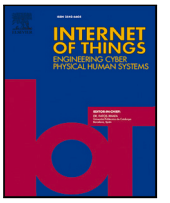
Internet of Things 27 (2024) 101227

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot



Verify and trust: A multidimensional survey of zero-trust security in the age of IoT

Muhammad Ajmal Azad [a,*], Sidrah Abdullah [b], Junaid Arshad [a], Harjinder Lallie [c], Yussuf Hassan Ahmed [a]

[a] Birmingham City University, United Kingdom
[b] NED University of Engineering and Technology, Pakistan
[c] University of Warwick, United Kingdom

ARTICLE INFO

Keywords:
Blockchain
Zero-trust architecture
Authentication and authorization
Policy-based authorization

ABSTRACT

The zero-trust (ZT) model assumes that all users, devices, and network traffic should not considered as trusted until proven. The Zero-trust model emphasizes the importance of verifying and authenticating every user and device, and limiting access to resources based on the principle of least privilege. Under the principle of the zero-trust model, devices are granted access after they have been successfully presented with their authentication credentials and access rights based on different factors, such as user identity, device health, location, and behaviour. Access controls are then continuously evaluated and updated as user properties, locations and behaviour change. The zero-trust model can be applied in various domains (healthcare, manufacturing, financial services, government etc.) to provide a comprehensive approach to cybersecurity that helps organizations to reduce risk and protect critical assets. This paper aims to provide a comprehensive and in-depth analysis of the zero-trust model, its principles, and its applications, as well as to propose recommendations for organizations looking to adopt this approach. We explore the major components of the zero-trust framework and their integration across different practical domains. Finally, we provide insightful discussions on open research issues within the zero-trust model in terms of the security and privacy of users and devices. This paper should help researchers and practitioners understand the importance of a zero-trust framework and adopt the zero-trust model for effective security, privacy, and resilience of their networks.

1. Introduction

The use of IoT devices is rapidly growing, and with that growth comes new cybersecurity risks. It is estimated by IDC that there will be more than 41 billion IoT devices in use worldwide and a large number of people who are using IoT devices reported they are concerned about the security and privacy of their IoT devices [1]. These statistics show that while the growth of the IoT industry presents many opportunities for innovation and convenience, it also creates significant cybersecurity risks. Data breaches are becoming increasingly expensive, with the global average cost reaching a staggering $4.45 million in 2023. This represents a significant 15% increase compared to just three years ago [2]. Cybersecurity Ventures predicts cybercrime's annual cost will explode to $10.5 trillion by 2025 [3]. These statistics show that cyber-attacks are a significant and growing problem that can have

* Corresponding author.
E-mail addresses: muhammadajmal.azad@bcu.ac.uk (M.A. Azad), hsabdullah0@gmail.com (S. Abdullah), junaid.arshad@bcu.ac.uk (J. Arshad), hl@warwick.ac.uk (H. Lallie), yussuf.ahmed@bcu.ac.uk (Y.H. Ahmed).

https://doi.org/10.1016/j.iot.2024.101227
Received 15 January 2024; Received in revised form 1 April 2024; Accepted 15 May 2024
Available online 27 May 2024

significant financial and reputation consequences for individuals and organizations. It is important to take steps to protect digital assets using strong authentication and access control mechanisms. Traditional authorization mechanisms, such as usernames and passwords, are increasingly vulnerable to cyber-attacks [4,5]. In a traditional security model, once a user, device, application or process is granted access to a network or resources, they are often given free access to everything within the network without further tracking the user's actions or location. This model assumes that everything inside the network is trusted, and as a result, makes it easier for cybercriminals to move laterally within the network once they have breached the perimeter defenses. When these mechanisms are compromised, cybercriminals can gain unauthorized access to sensitive data and resources. In contrast, the zero-trust framework is designed to minimize the risk of cyber-attacks by continuously verifying and authenticating users, devices, and applications. Zero-trust framework improves the security posture of the organization by dynamically verifying the authorization and access control rights of users, devices, applications and processes, reducing the risk posed by the insider and imposing better compliance mechanisms. The implementation of a zero-trust model would help to reduce the risk of cyber-attacks and data breaches thus saving organizations from financial losses and reputation damage.

The zero-trust model is becoming increasingly popular as organizations seek to improve their cybersecurity posture in the face of evolving threats. By assuming that all users, network devices, and applications are untrusted until proven trusted, the zero-trust model can help to reduce the attack footprints and minimize data breaches by continuously verifying and authenticating users, devices, and applications in a dynamic environment [5,6]. The zero-trust focused on restricting resource access and granting access on the principle of the least privileges required to perform the desired function. An operative definition of zero trust is that it is a security model that requires continuous verification and authentication of all users, devices, and applications before granting access to resources. Zero trust is a comprehensive security framework and operational policies that implement the zero-trust model across an organization's entire network, to minimize the risk of cyber-attacks and data breaches [7]. Zero trust is important because traditional security models, such as perimeter-based security, are no longer effective in today's complex and constantly evolving threat landscape. With the rise of distributed cloud computing, mobile and IoT devices, remote work and the implementation of Bring your own device (BYOD) scenario, the traditional security perimeter has become increasingly penetrable, making it a lucrative choice for cybercriminals to infiltrate networks and steal sensitive data for fun and profit. However implementing a zero-trust network within a heterogeneous network is very challenging because of complexity, interoperability, implementation cost, user experiences, and a huge number of management and access policies. To successfully implement a zero-trust approach, organizations need to evaluate the architecture of their network, technologies used, access policies, and scale of BYOD devices in a dynamically changing environment.

There may be fewer existing works on zero trust compared to more established topics in cybersecurity [8,9]. Zero Trust has the potential to be a strong security model, but more needs to be done to understand its technical foundations, organizational deployment issues, large-scale network compatibility, and how well it can secure businesses and the expanding IoT device landscape [4]. Christoph et al. [9] provide a comprehensive perspective on zero-trust covering academic literature and the standard guidelines, however, this work did not cover the implementation setups of zero-trust systems. Naeem et al. [8] evaluate the encryption, segmentation and network management methods used within the Zero trust system, however, the research did not address the challenge of implementing zero trust in a diverse heterogeneous network. Furthermore, the existing literature did not evaluate the zero-trust system along with the authentication mechanism, architectural setup and authorization policies. Furthermore, the MITRE framework has also not been used to evaluate different ZT models. There is a strong requirement for a systematic review of the zero-trust system that addresses the authentication, authorization and architectural setup along with the implemented domains. In this paper, we present a comprehensive survey on the fundamentals and importance of a zero-trust framework for the heterogeneous enterprise network. We address key challenges such as methods proposed for authentication and authorization, architecture setups for implementation and domains for which these systems have been proposed. By discussing existing solutions, this systematic survey provides critical insights and guidelines for academics to understand the zero-trust model in the diverse heterogeneous domains and networks. The survey also offers useful technical guidance to the network administrator and security practitioners for better understanding and implementation of the zero-trust framework for their organization. We believe this is the first attempt to investigate and review the zero-trust model in diverse domains. The contributions of this survey are four-fold.

- We discuss the fundamental principles and characteristics of the architecture of the zero-trust model, key features the zero-trust model provides over traditional authentication systems and enabling technologies.
- We investigate the scope of the zero trust framework in different aspects i.e. authentication, authorization, access control, security, privacy, data management etc. and discuss the critical challenges to address them.
- We review the most recent security and privacy defences being developed in academia and business, and we talk about how feasible they are for creating resilient, secure and privacy-preserving zero-trust models.
- We present open future research directions and questions for developing efficient, secure, and zero-trust models.

1.1. Paper selection methodology

To conduct this multi-dimensional literature survey, a qualitative methodology is followed to analyse and synthesize the existing works. We identified the main requirements of ZTA, its implementation domains, threats, threat vectors and threat agents, attacks and sources of attacks, design challenges specific to the domain and limitations related to Zero-trust security models. Our methodology consists of the following steps:

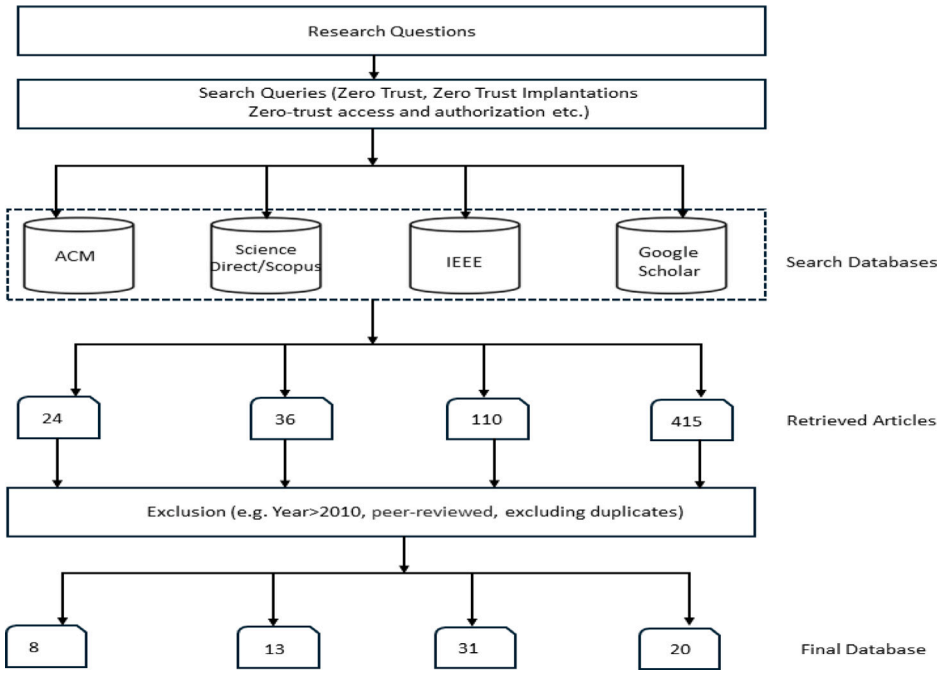


Fig. 1. Review workflow.

- We select the following digital libraries: ACM Digital Library, IEEE Xplore, Science Direct and Scopus. We also used Google Scholar to find the relevant study across other databases. Fig. 1 reports workflow of our review. First, we used the basic query i.e. Zero trust architecture, zero trust models, and zero trust frameworks to understand the architecture and working mechanism of the ZTA, and then we used some advanced queries to focus on the security aspects of ZTA. Specifically, we used queries like Zero trust security, zero trust model, zero-trust network segmentation, zero trust authentication and authorization, policy enforcement in Zero Trust models, zero trust for IoT and cloud networks, and blockchain implementations with zero trust.
- The objective was to select scientific contributions on security aspects and secure implementation of zero-trust models. We used the following criteria for the paper inclusion: papers focus on the security aspects of ZTA, it can be architecture, implementation or technology, and papers published in a peer-reviewed scientific journal and conference from 2010 onwards. The following exclusion criteria have been used: studies which are just a variant of commercial implementation of ZTA, studies which do not define the functional component of ZTA implementation and studies that are not published in the English language. Finally, we classify all the articles based on architecture, implementation domain and working architectures.
- After applying the inclusion and exclusion criteria, we selected 72 papers for the final analysis, including some supporting papers to support our arguments. The selected literature is then divided into different groups the first group contains the architecture used to propose the ZTA. We analysed the contributions in 3 dimensions, cloud-based implementation (19 contributions), IoT-based implementations (20 contributions) and blockchain-based implementations (12 contributions). The second group reviews the literature related to authentication (7 contributions) and authorization (12 contributions) and the third group is the implementation domains while focusing on segmentation, architecture, domain, and analysis.

1.2. Survey structure

This paper covers the systematic literature review of the Zero-Trust approach. Fig. 2 shows the outline of the paper. In addition Table 1 contains a list of the abbreviations used in the article. We begin by providing the background on the ZTA in Section 2, Section 3 discusses the requirements for the zero-trust and application of MITRE ATT&CK framework. Section 4 describes the different architecture frameworks of the zero-trust models. Section 5 discusses the adoption of zero-trust in practical environments. Section 6 discusses the authentication, authorization and access control mechanisms adopted in Zero-trust. Section 7 provides a comprehensive discussion on the implementation domains of the Zero-trust framework. Future research challenges are identified in Section 8. Section 9 concludes the paper.

2. Background

In this section, we introduce the zero-trust framework, its general architecture, key characteristics, and potential applications.

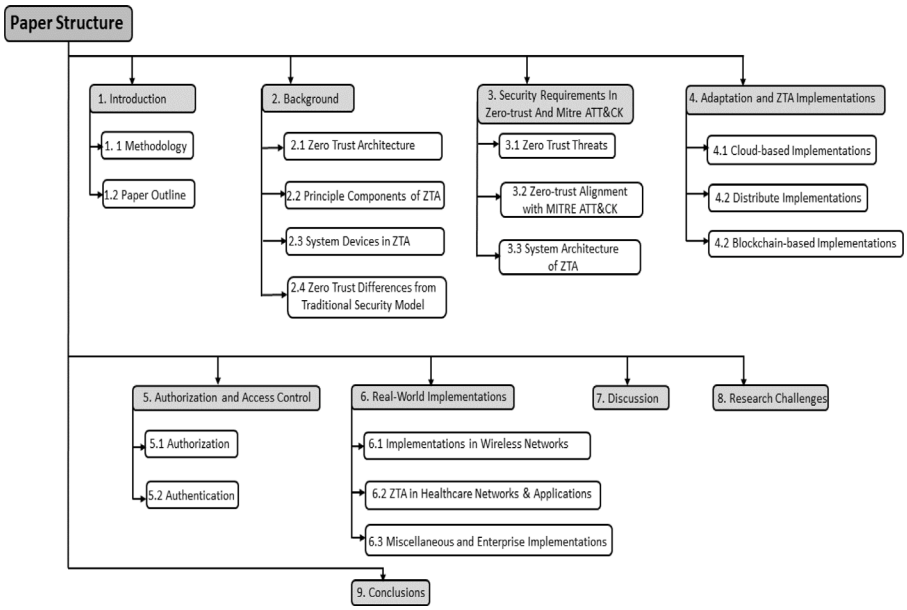


Fig. 2. An overview of the structure of the paper.

Table 1
List of important abbreviations.

