biometrics, implementing adaptive access authorization through machine learning, integrating ZT into supply chains, emphasizing API security, establishing continuous authorization practices, converging network and security infrastructure, adapting ZT for cloud and serverless applications, and transitioning to quantum-resilient cryptography for enhanced data protection against potential quantum computing threats.

Looking ahead, we predict that the persistent and significant challenges of verification and compliance assurance will continue to evolve alongside ZT architecture. As we delve deeper into the future of ZT security, several critical research and development areas warrant focused attention. These include safeguarding and securing AI and ML workloads, establishing unified access policies across multiple domains, and implementing privacy-preserving access controls. Further, the seamless integration of ZT with DevOps processes and practices represents another promising and essential direction for future exploration and development.

DECLARATIONS

Authors' contributions

Made substantial contributions to conception and design of the study: Weinberg AI, Cohen K
Conceptualization, Methodology, Writing - original draft: Weinberg AI
Conceptualization, Writing - review and editing: Cohen K

Availability of data and materials

Not applicable.

Financial support and sponsorship

None.

Conflicts of interest

Cohen K is an Editorial Board Member of the journal *Complex Engineering Systems*, and Abraham Itzhak Weinberg is affiliated with AI-WEINBERG.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Copyright

REFERENCES

1. IDC. Future of industry ecosystems: shared data and insights. 2021. Available from: https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/ [Last accessed on 23 Sep 2024].
2. Business. Cybercrime thrives during pandemic: verizon 2021 data breach investigations report. 2021. Available from: https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report [Last accessed on 23 Sep 2024].
3. The White House. Executive order on improving the nation's cybersecurity. 2021. Available from: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ [Last accessed on 23 Sep 2024].
4. Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero trust architecture (ZTA): a comprehensive survey. *IEEE Access* 2022;10:57143-79. DOI
5. Yampolskiy RV, Spellchecker MS. Artificial intelligence safety and cybersecurity: a timeline of AI failures. 2016. Available from: https://arxiv.org/pdf/1610.07997 [Last accessed on 23 Sep 2024].
6. Wylde A. Zero trust: never trust, always verify. In: 2021 international conference on cyber situational awareness, data analytics and assessment (CyberSA); 2021, pp. 1-4. DOI
7. Paes R, Mazur DC, Venne BK, Ostrzenski J. A guide to securing industrial control networks: Integrating IT and OT systems. *IEEE Ind Appl Mag* 2019;26:47-53. DOI
8. Zanasi C, Magnanini F, Russo S, Colajanni M. A zero trust approach for the cybersecurity of industrial control systems. In: 2022 IEEE 21st international symposium on network computing and applications; 2022, pp. 1-7. DOI
9. Li S, Iqbal M, Saxena N. Future industry internet of things with zero-trust security. *Inf Syst Front* 2022;1-14. DOI
10. Greenberg A. The untold story of NotPetya, the most devastating cyberattack in history. 2018. Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Last accessed on 23 Sep 2024].
11. Colombo P, Ferrari E, Tümer ED. Access control enforcement in IoT: state of the art and open challenges in the zero trust era. In: 2021 third IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-ISA); 2021, pp. 159-66. DOI
12. Chimakurthi VNSS. The challenge of achieving zero trust remote access in multi-cloud environment. *ABC J Adv Res* 2020;9:89-102. Available from: https://www.researchgate.net/publication/357920420_The_Challenge_of_Achieving_Zero_Trust_Remote_Access_in_Multi-Cloud_Environment/fulltext/639b2b3d484e65005b10b3d1/The-Challenge-of-Achieving-Zero-Trust-Remote-Access-in-Multi-Cloud-Environment.pdf [Last accessed on 23 Sep 2024].
13. Dhar S, Bose I. Securing IoT devices using zero trust and blockchain. *J Org Comput Elect Comm* 2021;31:18-34. DOI
14. Samaniego M, Deters R. Zero-trust hierarchical management in IoT. In: 2018 IEEE international congress on internet of things (ICIOT); 2018, pp. 88-95. DOI
15. Cheh C, Chen B. Analyzing openAPI specifications for security design issues. In: 2021 IEEE secure development conference (SecDev); 2021, pp. 15-22. DOI
16. Eckhart M, Ekelhart A. Digital twins for cyber-physical systems security: state of the art and outlook. In: Biffl S, Eckhart M, Lüder A, Weippl E, eds. Security and quality in cyber-physical systems engineering. Cham: Springer; 2019. DOI
17. Lv Z, Li Y, Feng H, Lv H. Deep learning for security in digital twins of cooperative intelligent transportation systems. *IEEE Trans Intell Transp Syst* 2021;23:16666-75. DOI
18. Sellitto GP, Aranha H, Masi M, Pavleska T. Enabling a zero trust architecture in smart grids through a digital twin. In: Dependable computing-EDCC 2021 workshops. 2021. pp. 73-81. DOI
19. Jagannath J, Ramezanpour K, Jagannath A. Digital twin virtualization with machine learning for IoT and beyond 5G networks: research directions for security and optimal control. *arXiv* 2022. pp. 81-6. DOI
20. Marsh SP. Formalising trust as a computational concept. PhD thesis. 1994. Available from: https://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf [Last accessed on 23 Sep 2024].
21. Welborn R, Kasten V. The Jericho principle: how companies use strategic collaboration to find new sources of value. John Wiley & Sons; 2003. Available from: https://hbswk.hbs.edu/archive/the-jericho-principle-how-companies-use-strategic-collaboration-to-find-new-sources-of-value [Last accessed on 23 Sep 2024].
22. Flanigan J. Zero trust network model. Medford, MA: Tufts University; 2018.
23. Kindervag J. Build security into your network's DNA: the zero trust network architecture. Forrester Research Inc. 2010.
24. Higgins KJ. Forrester pushes 'zero trust' model for security; 2010.