Abbreviation	Definition	Abbreviation	Definition
ZT	Zero-trust	VPN	Virtual Private Network
ZTA	Zero-trust Architecture	AI	Artificial Intelligence
PDP	Policy Decision Point	ML	Machine Learning
PEP	Policy Enforcement Point	PA	Policy Administrator
BYOD	Bring Your Own Devices	IoT	Internet of Things
PE	Policy Engine	ICS	Industrial Control Systems
DAC	Discretionary Access control	MAC	Mandatory Access Control (MAC)
RBAC	Role-based Access Control	IAM	Identity and Access Management
ABAC	Attributed-based Access Control	PBAC	Policy-based access control
MFA	Multi-factor authentication	ACL	Access control lists
IDS	Intrusion Detection Systems (IDS)	IPS	Intrusion Prevention Systems
SCADA	supervisory Control and Data Acquisition	UCON	Usage Control
Paas	Platform as a Service	SaaS	Software as a Service
HIPPA	Health Insurance Portability and Accountability Act	GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office	DOS	Denial-of-service
IR	Incident Response	ABE	Attribute-based Encryption

2.1. Importance of zero-trust

Zero Trust aims to improve the security of networks while assuming that all network traffic, devices, applications, and processes are potentially malicious and untrusted. This security approach constantly verifies everything, inside or outside the network, to minimize cyber risks and improve data and network privacy. Zero Trust grants access to users on the principle of least privileges. Users and devices only get the minimum access to resources and data required to do their jobs. This minimizes the damage if something gets compromised. Through ZT organizations can allocate resources and data more securely, effectively and dynamically while considering the changing behaviour of users, devices, processes and applications. Perimeter security can be used to protect networks and users by creating a boundary between the internal and the external networks, using firewalls, intrusion detection and prevention systems, and other security devices [10,11]. This approach assumes that everything within the network is trustworthy and that cyber threats mainly originate from external actors and considers internal users as honest and trustworthy. Within this setup, if the user has been granted access, then it could be considered trustworthy during its communication lifetime. However, insider threats are reported to be responsible for a significant portion of cyber incidents. According to a Cybersecurity Insiders report there is a rise of around 47% in the attacks from insiders from 2022 to 2024 with 34% of the businesses affected globally [12]. The financial impact due to insider attackers is also significant. The average cost estimated for an insider threat incident in 2023 is $15.38 million [13]. To protect the systems, networks and devices from malicious traffic, we need a system of constant vigilance, scrutinizing every access request and dynamically adjusting permissions based on the perceived trustworthiness of the access attempt [14]. This is achieved through continuous monitoring and analysis of user and device behaviour, network traffic, and other contextual information. ZT

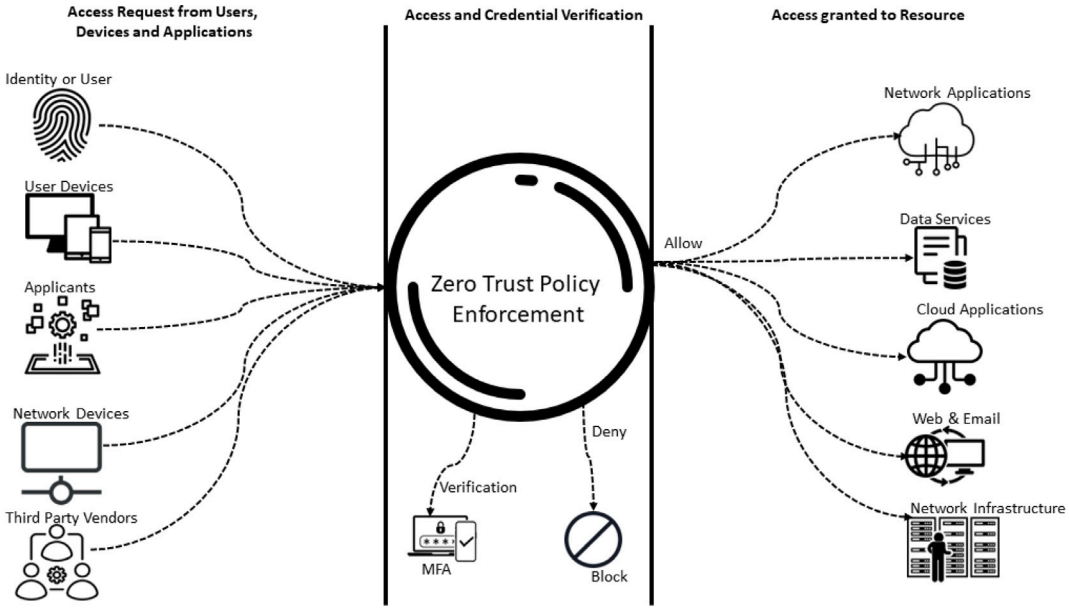


Fig. 3. Zero trust security model.

actively detects and stops malicious or suspected users before they can access and manipulate sensitive data by moving security controls to the point of access. By carefully analysing user behaviour and device IDs along with the dynamic authorization policies, it ensures that only permitted access is granted [15] to the users and devices. This approach emphasizes the importance of identity and access management and focuses on minimizing the attack surface considering the least privileges to grant access. In the continuously changing mobile environment where end-users can bring and use their mobile devices to access the organization's most critical data. In this emerging communication model, perimeter security would not provide effective classification between legitimate and malicious users and applications. Perimeter security solutions can be inflexible, making it difficult to adapt to changing environments or emerging threats [16–19]. For example, if a new attack vector emerges that is not covered by the perimeter security solution, it may take time to update the security posture to address the new threat. In contrast, ZT provides a more comprehensive and adaptable approach to security, enabling organizations to secure their networks and data regardless of location, time, attributes, device type and changing roles.

The idea behind the zero trust framework is that organizations should not automatically consider devices, users and traffic trustworthy whether they are insiders or outsiders. Fig. 3 presents the security model of the Zero-trust. A trusted centralized entity is required for authentication, authorization and enforcement of the policies to users, devices and network traffic [14,20]. The trusted entity accepts the request from the users and devices and decides whether access is to be granted or not. In some circumstances and based on policies the central entity could ask for further credentials [21,22]. The ZT makes access control decisions based on authenticating the identity of both the subject and the resources requested by the subject. Access rights can be granted, modified, or revoked based on the behavioural properties of the resource as well as the subject requiring access. Within this context, resources can be accessed based on the user's environment, access patterns, and other factors.

2.2. Requirements for ZTA

Organizations can create a universal and dynamic security approach by utilizing the Zero-trust framework, which can detect and mitigate malicious traffic and users in a real-time. This helps to minimize the attack surface, prevent data breaches, and improve the overall security posture of the organization. The network needs to deploy clear policies for authentication, authorization and data management. To maintain network integrity, confidentiality and availability of network resources, any request that does not match these requirements is blocked at the edge of the network. The following are the essential components of the zero-trust.

Identity Authentication: Identity is used to establish trust between users and the network resources they are trying to access. This is established by verifying the identity of users, devices, and processes and enforcing access policies based on their credentials and rights. The first step in Zero Trust is to identify and classify all devices, users, and applications that require access to the organization's resources. This includes understanding their roles, responsibilities, and data access requirements. In a zero-trust, identity verification and authentication plays an important role that only authorized users, entities and devices could access devices, data and information resources. There can be many identity authentication mechanisms that can be used in a zero trust framework, including password-based authentication, Multi-factor authentication (MFA), Identity and Access Management (IAM), use of public key infrastructure, user behaviour and device usage, user bio-metrics or other device characteristics etc [23,24]. In zero-trust, identity

verification and monitoring is a dynamic and continuous process. Users and devices are constantly monitored for their behaviour that could indicate a security threat. This helps to detect and prevent unauthorized access and data breaches from external and internal sources at the early stage of their malicious behaviour.

Network Segmentation: Network Segmentation is an important component of the zero-trust. It involves dividing an organization's network into smaller, more secure micro-segments or zones. Each segment is separated from other segments by deploying traditional security control mechanisms such as firewalls, access controls, demilitarized zones and other security mechanisms. Segmentation would help limit the impact of a security breach on that network segment attacked by the attacker [25,26]. If a particular part of the network is being affected by malicious traffic or cyber-attack then with segmentation, it is unlikely that the malicious actor has access to other segments to increase his footprint, as each segment is isolated and protected by its security controls and policies. In ZTA, segmentation is implemented through the creation of micro-perimeters around individual applications, network components, network perimeters, or services, which are then protected by specific access controls and security mechanisms. For example, within an IoT network the ZTA segmentation can be implemented by creating the micro-segments and enforcing the segmentation policies at the device, fog or edge level of the network [27,28]. The paradigm of software-defined networking can also be used to implement the ZTA segmentation [29–31]. This is because software-defined networks have complete control over network traffic flow, aligning perfectly with ZT's approach of isolating resources and minimizing trust. SDN-based implementation would automatically revoke access for a compromised device or adjust access levels based on a user's location or time of day [32–34].

Authorization: Authorization is an important component not only in the traditional IP networks but is also responsible for enforcing access control in a zero-trust. The authorization process makes sure that only trusted, verified and authorized users, devices, processes, and applications can use the network resources. Zero-trust requires that access to resources is managed and granted dynamically, based on the principle of least privilege, and further access is continuously verified before it is granted or revoked. Policies are created and enforced through policy-based access control mechanisms. There are several different ways to implement and enforce authorization policies in a zero-trust. Access control lists (ACLs) are widely used in the perimeter network to block unauthorized users at the edge of the network. The ACL within the zero-trust can be deployed and enforced at the segment or zone level [35–37]. Authorization can also be implemented through a role-based access control mechanism where access is granted based on the user's role within the organization [38–41]. Zero trust authorization can also be implemented using attribute-based access control (ABAC). In ABAC system users and entities can access network and information resources based on their unique attributes, such as their role, their location, or the type of device they are using [42,43]. Another way to enforce policies in ZT is to use the policy-based access control mechanism which involves defining access policies for a specific resource and then enforcing policies in a dynamic way based on the user's identity, user devices, location, and other important factors [44,45].

Encryption: Since integrity and confidentiality are very important for users and malicious actors can monitor their target communication messages, therefore ZTA works under the principle of least privilege and zero trust. To stop malicious access and data leaks, ZT continuously confirms the identities of users and devices as well as their access permissions. To ensure the integrity and confidentiality of communication, Encryption is used to protect data at various stages of its life cycle within the zero-trust. In a zero-trust, data needs to be protected at three stages, data at rest, in transit, and in processing. In permanent storage, such as disks or servers, data is static and at rest. When data is in transit, it is moving through networks between users and devices. Data in use is actively being processed by CPUs or other computational units. Within the Zero-trust framework encryption can be implemented in two modes, end-to-end encryption i.e., encrypting, and decrypting data at the end devices, and point-to-point encryption where each intermediate device is involved in encrypting and decrypting the exchanged data. Encryption can be used to enforce access controls. For example, an organization might require that all data be encrypted before it is transmitted over the network. This would help to prevent unauthorized access to the data, even if the network is compromised. The implementation of encryption approaches varies from setup to setup for example within an IoT environment the cryptographic mechanisms should be lightweight to deploy at the resource-constrained devices [8,46,47], should have small processing overhead and latency and have deployed efficient key-management system for large-scale IoT deployments and dynamic environment where users attribute changes continuously and dynamically [48,49].

Network Monitoring: Today's networks are complex and consist of heterogeneous devices, networks, applications and traffic sources which require a real-time response under a massive traffic rate. Continuous network monitoring in a zero-trust framework involves collecting and analysing a huge amount of data from a large number of different sources, including network logs, user devices, user behavioural patterns and interaction logs and operating system events. This data is used to detect potential security threats in real-time using advanced machine learning, event correlation and artificial intelligence [50]. Real-time monitoring would bring a lot of benefits for the organization as it helps to identify potential security incidents early on and would identify and block malicious users and devices. This would also improve the overall security posture of the organization and minimize the risks posed to the organization due to the emerging and continuously changing environment. Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems (IPS) have been widely used systems to monitor the network traffic for unauthorized access and stop them from unauthorized access [51,52]. Within the Zero-trust framework, IDS can be deployed at the network level, at the edge level, at the device layer, in the hybrid mode or can operate collaboratively as well [53,54]. ZT minimizes the attack surface by granting users and devices only the minimum permissions necessary for their specific tasks. This principle of least privilege significantly restricts actions and movement, thwarting adversaries even if they gain initial access [55].

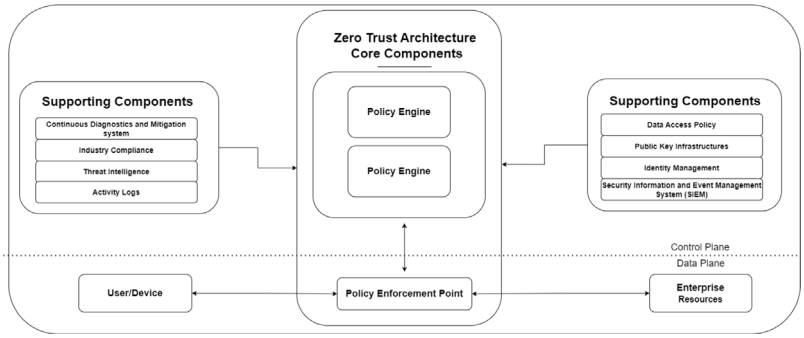


Fig. 4. Components of NIST zero trust architecture [56].

2.3. Components of zero-trust architecture

ZT works on the principle of verifying the devices before granting access to critical data, information or network resources of the organization. This can be achieved through proper policy definitions, characterization and profiling of users and devices. This definition would allow us to make access control decisions and policy enforcement based on defined policies. To address this NIST proposed three logical components for Zero Trust Architecture (ZTA) [7,56] as represented in Fig. 4:

Policy Decision Point (PDP): PDP is an important component of the Zero Trust Architecture (ZTA) and is responsible for making the access control and authorization decision based on the policies defined for the users, networks, devices, process, and the IP traffic type. The access control decision is made in a real-time and dynamic way while considering the relevant properties of devices or users. PDP is responsible for implementing and enforcing the policies (rules, contextual information, behaviour of user, type of device and risk assessment factors). The PDP also decides what level of access privileges should be granted to a particular user, device, or application based on the defined policy rules. PDP does not enforce policies itself; it contacts the Policy Enforcement Point (PEP) with its decision, which is responsible for enforcing the access control decisions made by the PDP. In a ZT, the PDP should be implemented as a centralized component that receives access requests from various sources, such as users, devices, applications, or network resources. The centralized system can be a single point of failure or a single point of attack therefore measures should be taken to implement the PDP as the redundant mode or adopt the decentralization or distrusted systems to implement the functionality of PDP [57–59]. The PDP also maintains a log of all access requests and decisions for auditing and compliance purposes. Policies can be grouped into two groups: low-level policies and high-level policies [60]. The low-level policies are typically implemented at a granular level defining which users, devices, or applications are allowed to particular resources under what conditions and high-level policies provide the way how to implement and enforce the low-level policies.

Policy Enforcement Point (PEP): The PEP is responsible for implementing the access control decisions made by the PDP. The PEP can be a physical device, a software component or a process that runs on a server and enforces the decision communicated by the PDP. The ideal location for PEP should be near the device, and the user who requires access as it minimizes the access delay for a user to the particular resource [61]. The PEP system should be scalable as the number of resources and devices within the network increases over time and the PEP needs to handle the growing network of devices and resources.

Policy Administrator (PA): The PA acts as the gatekeeper, managing the connection between resources and the subject which wants access. The PA is closely working with the policy decision point and relies on their decision to ultimately allow or deny a session. The PA is also responsible for issuing authentication tokens or credentials used by a user to access an enterprise resource. The PA is also responsible for policy enforcement and closely communicates with the PEP to enforce control policies at the network and application levels. The PA is normally implemented at the same level as of PDP.

2.4. How zero trust differs from traditional security models

Perimeter-based security is a widely used traditional security model that uses security controls such as firewalls, intrusion detection systems, data loss prevention, and virtual private networks (VPNs) at the edge of the network to protect the network from the malicious and untrusted actors [62]. The perimeter-based security creates a secure boundary around the network of devices and monitors the behaviour of the threat agents at the entry point. Fig. 5 presents the reference model for perimeter-based security to secure the network primarily from outsiders. The network can be divided into different functional components by using firewalls, intrusion detection systems and demilitarized zones to ensure the security of network resources, especially from outsiders. One of the bottlenecks of this approach is that it assumes that all users who are inside the network are trusted users while considering network traffic coming from outsiders as an untrusted [63,64]. However, an Insider (disgruntled employee, untrained user or former employee) could cause serious privacy and security threats to an organization which can have significant financial, reputational, and legal consequences. It has been estimated that insiders were responsible for 30% of all data breaches which could cause an organization a loss of around $11.45 million. Perimeter-based security also assumes that access control and authorization should be made based on user location, type of device and device authorization, however with networks such as Bring your OWN Device

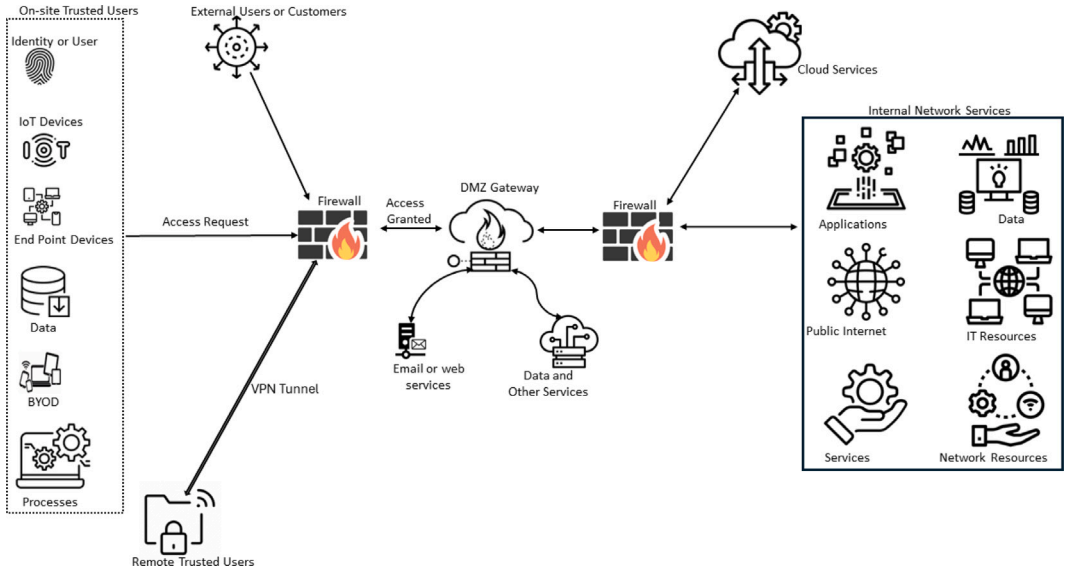


Fig. 5. Traditional security architecture.

(BYOD), IoT and cloud-based technologies user location is not a reliable indicator for trustworthy behaviour [65]. Perimeter-based security operates in the reactive mode and responds to security incidents after their occurrence which makes it less effective in the evolving heterogeneous networks. Perimeter-based security would not provide an effective defence against stealthy attacks such as low rate Dos or DDOS attacks, reflection and amplification attacks [66]. Another limitation of perimeter-based security is that it does not evolve itself to a dynamically changing environment, therefore the solution needs to be updated manually or completely replaced to protect the network from new emerging attacks. This can be a costly and time-consuming process [67]. Scalability is also difficult to implement and manage as organizations grow and become more complex with the use of more heterogeneous networks and devices.

ZTA, on the other hand, is a security control mechanism that assumes that all network devices, users, applications, and processes should be considered untrusted regardless of whether these devices and users are insiders or outsiders to the organizations. Fig. 6 presents the system architecture of ZT for the enterprise networks. This architecture is based on the principle of least privilege and relies on several security measures for its functions such as multi-factor authentication, attribute-based, role-based or policy-based access control, device level or gateway level device policies, and continuous monitoring of traffic passing through the network [68]. This would ensure that all network traffic, devices, identifies, processes, data and users are inspected, and verified before granted access regardless of their location, device type and data. Compared to perimeter-based security, implementing ZT brings more flexibility and allows users to access the network from any location while ensuring fundamental security properties such as confidentiality, integrity and availability. It provides strong zero-day security against sophisticated attacks originating from internal or external users [68]. This is because ZT assumes all devices, traffic, and users are untrusted unless proven trusted while evaluating the policies defined for users and devices. ZT is adaptable and easily evolves to provide effective security for emerging networks which are cloud-based heterogeneous and mobile, and use a large number of resource-constrained devices. This can be achieved while implementing policy enforcement and policy decision functions near the device and at the edge of the network. This brings another advantage of decentralized security measures without incurring additional communication delay and latency. ZT does have some drawbacks, too, like the fact that it requires some changes in the existing network to deploy several additional devices and is difficult to build and manage.

3. How zero-trust ensures security requirements of MITRE ATT&CK framework

Zero-trust strict access control, continuous monitoring, and multifactor authentication reduce the risk of cyber attacks. However, zero-trust security is not foolproof and can still be vulnerable to certain threats. In this section, we present a discussion on zero-trust threats and their alignment with the MITRE ATT&CK framework.

3.1. Threats to zero-trust framework

Modern information systems are dynamic, which facilitates ongoing learning and development. This includes addressing technical limitations, enhancing user experience, and exploring how human interaction can be more intuitive. Adversaries use these weaknesses to attack businesses for financial benefits or competition. Effective defences against modern attacks require a detailed analysis of the attack footprint adversaries are using to maliciously affect the organization. Finding out the attack surface helps

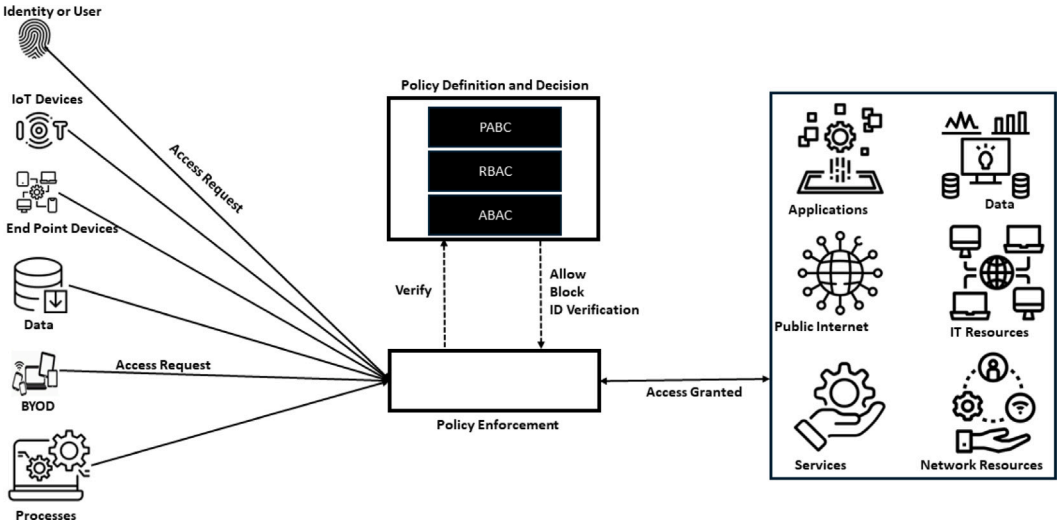


Fig. 6. High-level zero trust architecture.

organizations and enterprises identify a suitable defence mechanism to protect the network from malicious activities. This section presents components which are at cyber risk due to ZT paradigm.

User Credentials: Attacker finds ways to target the user credentials to access the sensitive information that can be used for financial benefit or compromising important assets of the organization. Attackers can attempt to gain unauthorized access to these accounts by exploiting vulnerabilities in the authentication and authorization process. Attackers can use various techniques to steal or compromise user credentials, including Phishing attacks, Credential stuffing, Password cracking, social engineering, default and commonly used credentials etc.

Internet of Things (IoT) devices: Over the years, IoT devices have seen massive deployment across organizations for many value-added services. These IoT devices are resource devices, can use different communication mechanisms and can also be managed by different vendors and service providers. IoT devices that are connected to the network can be exploited by attackers. IoT devices can be vulnerable to attacks such as botnets, malware, and ransomware [69,70]. IoT networks and resource-constrained devices can be vulnerable to various security threats, including botnets, malware, physical attacks, and Weak or default passwords.

Policy Definition and Policy Enforcement Points: In a zero-trust security model, policy decisions and policy enforcement are critical components for ensuring that access to sensitive information and systems is controlled and secured. PDPs are responsible for making access control decisions and PEPs are responsible for enforcing access control decisions. Together, PDPs and PEPs work to ensure that access to sensitive information and systems is only granted to authorized users and devices. Robust security around PDPs, PEPs, and the PE is crucial. Any one of these essential elements being compromised has the potential to make business services unavailable for legitimate users and provide access to manipulated or exfiltrated data. To implement a zero-trust security model effectively, it is important to ensure that policies are consistently enforced across all systems and applications and require protection from outages and cyber-attacks. The commonly used attacks that can compromise the functionality of PDP and PEP are Spoofing attacks, Denial-of-service (DoS) attacks and Privilege escalation attacks.

Third-party applications and services: Many organizations use third-party applications and services to manage various aspects of their business, such as HR systems, network management, outsourcing of some monitoring functions, and cloud-based storage solutions. However, these third-party solutions can also introduce security vulnerabilities into an organization's IT environment. Third-party applications and services can also be exploited by attackers. These applications can be used as a gateway to the network, giving attackers access to sensitive data and systems. The partners and vendor also require access to network resources of the organization such as intellectual property rights, important documents etc. These actors could also bring harm to the network assets of the organization or even steal confidential information.

Cloud-based Threats: As many organizations are migrating to Cloud-based systems and services for various tasks such as data-hosting or the use of computation devices. While cloud-based systems offer many benefits, such as scalability and flexibility, they can also introduce security vulnerabilities into an organization's IT environment. Cloud-based systems are a major component of network functionality and are an increasingly popular attack surface in a zero-trust security model as well. Some potential attack vectors against cloud-based systems include Account hijacking, Data breaches due to external or internal actors, misconfigurations, zero-day vulnerabilities and Malware.

Physical access: Organizations build physical security around sensitive devices and systems. Access control, surveillance security cameras, and sturdy perimeter fences work together to deter and detect intruders, keeping data and infrastructure safe. However, vulnerabilities in these systems can be another potential attack surface in a zero-trust security model. Attackers can gain access to devices or systems through various means, including social engineering, physical theft, or by exploiting vulnerabilities in physical security measures.

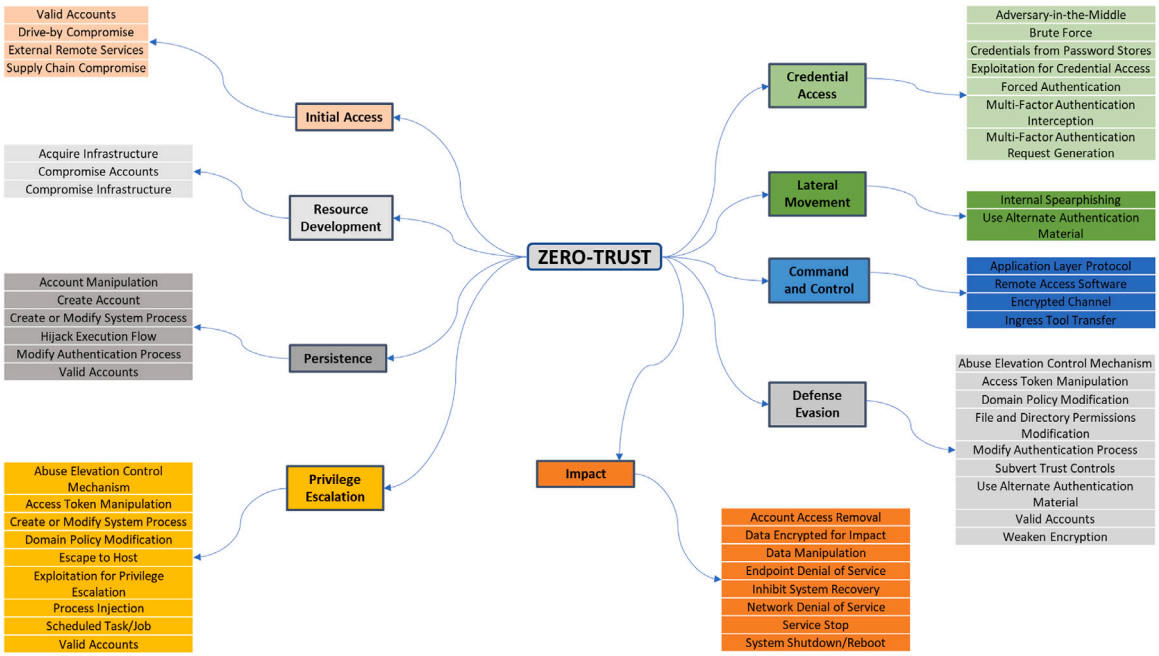


Fig. 7. Zero-trust with MITRE ATT&CK alignment.