25. Alagappan A, Venkatachary SK, Andrews LJB. Augmenting zero trust network architecture to enhance security in virtual power plants. *Energy Rep* 2022;8:1309-20. DOI
26. Basim Al-Ruwaii GDM. Basim Al-Ruwaii GDM. Why the time has come to embrace the zero-trust model of cybersecurity; 2021.
27. Cunningham C. The zero trust eXtended (ZTX) ecosystem. Cambridge, MA: Forrester; 2018.
28. Campbell M. Beyond zero trust: trust is a vulnerability. *Computer* 2020;53:110-13. DOI
29. Kerman A, Borchert O, Rose S, Tan A. Implementing a zero trust architecture. National Institute of Standards and Technology; 2020. Available from: https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf [Last accessed on 23 Sep 2024].
30. Pratt MK. The history and evolution of zero-trust security. Techtarget; 2022.
31. OKTA. The state of zero trust security 2023; 2023.
32. SANS. Building a zero trust framework: key strategies for 2024 and beyond; 2024.
33. MarketsandMarkets. Zero trust security market by solution type. 2023.
34. Chen B, Qiao S, Zhao J, et al. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Int Things J* 2020;8:10248-63. DOI
35. Stafford V. Zero trust architecture. NIST Special Publication; 2020.
36. Rose S, Borchert O, Mitchell S, Connelly S. Zero trust architecture. National Institute of Standards and Technology; 2020.
37. Gilman E, Barth D. Zero trust networks. O'Reilly Media, Incorporated; 2017.
38. Yan X, Wang H. Survey on zero-trust network security. In: Artificial intelligence and security: 6th international conference, ICAIS 2020. July 17-20, 2020; Hohhot, China; pp. 50-60. DOI
39. Buck C, Olenberger C, Schweizer A, Völter F, Eymann T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Comput Secur* 2021;110:102436. DOI
40. Kim D, Kwon BJ, Dumitraş T. Certified malware: measuring breaches of trust in the windows code-signing pki. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security; 2017. pp. 1435-48. DOI
41. Cao Y, Pokhrel SR, ZHU Y, Ram Mohan Doss R, Li G. Automation and orchestration of zero trust architecture: potential solutions and challenges. Elsevier; 2022. DOI
42. Tidjon LN, Khomh F. Never trust, always verify: a roadmap for Trustworthy AI? *arXiv* 2022. DOI
43. Zhou L, Su C, Li Z, Liu Z, Hancke GP. Automatic fine-grained access control in SCADA by machine learning. *Future Gener Comput Syst* 2019;93:548-59. DOI
44. Xiaopeng T, Haohao S. A zero trust method based on BLP and BIBA model. In: 2021 14th international symposium on computational intelligence and design (ISCID); 2021. pp. 96-100. DOI
45. Rousseau TL. Rousseau TL. Insider threat: replacing the trusted security model. Capella University; 2021.
46. Jansen JN, Tokerud S. Jansen JN, Tokerud S. Designing the extended zero trust maturity model a holistic approach to assessing and improving an organization's maturity within the technology, processes and people domains of information security. University of Agder; 2022.
47. Kak S. Kak S. Zero Trust evolution & transforming enterprise security. California State University San Marcos; 2022.
48. Liu N, Yu M, Zang W, Sandhu RS. Cost and effectiveness of trustzone defense and side-channel attack on ARM platform. *J Wirel Mob Netw Ubiquit Comput Depend Appl* 2020;11:1-15. DOI
49. Song M, Wang D. AB-PAKE: achieving fine-grained access control and flexible authentication. *IEEE Trans Inf Forensics Secur* 2024;19:6197-212 DOI
50. He Y, Huang D, Chen L, Ni Y, Ma X. A survey on zero trust architecture: challenges and future trends. *Wirel Commun Mob Com* 2022;2022:6476274. DOI
51. Tian S, Bai F, Shen T, Zhang C, Gong B. Vssb-raft: a secure and efficient zero trust consensus algorithm for blockchain. *ACM Trans Sensor Netw* 2024;20:1-22. DOI
52. Fernandez EB, Brazhuk A. A critical analysis of zero trust architecture (ZTA). *Comput Stand Inter* 2024;89:103832. DOI
53. Botacin M. GPThreats-3: is automatic malware generation a threat? In: 2023 IEEE security and privacy workshops (SPW); 2023. pp. 238-54. DOI
54. Zhao K, Pan L. A machine learning based trust evaluation framework for online social networks. In: 2014 IEEE 13th international conference on trust, security and privacy in computing and communications; 2014. pp. 69-74. DOI
55. El-Sayed H, Ignatious HA, Kulkarni P, Bouktif S. Machine learning based trust management framework for vehicular networks. *Veh Commun* 2020;25:100256. DOI
56. Alanazi R, Aljuhani A. Anomaly detection for industrial internet of things cyberattacks. *Comput Syst Sci Eng* 2023;44:2361-78. DOI
57. Ho S, Al Jufout S, Dajani K, Mozumdar M. A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network. *IEEE Open J Comput Soc* 2021;2:14-25. DOI
58. Saharkhizan M, Azmoodeh A, Dehghantanha A, Choo KKR, Parizi RM. An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. *IEEE Int Things J* 2020;7:8852-59. DOI
59. Takiddin A, Ismail M, Zafar U, Serpedin E. Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids. *IEEE Syst J* 2022;16:4106-17. DOI
60. Alaparthi S, Mishra M. Bidirectional encoder representations from transformers (BERT): a sentiment analysis odyssey. *arXiv* 2020. DOI
61. Gao Q, Wang Y, Cheng X, et al. Identification of vulnerable lines in smart grid systems based on affinity propagation clustering. *IEEE Int Things J* 2019;6:5163-71. DOI

62. Wang WT, Wu YL, Tang CY, Hor MK. Adaptive density-based spatial clustering of applications with noise (DBSCAN) according to data. In: 2015 International Conference on Machine Learning and Cybernetics (ICMLC); 2015. pp. 445-51. DOI
63. Nishikaze H, Ozawa S, Kitazono J, et al. Large-scale monitoring for cyber attacks by using cluster information on darknet traffic features. *Proc Comput Sci* 2015;53:175-82. DOI
64. An P, Wang Z, Zhang C. Ensemble unsupervised autoencoders and Gaussian mixture model for cyberattack detection. *Inf Proc Manag* 2022;59:102844. DOI
65. Kiss I, Genge B, Haller P. A clustering-based approach to detect cyber attacks in process control systems. In: 2015 IEEE 13th international conference on industrial informatics (INDIN); 2015. pp. 142-48. DOI
66. Kumar P, Kumar AA, Sahayakingsly C, Udayakumar A. Analysis of intrusion detection in cyber attacks using DEEP learning neural networks. *Peer Peer Netw Appl* 2021;14:2565-84. DOI
67. Lokhande MP, Patil DD. Trust computation model for iot devices using machine learning techniques. In: Proceeding of first doctoral symposium on natural computing research: DSNCR 2020. Springer; 2021. pp. 195-205. DOI
68. Kumari M, Gupta S. Performance comparison between Chaos and quantum-chaos based image encryption techniques. *Multimed Tools Appl* 2021;80:33213-55. DOI
69. Wu YG, Yan WH, Wang JZ. Real identity based access control technology under zero trust architecture. In: 2021 international conference on wireless communications and smart grid (ICWCSG); 2021. pp. 18-22. DOI
70. Wang Zh, Jin Mh, Jiang L, et al. Secure access method of power internet of things based on zero trust architecture. In: International conference on swarm intelligence. Springer; 2023. pp. 386-99. DOI
71. Sheikh N, Pawar M, Lawrence V. Zero trust using network micro segmentation. In: IEEE INFOCOM 2021-IEEE conference on computer communications workshops (INFOCOM WKSHPS); 2021. pp. 1-6. DOI
72. Tyler D, Viana T. Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. *Appl Sci* 2021;11:7499. DOI
73. Teerakanok S, Uehara T, Inomata A. Migrating to zero trust architecture: reviews and challenges. *Secur Commun Netw* 2021;2021:1-10. DOI
74. Ahmed I, Nahar T, Urmi SS, Taher KA. Protection of sensitive data in zero trust model. In: Proceedings of the international conference on computing advancements; 2020. pp. 1-5. DOI
75. Mehraj S, Banday MT. Establishing a zero trust strategy in cloud computing environment. In: 2020 International conference on computer communication and informatics (ICCCI); 2020. pp. 1-6. DOI
76. Patil AP, Karkal G, Wadhwa J, Sawood M, Reddy KD. Design and implementation of a consensus algorithm to build zero trust model. In: 2020 IEEE 17th India council international conference (INDICON); 2020. pp. 1-5. DOI
77. Garbis J, Chapman JW. Zero trust security: an enterprise guide. Springer; 2021. DOI
78. Vang T, Lind ML. Factors influencing cloud computing adoption in a zero-trust environment. Researchsquare; 2023.
79. Chuan T, Lv Y, Qi Z, Xie L, Guo W. An implementation method of zero-trust architecture. *J Phys Conf Ser* 2020;1651:012010. DOI
80. DeCusatis C, Liengtiraphan P, Sager A, Pinelli M. Implementing zero trust cloud networks with transport access control and first packet authentication. In: 2016 IEEE international conference on smart cloud (SmartCloud); 2016. pp. 5-10. DOI
81. Lookout. Airbus deploys lookout mobile endpoint security to 100,000+ global workforce; 2021.
82. Muncaster P. Capital one breach shines light on cloud security risks, human error, and insider threats. Phil Muncaster; 2022.
83. Mark S, Rachel C. The NASA pathway to zero trust. NASA; 2023.
84. STAMFORD C. Gartner predicts 75fail to implement zero trust security policies through 2026. GARTNER; 2024.
85. D'Silva D, Ambawade DD. Building a zero trust architecture using kubernetes. In: 2021 6th international conference for convergence in technology (i2ct); 2021. pp. 1-8. DOI
86. Bobbert Y, Scheerder J. Zero trust validation: from practice to theory: an empirical research project to improve zero trust implementations. In: 2022 IEEE 29th annual software technology conference (STC); 2022. pp. 93-104. DOI
87. Scott B. How a zero trust approach can help to secure your AWS environment. *Netw Secur* 2018;2018:5-8. DOI
88. Lambert KD. Applications of defense-in-depth and zero-trust cryptographic products in emergent cybersecurity environments. In: Emergent behavior in system of systems engineering. CRC Press; 2022. pp. 93-117.
89. Phiayura P, Teerakanok S. A comprehensive framework for migrating to zero trust architecture. *IEEE Access* 2023;11:19487-511. DOI
90. Adahman Z, Malik AW, Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Comput Secur* 2022;122:102911. DOI
91. Greenwood D. Applying the principles of zero-trust architecture to protect sensitive and critical data. *Netw Secur* 2021;2021:7-9. DOI
92. de Weever C, Andreou M. Zero trust network security model in containerized environments. Amsterdam, The Netherlands: University of Amsterdam; 2020.
93. Bodström TT. Strategic cyber environment management with zero trust and cyber counterintelligence. *J Inf Warf* 2022;21:1-12. Available from: https://www.jinfowar.com/journal/volume-21-issue-3/strategic-cyber-environment-management-zero-trust-cyber-counterintelligence [Last accessed on 23 Sep 2024].
94. DeWeaver III LF. Exploring how universities can reduce successful cyberattacks by incorporating zero trust. Colorado Technical University; 2021.
95. Hatakeyama K, Kotani D, Okabe Y. Zero trust federation: sharing context under user control towards zero trust in identity federation. In: 2021 IEEE international conference on pervasive computing and communications workshops and other affiliated events (percom workshops); 2021. pp. 514-19. DOI