Monitoring and Examination of the Network's Traffic: By analysing the network traffic, adversaries can learn about sensitive information about users as well as organization secrets. This would impact the confidentiality and integrity of users and organization data. Through traffic, analysis organizations can also detect and prevent potential threats, such as malware infections, data exfiltration, or unauthorized access to sensitive systems. Some potential attack vectors against monitoring and examination of network traffic include Encryption, Evasion techniques and Insider threats.

3.2. Zero-trust alignment with MITRE ATT&CK

The threats to zero-trust models can be aligned with the widely used threat knowledge based like MITRE ATT&CK framework as it provides a common language for discussing the methods, approaches and tactics adopted by attackers to breach the networks and help organizations to develop effective defence strategies against these attacks. By using the MITRE ATT&CK framework, organizations can gain a better understanding of the different types of threats they may face and how these threats could impact their operations. They can use this information to develop more effective threat detection and response strategies and to better prepare for potential attacks. The MITRE ATT&CK framework consists of 12 categories of mechanisms that are commonly used by attackers during cyber-attacks which are then subdivided into further-level attack mechanisms executed by the attacker. These categories are Initial Access, Execution, persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. The MITRE ATT&CK framework focused on three main application domains: Enterprise, this domain focused on techniques used to compromise traditional enterprise networks, including endpoints, servers, and cloud-based services. The mobile domain focuses on techniques used in mobile environments, including mobile devices, applications, and operating systems and the Industrial Control System (ICS) which covers the techniques used to attack industrial control systems, SCADA or cyber–physical systems. In Fig. 7, we mapped the techniques that are relevant to zero-trust models in the domain of enterprise security and industrial control systems. The first category presented in Fig. 7 is Initial Access which is the combination of different approaches used by the threat agents to gain access to the target system, device or network. This step is the first step in the attack process and once the attacker gains initial access, they can try other tactics to compromise the security and privacy of the network or systems. In this aspect, we validate accounts, drive-by-compromise, external services and supply chain compromise to allow an attacker to disturb the communication and compromise the network resources in an unintended way. Phishing can also be used to access resources; however, the continuous monitoring process of the zero-trust approach could provide a timely defence. Within ZT, users only have access to the specific resources they need, limiting the potential impact of a successful initial access attempt. Furthermore, the micro-segmentation also limits the attacker's capability to compromise the larger footprint of the network.

The second attack tactic is Resource Deployment. Resource Deployment is the technique used by the attacker to deploy and maintain their tools and infrastructure within the victim system and network. It is the essential component for maintaining persistent access to the target network resources. In this category, we model compromise accounts, compromise infrastructure, and acquire

infrastructure as the most important threat to zero-trust-based security systems. Zero Trust can leverage application control policies and the principle of least privileges to restrict the execution of unauthorized software or scripts, potentially blocking malicious payloads from execution and blocking malicious actors.

The third category we incorporated is Persistence which refers to various techniques used by the attacker to maintain continuous access to the system or network even after they have been detected, blocked and removed from the system. Here, we consider modifying the access credentials, creating accounts with full privilege rights, modifying the account and processes or even modifying the authentication process. The creation of a new valid account would provide persistent access to the attacker. Zero Trust focuses on assuming that every user and device is untrusted and requires continuous verification and validation of their identity and access rights therefore, zero trust could provide an effective defence against persistent access only if it is properly implemented. Next, we considered Privilege Escalation which refers to a set of approaches by attackers to gain higher levels of access to a system or network than they originally had. This tactic is often used in conjunction with other tactics, such as Initial Access or Persistence, and is essential for attackers to achieve their goals, such as stealing sensitive data or deploying malware. Zero-trust protects the network through strong access control policies and micro-segmentation which could limit the impact of Privilege Escalation attacks, as attackers will only have access to a limited portion of the network.

The fifth category we considered is credential access which refers to the techniques used by attackers to steal valid credentials to access a system or network. This tactic is a critical component of many attacks, as valid credentials are often required to move laterally through a network or to access sensitive data. Credentials stuffing, brute-force attacks and multi-factor authentication attacks are widely used techniques for credentials stuffing. Zero Trust significantly reduces the risk associated with stolen credentials. By requiring additional verification and limiting access privileges, Zero Trust makes it much harder for attackers to leverage compromised credentials to achieve their objectives.

The sixth category we considered is command and control which refers to the techniques used by attackers to communicate with and control compromised systems or networks. This tactic is a critical component of many attacks, as attackers need a way to remotely control their malware and exfiltrate stolen data. The application layer protocols, remote access applications and tools can be used to compromise the network and use it as a distribution point for malware or denial of service attacks. The implementation of zero-trust could reduce the attack surface for Command and Control attacks by requiring strong authentication and authorization measures for any communication between systems. Zero Trust disrupts command and control communication by implementing a "never trust, always verify" approach. Zero Trust also emphasizes continuous monitoring of user and system behaviour to further improve the security of the network.

The seventh category of Att&ck framework considered is Defense Evasion which refers to techniques used by attackers to avoid detection and bypass security measures deployed by organizations. This tactic is used to maintain their foothold in the compromised system or network and enable them to achieve their objectives without being detected. To this extent, Zero Trust's focus on least privilege access control directly counters attacker techniques that exploit stolen credentials for privilege escalation.

The eighth category we considered is the impact which describes the effects of an attack on a system or network. The impact can be defined as the result or consequence of a successful attack, and it can be used to measure the severity of the attack and its potential damage to an organization. The zero-trust could minimize the impact of the attack on the organization because of micro-segmentation and strong access policies. Even if an attacker breaches a system, Zero Trust's access controls mechanism limits the damage they can do. They would not have access to the entire network or sensitive data because of micro-segmentations and access policies.

Finally, we considered lateral movement which refers to the techniques used by attackers to move through a network after gaining initial access. Once attackers have gained access to a system or network, they attempt to move laterally through the network to identify and compromise additional systems or resources. The zero-trust requires continuous authentication which could resist the movement of the attacker inside the network. Zero Trust often utilizes micro-segmentation within networks, creating barriers between resources. This restricts attackers' ability to move laterally across the network after gaining initial access.

The Zero Trust approach is aligned with MITRE ATT&CK framework, as it addresses many of the tactics and techniques used by attackers to compromise systems and networks. If properly implemented it could improve the security posture of the network and minimize the impact of cyberattacks on the organization.

4. Zero-trust implementations

This section offers a fresh perspective on implementing zero-trust security, moving beyond the 'never trust, always verify' paradigm [71]. Recognizing potential limitations in broad applicability, this framework explores alternative approaches that cater to the diverse needs of different organizations. To this extent, we evaluate the works which have been performed in the perspective of zero trust [72]. Fig. 8 presents the implementation setup for ZTA. The core implementation models in ZT can adopt four approaches: centralized, decentralized, distributed, and blockchain-based as shown in figure Fig. 9.

Centralized Implementation: In a centralized ZTA, all the components, security functions, and decision and control functions are implemented and managed from a central location. Specifically, there exists only one PDP, PE, and PEP setup for all the network devices, users and segments. This architecture allows the administrator to implement consistent security solutions across the entire organization. A centralized system also enables to monitoring of the user and network activities from a single point thus bringing the benefit of easier administration and management. However, centralized systems have some limitations such as a single point of attack and failure, difficulty to scale with a large number of users and devices, and most importantly users need to trust these systems

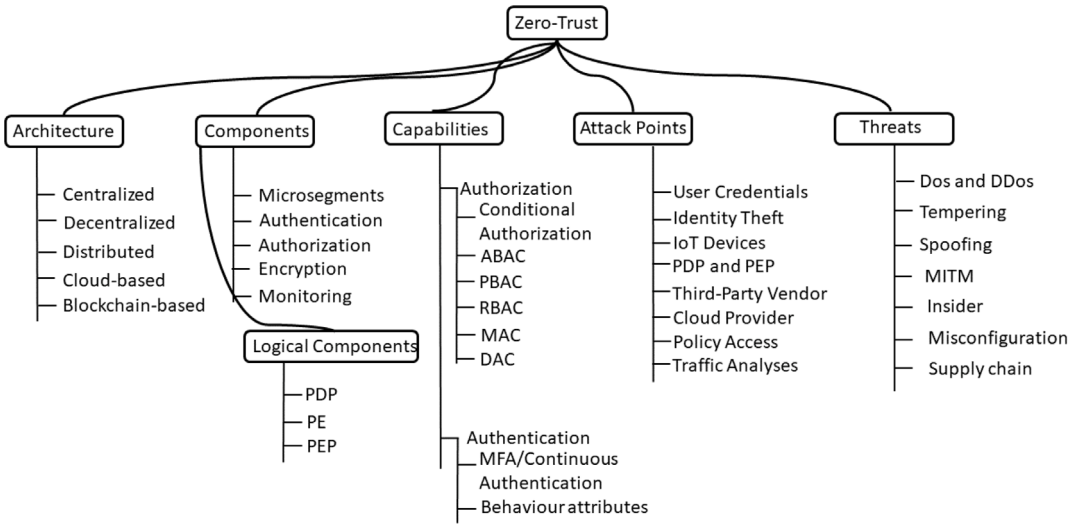


Fig. 8. Analysis framework to zero trust implementation.

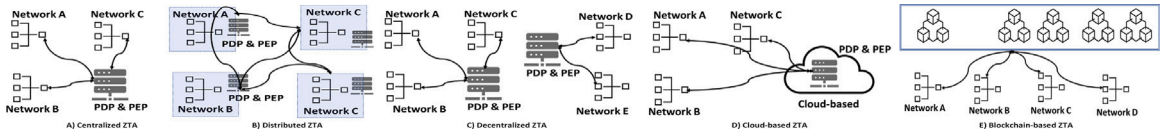


Fig. 9. Communication setup of zero-trust architecture.

for their privacy and security. The centralized system also becomes a bottleneck as all traffic passes through this core component. Centralized ZTA cannot support peer-to-peer, ad-hoc, and decentralized networks as well [72].

Distributed Implementation: The limitations of a single point of failure and attack can be minimized by distributing the core functional components of ZTA across all the network segments and these segments then communicate with each other directly or to outer networks. In this setup, each network segments have its own PDP, PEP and PE setup. The distributed setup has some important features such as it can provide some resilience if core components of a specific segment are failed by shifting the load to other segments, provide a dynamic trust level specific to segments, reduce the attack surface by minimizing the exposure of the network. The distributed setup also has some limitations as it requires careful planning to ensure consistent policies across the network and requires some resources for the management of complex network and traffic analysis.

Decentralized Implementations: Decentralized zero trust distributes the functionality of ZTA components across the network. A decentralized setup reduces the attack surface, provides resilience to the failure and single point of attack and allows the definition of policies related to a particular network. In some cases, more than one segment is logically connected and is controlled by the same policy enforcement system. The decentralization also allows the distribution of the policy definition function and policy enforcement function across the network, for example, policies are defined and managed at the central location but enforcement of policies is being performed very near to a segment or device, for example, the edge or fog device. This setup though brings some benefits over centralized setup but has management overheads for device and network management. The decentralization can also be implemented through the use of software-defined network and network function virtualization [73].

Blockchain-based Implementations: Blockchain technology can also be used to distribute the ZTA functionality across the network. In a blockchain-based ZTA, PDPs and PEPs can be implemented using smart contracts and distributed ledger technology. In a blockchain-based ZTA, PEPs can be implemented using smart contracts that are deployed on the network nodes. The PEP smart contract can verify the identity of the user or device trying to access a resource and check whether they are legitimate users or not via access PDP smart contract. The PDP smart contract responds with the result of the policy check, and the PEP smart contract enforces the access control policy accordingly. All transactions related to access, authorization and authentication are logged on the blockchain, providing a tamper-proof record of access and security events. This implementation not only reduces the single point of attack but also improves the security and privacy of users and devices using a tamper-proof ledger of transactions. A blockchain-based implementation of PDP and PEP can provide organizations with enhanced security and decentralized decision-making but at the expense of complexity and computation resources required for handling blockchain transactions.

Cloud-based Implementation: In the cloud-based system the ZTA components can be implemented and managed in the cloud. The cloud-based ZTA shifts implementation to cloud-based service thus offering scalability, resilience, security, and cost-effectiveness. Within this setup, the functionality of PDF can be implemented in the cloud by defining access rules and policies are

enforced at the edge point after accessing them from the cloud. Platform as a Service (PaaS) and Software as a Service (SaaS) can be used as the Policy Decision Function (PDF) and Policy Enforcement Point (PEP) in ZTA. Within this setup, PaaS and SaaS can provide resources to implement access control policies and their enforcement. Cloud-based Zero-trust systems can also Amazon web services, Azure or Google Cloud systems for policy and access management.

5. Adoption and implementation of zero-trust

ZTA implementation ensures that users, devices, and applications must be constantly authenticated and authorized to use the network resources. It also requires that access control and network usage policies must be implemented based on the identity of the user, the status of the device, and other contextual considerations. In this section, we will explore some possible implementations of zero-trust security in different organizational settings to achieve more robust and dynamic security [74]. Table 2 presents the related work regarding zero-trust implementations.

5.1. Cloud-based zero trust system

As organizations increasingly move their operations to the cloud, securing cloud infrastructure becomes a top priority for secure, resilient and trusted operations. A zero-trust-based model provides a more detailed and dynamic approach to securing the cloud infrastructure which might not be possible through perimeter-based security measures. Dynamic access control, continuous authentication and authorization of network devices, software and applications, and services are required regardless of location from where the request has been made for the cloud resources.

Decusatis C. et al. [75] explored the implementation of a zero-trust system with the use of transport-level access control and first packet authentication. First packet authentication analyses the first packet originated by the user and verifies the identity of the user through careful packet inspection and transport layer access control implements the authorization policies. Steganographic overlay has been implemented at the transport layer access control to block unauthorized traffic. The approach has a limitation as it is resource-intensive due to transport layer cryptographic operations resulting in computation and communication overheads [76] and TCP communication flows are vulnerable to session hijacking attacks [77,78]. Hussain F. et al. [79] proposed a security management framework based on the Intelligent Service Mesh Framework which incorporated a layer of intelligence using machine learning, and artificial intelligence to automate the discovery, configuration, and management of API security policies. The intelligent mesh framework improves security by creating zero trust around the core assets of the network and applications. Luca et al. [80] proposed a system that assumes that both data and control plane can be untrusted within the zero-trust frameworks. To protect the network, the authors proposed a survivable zero-trust framework that includes three main components: a trust engine, a fault-tolerant controller, and a survivable data plane. The trust engine is responsible for verifying access requests and enforcing security policies. The survivable data plane provides a secure communication channel between the trust engine and the protected resources. The critical limitation of the existing system is the non-compliance of encrypted messages during the evaluation of access control policies. The network perimeter in a cloud environment is constantly changing, and the traditional approach becomes challenging to maintain security. Zirak Zaheer et al. [81] proposed an approach a network-independent approach called ezTrust that protects microservices (application and data) by implementing zero-trust parameterization. The approach consists of three core components: the eZTrust Proxy, the eZTrust Controller, and the eZTrust Policy Engine.