96. Yao Q, Wang Q, Zhang X, Fei J. Dynamic access control and authorization system based on zero-trust architecture. In: Proceedings of the 2020 1st international conference on control, robotics and intelligent system; 2020. pp. 123-27. DOI
97. Anson S. Applied Incident Responsee; 2020. DOI
98. Alappat MR. Multifactor authentication using zero trust. Rochester Institute of Technology; 2023.
99. Yeoh W, Liu M, Shore M, Jiang F. Zero trust cybersecurity: critical success factors and a maturity assessment framework. *Comput Secur* 2023;133:103412. DOI
100. Cheng T, Moore P, Samara-Rubio D, Lee S. Universal wellpad control: an open automation and control platform with zero-trust and zero-touch provisioning system. In: Abu Dhabi international petroleum exhibition and conference; 2022. p. D011S027R002. DOI
101. Sanders G, Morrow T, Richmond N, Woody C, PA CMUP. Integrating zero trust and devsecops. Tech. Rep; 2021.
102. Devlekar S, Ramteke V. Identity and access management: high-level conceptual framework. *Cardiometry* 2022;24:393-99. DOI
103. Ahmed G. Improving IoT privacy, data protection and security concerns. *Int J Technol Innov Manag* 2021;1:18-33 DOI
104. Zakaria KN, Zainal A, Othman SH, Kassim MN. Feature extraction and selection method of cyber-attack and threat profiling in cybersecurity audit. In: 2019 international conference on cybersecurity (ICoCSec); 2019. pp. 1-6. DOI
105. Kato S, Tanabe R, Yoshioka K, Matsumoto T. Adaptive observation of emerging cyber attacks targeting various IoT devices. In: 2021 IFIP/IEEE international symposium on integrated network management (IM); 2021. pp. 143-51.
106. Bout E, Loscri V, Gallais A. How machine learning changes the nature of cyberattacks on IoT networks: a survey. *IEEE Commun Surv Tut* 2021;24:248-79. DOI
107. Adamsky F, Aubigny M, Battisti F, et al. Integrated protection of industrial control systems from cyber-attacks: the ATENA approach. *Int J Crit Infr Prot* 2018;21:72-82. DOI
108. Perera S, Jin X, Maurushat A, Opoku DGJ. Factors affecting reputational damage to organisations due to cyberattacks. *Informatics* 2022;9:28. DOI
109. Dasawat SS, Sharma S. Cyber security integration with smart new age sustainable startup business, risk management, automation and scaling system for entrepreneurs: an artificial intelligence approach. In: 2023 7th international conference on intelligent computing and control systems (ICICCS); 2023. pp. 1357-63. DOI
110. Qazi FA. Study of zero trust architecture for applications and network security. In: 2022 IEEE 19th international conference on smart communities: improving quality of life using ICT, IoT and AI (HONET); 2022. pp. 111-16. DOI
111. Eidle D, Ni SY, DeCusatis C, Sager A. Autonomic security for zero trust networks. In: 2017 IEEE 8th annual ubiquitous computing, electronics and mobile communication conference (UEMCON); 2017. pp. 288-93. DOI
112. Sheridan O. The state of zero trust in the age of fluid working. *Netw Secur* 2021;2021:15-17. DOI