Mehraj, S. and Banday, M. T. [82] discussed the challenges of implementing the zero-trust strategy in the cloud computing environment to improve their security posture. The authors implemented the security of the cloud network by dividing the network into small segments, using encryption for integrity and confidentiality and strict implementation of access control policies. The authors also analysed the use of machine learning algorithms and Artificial intelligence to detect and respond to security threats in real time. Koshi Ishide et al. [83] use supervised Machine learning and rule-based approaches for detecting malicious users and traffic in the heterogeneous zero trust architectures. The proposed method has shown improved performance in detecting malicious activity but its accuracy depends upon the quality of training data. Chuan T. et al. [84] proposed a ZTA methodology that leverages a set of access control policies to safeguard data exchange between external servers and internal networks. This approach is designed to be compatible with existing corporate network environments.

Zhang Xiaojian et al. [100] proposed a zero-trust framework that can be used to protect power IoT devices, big data and services from numerous security threats. Within the framework, they adopted micro-segmentation and then applied policies to each segment. The segmented network limits the footprint of attack, but it could increase some load over the resource-constrained devices. Zero-trust framework should have property self-governance, self-healing, and self-protecting mechanisms to provide continuous security and threat mitigation [125]. Dayna Eidle et al. [86] propose an autonomic security framework for zero trust which is itself capable of detecting, responding and recovering from security threats. The framework consists of four components, the policy manager, the event manager, the response manager and the assurance manager. This results in a proactive network security which minimizes the attack footprint and improves overall security of the enterprise network. This implementation also improves incident detection time and reduces the implementation cost of securing the network. Micro-segmentation is the major component of the zero-trust model and could reduce the attacker footprint during the execution of the attack. Micro-segments make it more difficult for attackers to move laterally across the network and exploit vulnerabilities. Nabeel Sheikh et al. [87] discuss the implementation of a zero-trust security model by micro-segmenting large network into small and manageable segments. Each micro-segment has their own security policies and controls as the effective defence against malicious actors. The micro-segmentation ensures that malicious actors would not cross the boundary of compromised segments thus reducing the attack surface and minimizing the potential damage from the

Table 2
A summary and comparison of implementation architecture, authentication, authorization and access control mechanisms for zero trust enabled security.

Reference	Architecture	Application	Authorization	Authentication	Access control	Cryptography	Multifactor authentication	Network segmentation
Cloud-based systems								
Chuan et al. [84]	Decentralized	Cloud	✗	✗	✓	✗	✗	✗
Mehraj, S. et al. [82]	Centralized	Cloud	✗	✓	✗	✗	✓	✓
Decusatis, C. et al. [75]	Distributed	Cloud	✗	✓	✗	✗	✓	✓
Krx et al. [85]	Distributed	Cloud	✓	✗	✓	✗	✗	✗
Fatima et al. [79]	Centralized	Cloud	✗	✓	✗	✗	✗	✗
Zaheer et al. [81]	Distributed	Cloud	✗	✓	✗	✓	✓	✓
Ferretti et al. [80]	Decentralized	Cloud	✓	✓	✓	✓	✗	✗
Eidle et al. [86]	Centralized	Cloud	✗	✓	✓	✗	✓	✗
Sheikh et al. [87]	Decentralized	Cloud	✗	✗	✗	✓	✗	✗
Yang et al. [88]	Distributed	Cloud	✗	✓	✗	✓	✗	✓
Krishnan and Sreeja [89]	Centralized	Cloud	✗	✓	✓	✗	✗	✗
Dimitrakos et al. [90]	Decentralized	Cloud	✓	✗	✓	✗	✗	✗
Zhao et al. [91]	Hybrid	Cloud	✓	✗	✓	✗	✗	✗
Sengupta et al. [92]	Distributed	Enterprise	✓	✓	✗	✓	✗	✗
Jin and Wang [93]	Distributed	Cloud	✗	✗	✓	✗	✗	✗
Ghate et al. [94]	Centralized	Cloud	✗	✓	✓	✓	✗	✓
Hatakeyama et al. [95]	Centralized	Cloud	✓	✓	✓	✗	✗	✓
Tian and Song [96]	Decentralized	Cloud	✗	✓	✓	✗	✗	✗
Ahmed et al. [97]	Distributed	Cloud	✗	✓	✓	✗	✗	✓
IOT-based system								
Wenhua Huang et al. [98]	Cloud	Power-IoT	✓	✗	✓	✗	✗	✓
Samaniego et al. [99]	Blockchain	IOT	✓	✗	✓	✗	✗	✓
Claudio et al. [25]	SDN	IIOT	✓	✓	✗	✗	✓	✗
Zhang X. et al. [100]	Centralized	IOT	✓	✓	✗	✗	✓	✗
Anil G et al. [101]	Centralized	IOT	✗	✓	✗	✗	✓	✓
Liu Y. et al. [102]	Decentralized	IOT	✗	✓	✓	✗	✗	✗
J Wang et al. [103]	Distributed	IOT	✗	✗	✓	✓	✓	✓
Dimitrakos et al. [104]	Centralized	IOT	✗	✓	✓	✗	✗	✗
Abhiram et al. [105]	Distributed	IOT	✗	✓	✓	✗	✓	✗
Yao and Wang [14]	Centralized	IIOT	✓	✓	✓	✗	✗	✓
Colombo et al. [106]	Distributed	IOT	✓	✗	✓	✗	✓	✗
Shah et al. [107]	Distributed	IOT	✗	✓	✗	✗	✓	✓
Gutmann et al. [108]	Decentralized	IOT	✓	✓	✗	✗	✗	✗
Da silva et al. [109]	Distributed	IOT	✓	✓	✗	✗	✗	✓
Wei et al. [110]	Distributed	IOT	✗	✓	✗	✓	✗	✓
Mandal et al. [111]	Centralized	IIOT	✗	✗	✓	✗	✓	✗
Halter et al. [112]	Decentralized	IOT	✗	✓	✓	✗	✓	✓
Sasada et al. [113],	Distributed	IOT	✗	✓	✓	✗	✗	✗
Wu and Wang [114]	Decentralized	IIOT	✗	✓	✓	✓	✓	✗
Fang and Guan [115]	Distributed	IOT	✓	✓	✓	✓	✓	✗
Vanickis et al. [116]	Centralized	IIOT	✗	✓	✓	✗	✗	✓
Lee et al. [117]	Distributed	IOT	✗	✗	✓	✗	✗	✗
Decentralized and blockchain-based Systems								
Chenchen Han et al. [118]	Decentralized	IOT	✗	✓	✗	✗	✓	✗
Peirong Li et al. [119]	Blockchain	Electric vehicles	✗	✓	✗	✓	✓	✓
Alevizos et al. [67]	Blockchain	Enterprise	✗	✗	✓	✗	✗	✗
Mukesh Kumar et al. [120]	Decentralized	6G network	✗	✓	✓	✓	✗	✗
Patil et al. [121]	Decentralized	Blockchain	✓	✓	✗	✓	✗	✗
Dhar et al. [122]	Blockchain	IOT	✓	✓	✗	✓	✓	✓
Li, D. et al [123]	Blockchain	Edge computing	✗	✓	✗	✓	✗	✓
Nannan Wu et al. [37]	Blockchain	Centralized	✓	✗	✓	✓	✗	✗
Gai Keke et al. [40]	Blockchain	Centralized	✓	✗	✓	✓	✗	✗

(*continued on next page*)

Table 2 (*continued*).

Samia et al. [42]	Blockchain	Edge	✓	✗	✗	✗	✗	✗
Albuali et al. [124]	Blockchain	IOT	✓	✓	✓	✗	✓	✓
Zhao et al. [91]	Blockchain	IOT	✓	✓	✗	✗	✗	✓

security breach. However, this makes the network more complex, and expensive and incurs communication delays while checking and enforcing policies on each micro-segment. Krx et al. [85] present a Zero-trust model based on distributed cloud architecture to potentially overcome the access control protocols within the cloud infrastructure. The system utilizes thin and micro cloud techniques within both its configurations. Simone Rodigari et al. [126] present a performance analysis of a zero-trust security model implemented in a multi-cloud environment. The experiments involved deploying a web application in a multi-cloud environment and measuring various performance metrics, including response time, throughput, and resource utilization. The results show that a zero-trust security model can be implemented with minimal impact on performance. Zero-trust cloud architecture may enhance security, lower the risk of data breaches, and increase flexibility, making it a worthwhile investment for businesses that rely on cloud-based services. Claudio et al. [25] provide a new Zero Trust Architecture that can be easily integrated into cloud computing and Internet of Things solutions to secure the devices within heterogeneous industrial networks. Authors adopted software-defined networks for enforcing access policies in a micro-segmented network.

5.2. Distributed IoT based zero trust frameworks

The distributed zero-trust approach protects the IoT devices and networks which are not only resource-constrained but are dispersed across numerous networks and locations. The conventional security models are insufficient to protect these networks because of the dynamic nature and resources available, however Implementing an IoT-based zero-trust system can be challenging, requiring careful planning and a thorough understanding of IoT security best practices.

Shancang Li [127] discussed the application of the zero-trust security model in the context of the Internet of Things (IoT). The author highlights the unique security challenges posed by the IoT and proposes a zero-trust approach as a solution. The author also discussed the use of blockchain technology as a means of providing trust in the IoT. However, this work did not protect against dynamic IoT threats. The enterprise Internet of Things (E-IoT) is a distributed and complicated system made up of a huge number of heterogeneous devices having different network connectivity and resources. These systems frequently have internet connections, making them open to various security risks such as unauthorized access, data alteration, and denial of service assaults. Anil, G. [101] et al. proposed a framework that can be applied to secure the E-IoT. The framework consists of two major components a lightweight cryptography-based secure data transmission mechanism and a machine learning-based intrusion identification system. Safwa Ameer et al. [128] implement Zero-trust by defining and designing the access control policies from smart IoT systems. The authorization is based on the score-based authorization model. In a score-based authorization model, each device and user is assigned a score based on a variety of factors, such as their identity, their location, and their past behaviour. Yinghong Yang et al. [129] proposed a blockchain cross-chain communication protocol to minimize privacy breaches within a zero-trust IoT environment. The protocol uses relay chains and protect sensitive information by concealing inter-chain transaction addresses. Adel Atieh et al. [130] proposed a zero-trust model for the industrial Internet of Things (IIoT) to mitigate the existing risks within the IIoT environment. The framework is based on the principle of zoning which is then protected based on zone score.

Liu Y. et al. [102] Proposed a decentralized system for sharing information in the zero-trust Internet-of-Things (IoT). The system allows IoT devices to share information in a secure and trustless manner using a blockchain system and a smart contract to control access to the information. The system is fair and transparent in the sense that all authenticated devices can have access to information [131]. The proposed approach faces challenges in terms of latency, with potential delays in data transmission due to additional security checks. Additionally, the protocols may increase processing overhead on network devices. Abhiram D et al. [105] proposed a VPN-based zero-trust architecture that employs software-defined parameters (SDP) to govern access control and reinforce security measures within network communications. Dimitrakos et al. [104] proposed a trust-aware continuous authorization framework for consumer Internet of Things (IoT) devices. The framework is based on the Usage Control (UCON) model, dynamic authorization (Attribute Based Access Control (ABAC)) which grants users resources based on the context of a request. The framework also incorporates trust evaluation, which allows for dynamic authorization decisions based on the current trustworthiness of a device. Samaniego et al. [99] propose a zero-trust hierarchical management framework for the Internet of Things (IoT). The framework is designed to address the security challenges of IoT, such as unauthorized access, data tampering, and denial of service. The framework consists of three main components: the policy manager, the attribute authority and the policy enforcement point. J Wang et al. [103] propose a distributed ledger-based system to store confidential information of the user in the Internet of Things (IoT). This makes it ideal for storing sensitive data, such as IoT data, which needs to be protected from unauthorized access. The first layer is the data layer, which stores the actual IoT data. The second layer is the security layer, which provides security and privacy features for the data. This method makes proof of work sizes smaller by combining evidence from different parts of the blockchain. This helps IoT and blockchain systems talk to each other more easily and efficiently. Samia et al. [42] proposed ZAIB (Zero-Trust and ABAC for IoT using Blockchain) to facilitate machine-to-machine communication while ensuring access policies through edge-based deployment and the blockchain setup. The trust of the devices is evaluated based on each request while ensuring minimum latency or delay. The paper did not provide any analysis towards the implementation of access control policies and the security of device data and policies.

The IoT is a growing network of connected devices and has many application domains for example smart homes, smart manufacturing, smart cities etc. While IoT devices have the potential to provide significant benefits, such as increased efficiency and productivity, they also introduce new security risks. IoT devices are resource-constrained and do not have sophisticated security measures, making them vulnerable to cyber-attacks. ZT could provide a comprehensive security framework that can detect and mitigate threats at all levels of the network, from the device to the application layer [132]. IoT networks are dynamic with devices joining and leaving the network frequently. ZTA can provide continuous authentication and authorization of all network access requests, ensuring that only trusted devices and users are allowed to access the network [133,134]. IoT networks consist of thousands or even millions of devices, making traditional security measures such as firewalls and perimeter-based security insufficient. IoT can be applied to critical sectors such as health as well which requires a high level of security and ZT could ensure the confidentiality, integrity, and availability of data in these applications with minimal user intervention [135]. SDN and ZTA can also deploy together to secure the IoT network from sophisticated attacks while reducing the computation load from the resource-constrained devices [62,136,137]. This implementation would make the network more secure, simple and efficient by allowing network administrators to manage network resources and security from a centralized location. This would also allow the network to divide the implementation as the control plane and data plane with different implementation policies [138].

5.3. Centralized zero-trust systems

ZTA can be implemented as a centralized system setup where there is a centralized authority which acts as the proxy for verifying the user or device identity and grants access based on predefined access policies. These policies can be dynamic, or static implemented on PDP or PEP but can be routed through the centralized system. Omar et al. [20] compare two centralized security mechanisms namely network access control (NAC) and software-defined perimeter (SDP) to enforce the policies using the centralized software-defined network. NAC is responsible for controlling the access based on predefined policies and SDP creates an isolated fence network around the resources, applications, and devices. Authors argued that SDP is more effective and secure than NAC, as it provides strong security and a more flexible approach to defining and enforcing access control policies. Puthal et al. [139] proposed a ZT model by enforcing the policies based on software-defined networking (SDN). The centralized SDN controller is used to create a virtual perimeter around the network which can be used to control access to the network based on different authorization and access control policies. However, these schemes are mainly based on centralized design to enforce the policies in a distributed environment in a centralized way and have some limitations such as dynamic scalability, low flexibility, and do not have dynamic access control management.

Healthcare organizations hold and process patient confidential data, such as medical records, personal identification information, scan results, and insurance details for meaningful and automated decisions. These sensitive data need continuous access, can be seen by the person who is authorized based on their role and should not move outside the perimeter of the organization [140]. Within this emerging eco-system perimeter-based traditional security systems would not provide effective security and privacy of user data and network devices. A ZT security model within an emerging healthcare network can help ensure that users' data and devices are protected from unauthorized access, ensuring patient privacy and confidentiality. Implementing a ZT could mitigate the risk of data breaches by allowing controlled access to patient-sensitive data and blocking malicious actors at the early stage of the attack. Healthcare organizations also ensure that they have placed effective security measures to fulfil the compliance regulations (HIPPA, GDPR, ICO etc.) [141,142]. A ZT approach can help healthcare organizations comply with these regulations by ensuring that patient data is protected from unauthorized access. As stated, traditional security measures would not protect the network from insiders, however, a ZT approach can help mitigate this risk by limiting access to data based on the user's role, privileges, and continuous authentication [143].

Finally, a ZT approach can help healthcare organizations manage this complexity by segmenting the network into smaller, more secure sections, and limiting access to each section based on the user's role and permissions [144]. Chen et al. [145] propose a ZTA based security and privacy protection systems for smart and interconnected healthcare system. The system consists of four layers: the perception layer, the network or inter-networking layer, the application layer, and the network management layer. The perception layer collects sensor data, communication between device handles through the network layer, the application layer provides access to remote users and the management layer enforces user policies. Continuous authentication and authorization have been implemented in a multi-tiered healthcare network to ensure the security of data and devices [146,147]. For healthcare platforms, this approach performs quite well in terms of functionality and efficiency. Its robust features and reliable performance make it an acceptable choice for managing sensitive medical data and supporting critical healthcare operations. Network slicing and segmentation can also be used to secure the healthcare network [148]. Network slicing can secure telemedicine consultations by allocating them to a dedicated network slice with stricter security measures, guaranteeing patient privacy and uninterrupted communication. Segmentation can isolate administrative networks from patient data systems, preventing malware or unauthorized access from one side from jeopardizing the other. This would allow the implementation of policies based on their role and within the divided segment. The management of such a network might be challenging and requires some extra investment in terms of deploying a firewall for each segment.

5.4. Blockchain-based zero-trust systems

A blockchain-based zero-trust system is a security architecture that uses blockchain technology to implement the zero-trust security model. Blockchain technology can be used to implement zero trust by providing a secure and immutable ledger of all authentication and access policies. The ledger can be used to verify the identity of users and devices, revoke and enforce access policies and track users' activities across the network. A Blockchain-Based zero-trust system is decentralized, which means that there is no single point of failure and single point of attack. The distributed nature of the system ensures that no single entity has control over the network, and any attempt to tamper with the data is immediately detected and prevented. Blockchain has a wide range of potential applications in different domains such as the Internet of things, metaverse, supply chain management, healthcare etc [67,149–152]. The challenge to using the blockchain-based zero trust is that the implementation is complex, might have an additional delay while enforcing the authentication and access policies and can be difficult to implement and manage. Blockchain would help systems to be secure by making it hard to change data, and the zero-trust model makes sure people with approved credentials can access the data and resources.

Li et al. [119] propose a comprehensive security architecture for smart EV chargers, employing zero-trust principles for access control, blockchain for reliable key management, and ShangMi cryptography for enhanced data integrity. The zero-trust architecture enforces identity and access management (IAM), allowing only authorized entities could access the sensitive data. Saima et al. [153]propose a blockchain-based attribute-based zero-trust access control model for the Internet of Things (IoT). The model is designed to address the security challenges of IoT, such as unauthorized access, data tampering, and denial of service. The model is based on the following key principles: Zero trust, Attribute-based access control and Blockchain. Mukesh Kumar et al. [120] propose a blockchain-based group authentication scheme for 6G communication networks. The scheme is designed to address the security challenges of 6G networks, such as unauthorized access, data tampering, and denial of service. The scheme ensures the integrity and confidentiality of user data through the use of group authentication and Blockchain.

Chenchen Han et al. [118] proposes a blockchain-based zero-trust scheme to ensure security and privacy within 6G edge IoT. The scheme is designed to address the security challenges of 6G edge IoT, such as unauthorized access, data tampering, and denial of service. The scheme is based on the following components: the creation of zero-trust among users and devices, the implementation of the blockchain system and the utilization of the edge computing concept to deploy the functionality of the blockchain system. The zero trust-based BDS storage leaves complex blockchain architectures susceptible to security breaches, warranting additional defencive measures. Alevizos et al. [67] provides a comprehensive review of the state-of-the-art in blockchain-based ZTAs and identifies how blockchain could be used to implement Zero-trust on end devices. The scope of Blockchain is currently limited to the IoT, the security of the network can be improved and reshaped by integrating blockchain and zero-trust within IoT and resource-constrained devices. These integrated control mechanisms might potentially safeguard diverse network landscapes.

Patil et al. [121] proposes a consensus algorithm for building a zero-trust model. The algorithm utilizes the concepts of decentralization, transparency and immutability using a distributed ledger. The algorithm is implemented on the consensus IoT nodes. The consensus technique makes sure the system works right in a decentralized way without the centralized entity. Dhar and Bose [122] the risk score by using access control policies, segmentation, identity management and zero trust enforcement using a blockchain system. Li et al. A ZT [123] ensures the security of end devices by making access control policies at the edge devices by enabling identity verification, authentication and authorization using distributed blockchain. To test their approach, they established a blockchain-based edge computing alliance where devices collaborate with each other to report security incidents. Nannan Wu et al. [37] proposed an attribute-based access control mechanism based on block-chains in order to ensure user's, network policies and their attributes. The integrity and confidentiality of attributes are ensured through homo homomorphic cryptosystem. Gai Keke et al. [40] proposed a framework which enables different service providers to exchange information in a privacy-preserving way. They adopted a blockchain-based access control scheme with participating members of the consortium in order to ensure the confidentiality and integrity of user's data and the organization's confidential information. Blockchain technology can also be used to enforce the secure, decentralized authentication [154–156] and access control mechanisms [157–159] in healthcare organizations. This method has some computation and communication overheads over public blockchain since it takes time for peer-to-peer node verification and authentication. The implementation of blockchain with ZT still requires several challenges to address before it is deployed in real resource-constrained and dynamic networks. These challenges require a balance between security, decentralization, scalability, privacy, interoperability between different networks, lightweight consensus algorithms, and performance overheads such as computation power and bandwidth.

6. Authentication, authorization and access control in ZTA

In a ZT environment, authorization and access control are more critical components as the ZT model assumes that no user, application, process, traffic, or device within the network can be trusted. Therefore, all access requests must be verified and authenticated before being granted. Authorization and access control in ZT are designed to ensure that only authorized users and devices can access resources, and only for as long as they need to while considering the characteristics of the network, traffic, and users in a dynamic way. By verifying the identity of users and devices, and then granting them access to resources based on their need to know, zero trust can help to mitigate the risk of data breaches. The implementation of authorization and access control within ZT security would bring several benefits including reduced risk of data breaches, improved visibility and control in a highly dynamic and heterogeneous network, greatly improved user experience while still using their own devices and a secure network from internal and external threats. These benefits would greatly help the organization to minimize security threats, save finances because

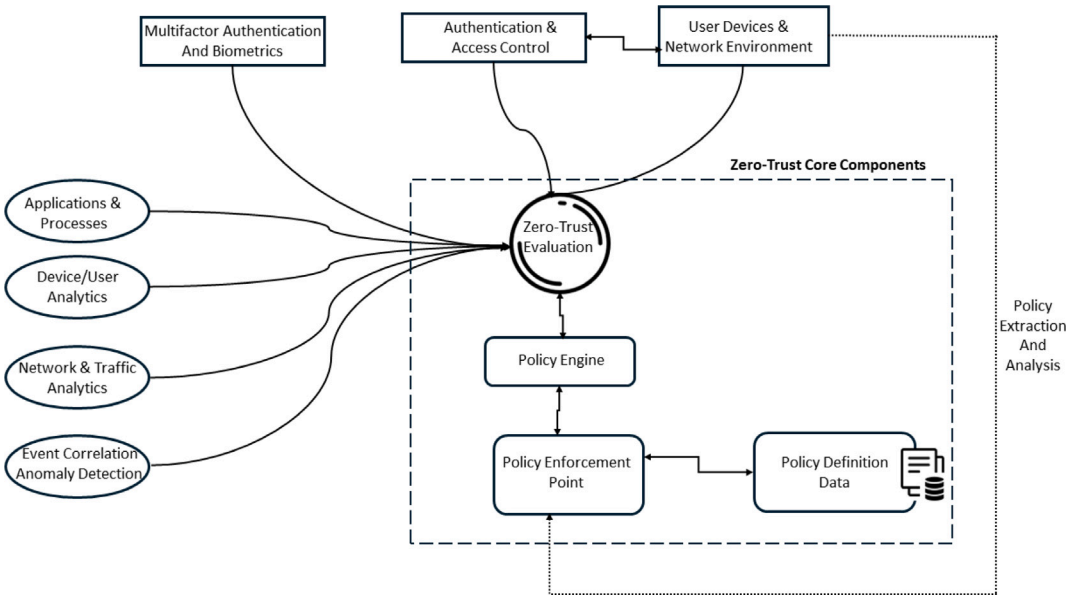


Fig. 10. Seven basic pillars of zero trust architecture for authentication and authorization.

of ongoing security threats, minimize unauthorized access and improve security posture [160]. Fig. 10 presents the authentication and authorization architecture of ZTA. In this section, we discussed Zero trust from the perspective of authorization and access control. We explained how Zero trust requires every request for access to a resource to be verified and authenticated, regardless of whether the request is coming from inside or outside the network. Table presents the related work covering authentication, authorization and access control within zero-trust.

6.1. Authorization

Authorization involves defining and enforcing access control policies, which specify the permissions that have been assigned to users and devices for accessing the organization's resources. Access control policies can be based on various factors, such as user roles, job functions, and security clearances, and can be implemented at different levels, such as application, database, or network. There are several methods of authorization, including DAC MAC, and RBAC [106]. In a Zero trust authorization is a critical component of access control, and every access request must be continuously verified and authenticated. Dynamic authorization is an essential aspect of Zero trust security, as access control policies must be continuously updated based on user behaviour. Qigui Yao et al. [14] proposes a dynamic access control and authorization system based on a ZT security architecture. The system utilizes the continuous risk and trust assessment to validate users' policies and grant access dynamically. The system consists of four main components: a trust assessment module, a policy management module, an access control module, and an authorization module. The system also uses machine learning algorithms to detect anomalous user behaviour and automatically revoke access when necessary.

ZT networks operate on a zero-trust foundation, demanding rigorous scrutiny of every access request. The four pillars of the authorization architecture – Enforcement, Policy Engine, Trust Engine, and Datastores – form a robust defence mechanism, filtering out unauthorized attempts and granting access only to those deemed trustworthy. Merging these components under one umbrella risks creating a single point of failure, a fatal vulnerability in the ZT security architecture [90]. Wenhua Huang et al. [98] proposes a ZT access control mechanism that uses attribute-based encryption (ABE) to secure the power of IoT devices. This makes it possible to control access to data based on the attributes of the users and devices that are requesting access. The trust score of the user and devices is calculated in real-time which can block access to the user having abnormal behaviour to gain access permissions. García-Teodoro et al. [43] enhanced the security of the network by using a ZT network access control scheme based on the security profile of devices and users. The scheme consists of four main components: a trust assessment module, a policy management module, an access control module, and an authorization module. The system continuously monitors device and user behaviour to dynamically update access control policies in real time. If a device or user is found to be non-compliant with security policies, access is automatically denied or restricted.

Zhao et al. [161] propose a method for controlling access to a network based on cloud sea big data fuzzy clustering. The method uses a fuzzy clustering algorithm to cluster users and devices into different groups and then uses a trust evaluation mechanism to determine the trust level of each group. The access authorization and control mechanism is then used to control access to the network based on the trust level of each group. The technique can regulate access authorization at the network's perimeter. Binanda et al. [92] proposed a system called Distritrust that provides distributed and low-latency access validation in a ZTA. The system consists of two major components: the validation engine and the distribution engine. The validation engine is responsible for validating and

enforcing access requests from users, network devices or applications and the distribution engine is responsible for distributing the validation workload across multiple nodes to achieve low-latency performance thus achieving scalability and resilience.

Abdullah Ztimm et al. [124] proposed a zero-trust-based distributed identity management model for volunteer cloud computing where cloud computing resources are shared among users. The identity management system is responsible for managing user identities and ensuring that only authorized users are granted access to the resources. The access control system is responsible for enforcing fine-grained access control policies and ensuring that users are only granted access to the resources they are authorized to access. The trust management system is responsible for assessing the trustworthiness of the computing resources and ensuring that only trusted resources are used.

Access control aims to ensure that only authorized entities, such as users, devices, or applications, are granted access to the resources they intend to use. It can be used in various environments, including computer systems, IoT devices, applications, software, cyber–physical systems, networks, physical premises, and cloud computing. The most widely used models are RBAC, MAC, ABAC, and rule-based access controls. [79]. A number of access control policies have also been proposed within a ZT environment based on traffic analysis [97,111], based on dynamic allocation of resources and access rights [93,113], using traffic and resource context to allow the device access [94,112]. Identity-based access control (IBAC) controls access to resources based on the identity of the user or entity requesting access [95,114,115]. It can help to improve security, reduce risk, increase compliance, and improve efficiency, however, scalability and interoperability are the big challenges to consider before its implementation. The risk associated with the device and end-users has also been used to evaluate the access rights of the entity. Risk-based access control as signs access rights to users based on their job function or role within an organization, rather than on their identity [96,116,117,162].