113. Zanasi C, Russo S, Colajanni M. Flexible zero trust architecture for the cybersecurity of industrial iot infrastructures. *Ad Hoc Netw* 2024;156:103414. DOI
114. Xiao S, Ye Y, Kanwal N, Newe T, Lee B. SoK: context and risk aware access control for zero trust systems. *Secur Commun Netw* 2022;2022:7026779. DOI
115. Selim GEI, Hemdan EED, Shehata AM, El-Fishawy NA. Anomaly events classification and detection system in critical industrial internet of things infrastructure using machine learning algorithms. *Multimed Tools Appl* 2021;80:12619-40. DOI
116. GEORGE DAS, George AH, Baskar T, Pandey D. XDR: the evolution of endpoint security solutions-superior extensibility and analytics to satisfy the organizational needs of the future. *Int J Adv Res Sci Commun Technol* 2021;8:493-501. DOI
117. Hassan WU, Bates A, Marino D. Tactical provenance analysis for endpoint detection and response systems. In: 2020 IEEE symposium on security and privacy (SP); 2020. pp. 1172-89. DOI
118. Zaheer Z, Chang H, Mukherjee S, Van der Merwe J. eztrust: network-independent zero-trust perimeterization for microservices. In: Proceedings of the 2019 ACM Symposium on SDN Research; 2019. pp. 49-61. DOI
119. Ali B, Hijjawi S, Campbell LH, Gregory MA, Li S. A maturity framework for zero-trust security in multiaccess edge computing. *Secur Commun Netw* 2022;2022:3178760. DOI
120. Bertino E, Brancik K. Services for zero trust architectures-a research roadmap. In: 2021 IEEE international conference on web services (ICWS); 2021. pp. 14-20. DOI
121. Khan MS, Ferens K, Kinsner W. A chaotic complexity measure for cognitive machine classification of cyber-attacks on computer networks. *Int J Cogn Inform Nat Intell* 2014;8:45-69. DOI
122. Shaukat S, Arshid A, Eleyan A, et al. Chaos theory and its application: an essential framework for image encryption. *Chaos Theory Appl* 2020;2:17-22.
123. Alabdulkreem E, Alotaibi SS, Alamgeer M, et al. Intelligent cybersecurity classification using chaos game optimization with deep learning model. *Comput Syst Sci Eng* 2023;45:971-83. DOI
124. Okumura M, Tomoki K, Okamoto E, Yamamoto T. Chaos-based interleave division multiple access scheme with physical layer security. In: 2021 IEEE 18th annual consumer communications & networking conference (CCNC); 2021. pp. 1-2. DOI
125. Mogos G. Quantum fingerprint scrambling algorithm based on chaos theory. In: 2023 17th international conference on engineering of modern electric systems (EMES); 2023. pp. 1-4. DOI
126. de Lima Marquezino, F., Portugal, R., Lavor, C. Shor's algorithm for integer factorization. In: A primer on quantum computing. Cham: Springer; 2019. DOI
127. Zhang K, Korepin VE. Depth optimization of quantum search algorithms beyond Grover's algorithm. *Phys Rev A* 2020;101:032346. DOI
128. Long GL. Grover algorithm with zero theoretical failure rate. *Phys Rev A* 2001;64:022307.
129. Lavor C, Manssur LRU, Portugal R. Grover's algorithm: quantum database search. *arXiv*; 2003. Available from: https://arxiv.org/abs/