6.2. Authentication

Access is granted to users or devices only after they have been thoroughly authenticated and authorized in a ZT authentication model. Multiple layers of authentication may be used, such as verifying a user's identity with a username and password, as well as additional factors such as biometric data or a physical security key. Furthermore, ZT authentication continuously monitors and analyses user behaviour to detect and respond to any malicious activities or anomalies. This would help even if a user's credentials are compromised, their access can be immediately revoked to prevent any unauthorized access to sensitive information or systems. Identity theft is a significant problem globally, with many individuals and organizations falling victim to this type of crime. Norton identified that over 81 million people in 10 countries experienced ID theft in the year 2021 which cost users and organizations around $4.2 billion [163]. FTC received more than 1.4 million reports of identity theft from US citizens [164]. Common approaches used to reduce the impact of identity theft are the use of strong and unique passwords, multifactor authentication, limited sharing of information online, regularly monitoring credit reports and using identity theft protection services [107]. Furthermore, traditional authentication assumes that all users within a network can be trusted and that attackers are external to the network. However, today's threat landscape is very dynamic and sophisticated, and attackers can be both internal and external to an organization. ZT authentication can provide another layer of security for protection against identity theft and detecting suspicious activity. By implementing a ZT approach, the organization would be able to prevent a potential data breach and protect its sensitive information and systems from unauthorized access. Zero trust incorporates a range of security controls, including multi-factor authentication, network segmentation, and continuous monitoring, to ensure that users and devices are who they claim to be and that their access is limited to only the resources they need to perform their jobs.

Tang et al. [165] proposed a privacy-preserving authentication scheme based on zero trust architecture which uses a pseudonymous authentication protocol for enforcing access policies. The proposed scheme also incorporates the use of a trusted third-party verifier to perform user verification without exposing sensitive user information. Lei et al. [22] propose a continuous authentication protocol that is designed for a ZTA and does not require a trusted authority. The protocol is based on the concept of "secret sharing", where a secret is divided into multiple shares, and each share is distributed among different entities. In a ZT environment, continuous authentication involves monitoring user behaviour, location, and device information in real-time to detect any anomalous activity or behaviour. This approach allows organizations to identify potential security threats and take appropriate action before any damage can occur. Continuous authentication typically involves the use of advanced analytics and machine learning algorithms to analyse user and device behaviour and detect any unusual or suspicious activity [89,107,109,166–168]. Within this authentication ecosystem protocols also need to have the enhanced property of being lightweight so can be implemented over resource-constrained devices without affecting the security and privacy [107,108,110]. In most authentication mechanisms, there exists a centralized system which is the single point of failure and a single point of attack. These systems also require that their users must trust them which is difficult to achieve in a realistic and continuously changing environment. The implementation of blockchain-based authentication eliminates the need for a central authentication authority thus ensuring privacy and transparency. Blockchain-based authentication systems have been proposed within the ZT models which do not require any trusted system but instead require a distributed and immutable ledger [91,169–173].

7. Discussion

Zero trust is a security model that allows organizations to access and verify users and devices before granting them access to resources, regardless of whether they are insiders or outsiders, asking for first-time access repetitive access. It operates on the principle that all access requests should be authenticated, authorized, and continuously monitored. Therefore, zero trust focuses on protecting sensitive data and resources by controlling access to them, regardless of the user's location or the type of device. However,

implementing a ZT can be complex and challenging, especially for organizations that have been using traditional perimeter-based security solutions for years. The adaptation also has further challenges such as deployment, investment, changes in policies and procedures as well as user training for using ZT-based security systems. The ZT policy is relatively new to the organization and has yet to get widespread implementations. Furthermore, the implementation becomes more challenging and expensive in a network that utilizes a huge number of IoT devices, allowing BYOD and unmanaged devices. This is because these devices are resource-constrained, huge in numbers and generate various types of network traffic, manufactured by diverse vendors, offer different functions and have different communication capabilities.

In this literature review, we reviewed different aspects of enforcing security within the enterprise network namely, authentication and authorization, access control mechanism, securing transfer of data in rest, transit or in process using light-weight encryption, implementation scenarios for enforcing ZT and network segmentation etc. We have observed that a large number of ZT systems are cloud-based systems which shift the functionality of ZT between the ZT cloud and the ZT host/device. This can be implemented in two modes a centralized cloud-based system and an edge-based decentralized system. The centralized cloud-based system offer is simple and offers more stable services however latency and delay in such implementation would be high. Furthermore, such implementation would require more resources for enforcing real-time decisions. The edge-based implementation allows policies to be enforced near the devices thus minimizing communication delay and reducing overheads, however, implementation becomes more complex in terms of policy management and enforcement. This implementation is more secure as it divides the network into small manageable segments with their own defined policies. Distributed and Blockchain-based systems have also been proposed but these systems still require work regarding their deployment, communication and processing overheads and employee training to use the system in real deployment. These systems also have some resource bottlenecks when comes to resource-constrained devices and networks. There requires an extensive evaluation in terms of consensus algorithm, communication structure, and user involvement before deploying such a network as efficient security requires resilience as well as effective communication with minimum overheads and costs.

Besides implementation or architectural setup, authorization has also been researched in the literature. This is an important aspect as different network requires different types of authorization models depending upon the resources and architecture of the network. RBAC, PBAC and ABAC are commonly used authorization mechanisms in ZT environments, and continuous authorization ensures that access is only granted when it is necessary. RBAC works well for static networks, but zero trust requires real-time policy decisions based on context, time, location, device type, behaviour etc. The implementation of RBAC's pre-defined policies might not adapt and scale well to these changing contexts and changing communication behaviour. PBAC and ABAC perform well for continuously changing network environments and can handle diverse devices, however crafting and managing dynamic policies for PBAC and ABAC implementation can be complex and require resources, especially for large organizations with diverse access needs. By implementing Zero Trust's principle of least privilege, organizations significantly reduce the attack surface for unauthorized access attempts, minimizing the risk of data breaches and device compromise. The implementation of authorization and access control in zero trust still requires research especially addressing the challenge of integrating the system with the legacy system, having a less complex system that can be adopted for both computing devices as well as the IoT devices, user and administrative training and definition and management of roles and permissions. These implementation scenarios should be designed while considering the type of underlying network and can support interoperability as well. One of the major aspects missing from the existing literature is the incident response as enterprises need to have a plan in place for responding to security incidents, including who to notify, how to contain the incident, and how to restore systems to normal operations. The challenge with the incident response for ZT-based networks is two-fold: first, the micro-segmentation can limit the visibility of network traffic and network attacks, which makes identifying suspicious users and devices a bit difficult; and secondly, zero-trust networks generate a high volume of control traffic for the continuous access and authorization. This could lead to complex event correlation and could miss the critical events due to information load from different devices. Furthermore, devices within ZT are from different vendors which often use different protocol stacks, and generate different types of traffic which limits incident response to perform effectively in such a dynamic environment. Finally, we have also identified that existing literature has not focused much on providing the end-to-end security of user data between devices. Most traditional methods of security have been adopted for securing the data exchange but these cannot provide efficient communication, security, privacy, and integrity within the dynamic ZT environments and resource-constrained devices. End-to-end encryption becomes more challenging in a ZT, especially when there are multiple segments between the source and the destination, and where numerous devices are involved for policy enforcement and data management. The encryption can also require setup for the key management across different segments and diverse devices. Attribute-based encryption (ABE) can be a logical approach for securing user data based on user or device attributes. However, the implementation of ABE systems can be complex in a dynamic environment where policies, attributes device properties and traffic change very frequently. The scalability and interoperability of ABE across different device types, traffic and attributes can be challenging in resource-constrained and large-scale networks.

8. Future challenges

This section discusses the key challenges ZTA needs to address before securing real-world networks [174].

Segmentation: One of the major components of ZTA is dividing the network into small segments to minimize the risk of data breaches. The effective implementation of segmentation and the creation of small zones in a heterogeneous network can further improve security, however, there are several challenges that organizations may face when adopting and implementing segmentation in the ZTA. Today's networks are very complex consisting of a large number of devices developed by different

vendors, using a different set of protocols based on different communication technologies. Network segmentation within this setup can be a complex and daunting task, especially in networks with multiple network devices, systems, protocols, and management authorities. Implementation and segmentation strategy in this setup can be challenging and require careful segmentation of network resources and the device can be complex, especially in large and complex organizations with multiple network devices and systems. Today's network needs to be integrated with the legacy systems for example decentralized identity needs to be integrated with the legacy systems for smooth operations. The segmentation in such a scenario is also challenging as these systems may not be compatible with modern segmentation technologies, and they may not be able to be easily modified. Integration is another challenge while considering segmentation as it requires integration with many security technologies and tools, such as an Intrusion detection system, intrusion prevention access, access control systems and authentication system. These systems may use different protocols developed by different vendors therefore integration can be a challenging task and may require automated configuration and management so different segments of the network work together. The implementation of segmentation has another bottleneck which is resource constraints devices as these devices may not have the necessary processing power or memory to support traditional segmentation technologies such as firewalls or virtual LANs (VLANs). Furthermore, resource-constrained networks may collect and transmit sensitive data, which can be at risk of exposure or compromise. There is a requirement to develop lightweight systems and methods for segmentation that can ensure the privacy and confidentiality of sensitive data on the resource-constrained segmented network. Finally, the segmentation requires efficient monitoring systems that can easily integrate with different devices using the same protocol without having management overheads. Research is required in this domain to develop a protocol that can serve as an interface with legacy systems, resource-constrained devices and devices from different vendors for effective monitoring and troubleshooting of network attacks.

Scalability: Scalability is a key challenge for the ZTA as ZTA implementation must be able to scale and meet the needs of a growing organization both in terms of the number of users, number of devices and volume of the data. Today's networks are growing both in terms of users and the volume of internal or external data. These users and devices should operate in plug and play manner and need security from the time it joins the network regardless of the type of device, communication protocol, technology or location. Within this ecosystem, scalability requires a comprehensive and consistent security approach across all devices, users, and networks so that devices can be introduced into the network while still ensuring the security and privacy of user and network data. Scalability issues should also be investigated along with the use of Machine learning and Artificial Intelligence systems to manage the security policies and access control policies in an automated way. The use of emerging technologies Software-defined networking (SDN), Network Function Virtualization (NVF) and cloud computing should also be investigated for the purpose of scalability in the design of ZTA architecture. All these should be implemented with the security and privacy of the end-users therefore require systems which should be easily implemented on the resource-constraints devices.

Decentralized Implementation: Decentralization is another research issue that requires further investigation within the domain of ZTA. Decentralization aims to control access control and authentication by distributing the functionalities across the network segment without having this functionality at a single centralized system or device. By implementing decentralized security measures, ZTA reduces the attack surface and makes it more difficult for an attacker to penetrate the network. Furthermore, decentralization may offer resilience and scalability within the design of the ZT architecture. However, the use of decentralization in ZTA has some challenges such as complexity, management, integration, and cost of its implementation. One of the major challenges within decentralization is complexity while ensuring the security and privacy of data, devices, and users. This is because within decentralization data is being exchanged and distrusted through the network which makes it challenging to manage and enforce the security policies. It also makes it difficult to ensure privacy within this type of data and data is being exchanged between different segments of the network. The blockchain-based system is one approach that can be used to enforce the principle of decentralization, but it inherits several challenges because of complex network architecture, compliance, and interoperability. Blockchain technology can be resource-intensive and slow, which can impact network performance and scalability. This can make it challenging to implement blockchain-based solutions in high-performance environments. Research is required to investigate consensus algorithms which should not require huge computation, communication, and memory overheads. The blockchain should also be investigated along with the design choice of software-defined network or off-chain services.

Interoperability: The diverse and evolving nature of zero trust necessitates a bespoke approach. By combining technologies from diverse sources, organizations can build robust security postures today, paving the way for a unified future. In zero trust, interoperability is the ability of different security solutions to work together to protect the organization's data, devices and users. There exists no standard or guideline exists for vendors to follow while developing and designing ZT systems. This makes it difficult to integrate different security solutions to achieve the objectives of security and privacy. Research is still required in this domain to define and design standard protocols which all ZT vendors and networks should follow for communication between heterogeneous network devices. There should be an agreed standard as well that allows devices to exchange data of different formats without largely affecting the security and privacy of users and developers.

Machine Learning and Artificial Intelligence: The major component of the ZTA is micro-segmentation access control and traffic analysis in real-time. Machine learning and artificial intelligence can play an important role in all three dimensions to enhance ZT security. Machine learning and AI can be applied to analyse the behaviour of users to identify malicious users that can then be used to rank user behaviour for access control permissions based on user current and past behaviour, user's device risk scores, location and other behavioural features [175,176]. Machine learning and AI can also be used for the visualization of the huge amount of traffic to identify emerging threats prioritize them for further investigation and generate an automated response to emerging and zero-day threats. While machine learning and AI can provide significant benefits in enhancing ZT security, there are also some challenges that organizations may face. Firstly, ZTA networks are divided into microsegments each having its own footprint and

security features. The microsegments might contain private information about users, devices, and organizational operation data. Sharing this data among themselves for effective security might increase security but at the cost of privacy. ZTA requires effective ML and AI techniques such as federated learning [177–179] that do not pose any threat to data security and have the features of lightweight and explainability. Another challenge that needs to be investigated is the deployment and management of machine learning models which can be complex and resource-intensive, requiring specialized skills and infrastructure.

9. Conclusion

Zero trust assumes that all users, devices, processes, and applications within a network are not inherently trustworthy, and as such, all ingress and egress traffic must be authenticated, authorized, and verified before access is granted to network resources. In this paper, we systematically reviewed the Zero-trust architecture in three dimensions, the architectural setup, the authorization and authentication mechanism and its alignment with the MITRE attack frame. We developed a systematic framework to investigate the existing literature in different dimensions. We looked at different types of systems based on how they use the cloud, the Internet of Things, and blockchain. We also checked their security and privacy features. We have identified that implementing Zero-trust in a continuously changing, resource-intensive environment is very challenging and may face hurdles such as resources, training, and implementation scenarios. We have identified some future research questions that would help practitioners, researchers and administrators to consider while adopting zero-trust for their organizations. Zero-trust is likely to reduce zero-day attack and minimize the attacker footprint, resulting in a micro-segmented and manageable network, however, organizations should carefully evaluate their network needs, budget, and human resource constraints before implementing zero-trust across their networks.