quant-ph/0301079 [Last accessed on 23 Sep 2024].

130. Weinstein YS, Pravia M, Fortunato E, Lloyd S, Cory DG. Implementation of the quantum Fourier transform. *Phys Rev Lett* 2001;86:1889.
131. Martin A, Lamata L, Solano E, Sanz M. Digital-analog quantum algorithm for the quantum fourier transform. *Phys Rev Res* 2020;2:013012. DOI
132. Aaronson S, Rall P. Quantum approximate counting, simplified. In: Symposium on simplicity in algorithms; 2020. pp. 24-32. DOI
133. Szymanski TH. The “cyber security via determinism” paradigm for a quantum safe zero trust deterministic internet of things (IoT). *IEEE Access* 2022;10:45893-930. DOI
134. Perlner RA, Cooper DA. Quantum resistant public key cryptography: a survey. In: Proceedings of the 8th symposium on identity and trust on the internet; 2009. pp. 85-93. DOI
135. Abdolmaleki B, Blümel H, Fenzi G, Khajeh H, KOpsell S, Zarezadeh M. Post-quantum access control with application to secure data retrieval; 2024. Available from: https://eprint.iacr.org/2024/1160 [Last accessed on 23 Sep 2024].
136. Jemihin ZB, Tan SF, Chung GC. Attribute-based encryption in securing big data from post-quantum perspective: a survey. *Cryptography* 2022;6:40. DOI
137. Farouk A, Al-Kuwari S, Abulkasim H, et al. Quantum computing: a tool for zero-trust wireless networks. *IEEE Netw* 2024;1:1. DOI
138. Jiang J, Wang D. QPASE: quantum-resistant password-authenticated searchable encryption for cloud storage. *IEEE Trans Inf Forensics Secur* 2024;19:4231-46 DOI
139. Simpson WR. Toward a zero trust metric. *Proc Comput Sci* 2022;204:123-30. DOI
140. Basta N, Ikram M, Kaafar MA, Walker A. Towards a zero-trust micro-segmentation network security strategy: an evaluation framework. In: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium; 2022. pp. 1-7. DOI
141. Xiaojian Z, Liandong C, Jie F, Xiangqun W, Qi W. Power IoT security protection architecture based on zero trust framework. In: 2021 IEEE 5th international conference on cryptography, security and privacy (CSP); 2021. pp. 166-70. DOI