CRediT authorship contribution statement

Muhammad Ajmal Azad: Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Sidrah Abdullah:** Writing – review & editing, Writing – original draft, Methodology, Data curation. **Junaid Arshad:** Writing – review & editing, Supervision, Resources, Project administration, Methodology. **Harjinder Lallie:** Writing – review & editing, Validation, Supervision, Resources, Investigation. **Yussuf Hassan Ahmed:** Writing – review & editing, Visualization, Resources, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] IDC Report, Future of industry ecosystems: Shared data and insights, 2022, https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/.
[2] IBM Report, Fight back against data breaches, 2022, https://https://www.ibm.com/reports/data-breach.
[3] Editor-in-Chief Steve Morgan, Cybercrime to cost the world $10.5 trillion annually by 2025, 2022, https://shorturl.at/fozX2.
[4] Pedro Assunção, A zero trust approach to network security, in: Proceedings of the Digital Privacy and Security Conference 2019, 2019.
[5] Louis F. DeWeaver III, Exploring How Universities Can Reduce Successful Cyberattacks by Incorporating Zero Trust (PhD thesis), Colorado Technical University, 2021.
[6] Malcolm Shore, Sherali Zeadally, Astha Keshariya, Zero trust: The what, how, why, and when, Computer 54 (11) (2021) 26–35.
[7] Scott Rose and Oliver Borchert and Stu Mitchell and Sean Connelly.
[8] Naeem Firdous Syed, Syed W. Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig, Robin Doss, Zero Trust Architecture (ZTA): A comprehensive survey, IEEE Access 10 (2022) 57143–57179.
[9] Allison Wylde, Zero trust: Never trust, always verify, in: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cybersa, IEEE, 2021, pp. 1–4.
[10] Göksel UÇTU, Mustafa ALKAN, İbrahim Alper Doğru, Murat Dörterler, Perimeter network security solutions: A survey, in: 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT, 2019, pp. 1–6.
[11] G.A. Marin, Network security basics, IEEE Secur. Privacy 3 (6) (2005) 68–72.
[12] Yana Storchak, Insider threat statistics for 2024: Reports, facts, actors, and costs origin, 2024, https://tinyurl.com/22nn2z5j.
[13] Susan Laborde, 31 Insider threat statistics you need to know in 2023, 2024, https://tinyurl.com/2ju32nrh.
[14] Qigui Yao, Qi Wang, Xiaojian Zhang, Jiaxuan Fei, 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. 123–127.
[15] Kurt DelBene, Milo Medin, Richard Murray, The Road to Zero Trust (Security), Vol. 9, DIB Zero Trust White Paper, 2019.
[16] M. Ph. Stoecklin, K. Singh, L. Koved, X. Hu, S.N. Chari, J.R. Rao, P.-C. Cheng, M. Christodorescu, R. Sailer, D.L. Schales, Passive security intelligence to analyze the security risks of mobile/BYOD activities, IBM J. Res. Dev. 60 (4) (2016) 9:1–9:13.
[17] Kevin Timms, BYOD must be met with a wider appreciation of the cyber-security threat, Comput. Fraud Secur. 2017 (7) (2017) 5–8.
[18] Chris Edwards, Identity – the new security perimeter, Comput. Fraud Secur. 2013 (9) (2013) 18–19.
[19] Meisam Eslahi, Maryam Var Naseri, H. Hashim, N.M. Tahir, Ezril Hisham Mat Saad, BYOD: Current state and security challenges, in: 2014 IEEE Symposium on Computer Applications and Industrial Electronics, ISCAIE, 2014, pp. 189–192.

[20] Rami Radwan Omar, Tawfig M. Abdelaziz, A comparative study of network access control and software-defined perimeter, in: Proceedings of the 6th International Conference on Engineering & MIS 2020, ICEMIS '20, Association for Computing Machinery, New York, NY, USA, 2020.

[21] Ivana Kovacevic, Milan Stojkov, Milos Simic, Authentication and identity management based on zero trust security model in micro-cloud environment, in: Miroslav Trajanovic, Nenad Filipovic, Milan Zdravkovic (Eds.), Disruptive Information Technologies for a Smart Society, Springer Nature Switzerland, Cham, 2024, pp. 481–489.

[22] Lei Meng, Daochao Huang, Jiahang An, Xianwei Zhou, Fuhong Lin, A continuous authentication protocol without trust authority for zero trust architecture, China Commun. 19 (8) (2022) 198–213.

[23] DOD Zero Trust Engineering Team, Department of Defense (DoD) zero trust reference architecture version 2, 2024, https://tinyurl.com/nhf9z45p.

[24] Hongzhaoning Kang, Gang Liu, Wang Quan, Lei Meng, Jing Liu, Theory and application of zero trust security: A brief survey, Entropy 25 (2023) 1595.

[25] Claudio Zanasi, Silvio Russo, Michele Colajanni, Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures, Ad Hoc Netw. 156 (2024) 103414.

[26] Nardine Basta, Muhammad Ikram, Mohamed Ali Kaafar, Andy Walker, 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.

[27] Jasenka Dizdarević, Francisco Carpio, Admela Jukan, Xavi Masip-Bruin, A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration, ACM Comput. Surv. 51 (6) (2019).

[28] Pankesh Patel, Muhammad Intizar Ali, Amit Sheth, On using the intelligent edge for IoT analytics, IEEE Intell. Syst. 32 (5) (2017) 64–69.

[29] Raj Jain, Subharthi Paul, Network virtualization and software defined networking for cloud computing: a survey, IEEE Commun. Mag. 51 (11) (2013) 24–31.

[30] Sandra Scott-Hayward, Sriram Natarajan, Sakir Sezer, A survey of security in software defined networks, IEEE Commun. Surv. Tutor. 18 (1) (2016) 623–654.

[31] Monzir Babiker Mohamed, Olasunkanmi Matthew Alofe, Muhammad Ajmal Azad, Harjinder Singh Lallie, Kaniz Fatema, Tahir Sharif, A comprehensive survey on secure software-defined network for the Internet of Things, Trans. Emerg. Telecommun. Technol. 33 (1) (2022) e4391.

[32] Eduardo B. Fernandez, Andrei Brazhuk, A critical analysis of Zero Trust Architecture (ZTA), Comput. Stand. Interfaces 89 (2024) 103832.

[33] Weiwei Jiang, Yafeng Zhan, Guanming Zeng, Jianhua Lu, Probabilistic-forecasting-based admission control for network slicing in software-defined networks, IEEE Internet Things J. 9 (15) (2022) 14030–14047.

[34] Quan Shen, Yanming Shen, Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach, Comput. Secur. 136 (2024) 103537.

[35] Romans Vanickis, Paul Jacob, Sohelia Dehghanzadeh, Brian Lee, Access control policy enforcement for zero-trust-networking, in: 2018 29th Irish Signals and Systems Conference, ISSC, 2018, pp. 1–6.

[36] Theo Dimitrakos, Tezcan Dilshener, Alexander Kravtsov, Antonio La Marra, Fabio Martinelli, Athanasios Rizos, Alessandro Rosetti, Andrea Saracino, Trust aware continuous authorization for zero trust in consumer internet of things, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom, 2020, pp. 1801–1812.

[37] Nannan Wu, Lei Xu, Liehuang Zhu, A blockchain based access control scheme with hidden policy and attribute, Future Gener. Comput. Syst. 141 (2023) 186–196.

[38] Ravi S. Sandhu, Role-based access control, in: Marvin V. Zelkowitz (Ed.), in: Advances in Computers, Vol. 46, Elsevier, 1998, pp. 237–286.

[39] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, Role-based access control models, Computer 29 (2) (1996) 38–47.

[40] Keke Gai, Yufeng She, Liehuang Zhu, Kim-Kwang Raymond Choo, Zhiguo Wan, A blockchain-based access control scheme for zero trust cross-organizational data sharing, ACM Trans. Internet Technol. (2022) Just Accepted.

[41] Iftekhar Ahmed, Tahmin Nahar, Shahina Sultana Urmi, Kazi Abu Taher, Protection of sensitive data in zero trust model, in: Proceedings of the International Conference on Computing Advancements, in: ICCA 2020, Association for Computing Machinery, New York, NY, USA, 2020.

[42] Samia Masood Awan, Muhammad Ajmal Azad, Junaid Arshad, Urooj Waheed, Tahir Sharif, A blockchain-inspired attribute-based zero-trust access control model for IoT, Information 14 (2) (2023).

[43] P. García-Teodoro, J. Camacho, G. Maciá-Fernández, J.A. Gómez-Hernández, V.J. López-Marín, A novel zero-trust network access control scheme based on the security profile of devices and users, Comput. Netw. 212 (2022) 109068.

[44] Saima Mehraj, M. Tariq Banday, Establishing a zero trust strategy in cloud computing environment, in: 2020 International Conference on Computer Communication and Informatics, ICCCI, 2020, pp. 1–6.

[45] Iftekhar Ahmed, Tahmin Nahar, Shahina Sultana Urmi, Kazi Abu Taher, Protection of sensitive data in zero trust model, in: Proceedings of the International Conference on Computing Advancements, in: ICCA 2020, Association for Computing Machinery, New York, NY, USA, 2020.

[46] Daojing He, Yanchang Cai, Shanshan Zhu, Ziming Zhao, Sammy Chan, Mohsen Guizani, A lightweight authentication and key exchange protocol with anonymity for IoT, IEEE Trans. Wireless Commun. (2023) 1.

[47] Xuanxia Yao, Zhi Chen, Ye Tian, A lightweight attribute-based encryption scheme for the Internet of Things, Future Gener. Comput. Syst. 49 (2015) 104–112.

[48] Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Mauro Conti, Minho Jo, Design of secure user authenticated key management protocol for generic IoT networks, IEEE Internet Things J. 5 (1) (2018) 269–282.

[49] Savio Sciancalepore, Angelo Capossele, Giuseppe Piro, Gennaro Boggia, Giuseppe Bianchi, Key management protocol with implicit certificates for IoT systems, in: Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems, in: IoT-Sys '15, Association for Computing Machinery, New York, NY, USA, 2015, pp. 37–42.

[50] Wiem Bekri, Rihab Jmal, Lamia Chaari Fourati, Softwarized internet of things network monitoring, IEEE Syst. J. 15 (1) (2021) 826–834.

[51] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga, A survey of intrusion detection in Internet of Things, J. Netw. Comput. Appl. 84 (2017) 25–37.

[52] Wenjuan Li, Steven Tug, Weizhi Meng, Yu Wang, Designing collaborative blockchained signature-based intrusion detection in IoT environments, Future Gener. Comput. Syst. 96 (2019) 481–489.

[53] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga, A survey of intrusion detection in Internet of Things, J. Netw. Comput. Appl. 84 (2017) 25–37.

[54] Abeer Alalmaie, Priyadarsi Nanda, Xiangjian He, Zero trust network intrusion detection system (NIDS) using auto encoder for attention-based CNN-BiLSTM, in: Proceedings of the 2023 Australasian Computer Science Week, ACSW '23, Association for Computing Machinery, New York, NY, USA, 2023, pp. 1–9.

[55] K.D. Uttecht, Zero Trust (ZT) Concepts for Federal Government Architectures, Technical Report, Massachusetts Inst of Tech Lexington, 2020.

[56] Alper Kerman, Oliver Borchert, Scott Rose, Allen Tan, Implementing a Zero Trust Architecture, National Institute of Standards and Technology (NIST), 2020.

[57] P. Baran, On distributed communications networks, IEEE Trans. Commun. Syst. 12 (1) (1964) 1–9.

[58] Kevin Hoffman, David Zage, Cristina Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Comput. Surv. 42 (1) (2009).

[59] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, Zero Trust Architecture, Technical Report, National Institute of Standards and Technology, 2020.

[60] Weili Han, Chang Lei, A survey on policy languages in network and security management, Comput. Netw. 56 (1) (2012) 477–489.

[61] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini, Security towards the edge: Sticky policy enforcement for networked smart objects, Inf. Syst. 71 (2017) 78–89.
[62] Mark Campbell, Beyond zero trust: Trust is a vulnerability, Computer 53 (10) (2020) 110–113.
[63] Steven Walker-Roberts, Mohammad Hammoudeh, Omar Aldabbas, Mehmet Aydin, Ali Dehghantanha, Threats on the horizon: Understanding security threats in the era of cyber-physical systems, J. Supercomput. 76 (2020) 2643–2664.
[64] Mengru Tsai, Shanhsin Lee, Shiuhpyng Winston Shieh, Strategy for implementing of zero trust architecture, IEEE Trans. Reliab. 73 (1) (2024) 93–100.
[65] Geoffrey Sanders, Timothy Morrow, Nataniel Richmond, Carol Woody, Integrating Zero Trust and Devsecops, Technical Report, Carnegie-Mellon Univ Pittsburgh Pa, 2021.
[66] Yu Chen, Kai Hwang, Wei-Shinn Ku, Collaborative detection of DDoS attacks over multiple network domains, IEEE Trans. Parallel Distrib. Syst. 18 (12) (2007) 1649–1662.
[67] Lampis Alevizos, Vinh Thong Ta, Max Hashem Eiza, Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review, Secur. privacy 5 (1) (2022) e191, e191 SPY-2021-0038.R2.
[68] Ignacio Velásquez, Angélica Caro, Alfonso Rodríguez, Authentication schemes and methods: A systematic literature review, Inf. Softw. Technol. 94 (2018) 30–37.
[69] M Antonakakis, T April, M Bailey, M Bernhard, E Bursztein, J Cochran, Z Durumeric, J Halderman, L Invernizzi, M Kallitsis, D Kumar, C Lever, X Ma, J Mason, D Menscher, C Seaman, N Sullivan, K Thomas, Y Zhou, Understanding the Mirai botnet, in: USENIX Security Symp., 2017, p. 18.
[70] Artur Marzano, David Alexander, Osvaldo Fonseca, Elverton Fazzion, Cristine Hoepers, Klaus Steding-Jessen, Marcelo H. P. C. Chaves, Ítalo Cunha, Dorgival Guedes, Wagner Meira, The evolution of bashlite and mirai IoT botnets, in: 2018 IEEE Symposium on Computers and Communications, ISCC, 2018, pp. 00813–00818.
[71] Christoph Buck, Christian Olenberger, André Schweizer, Fabiane Völter, Torsten Eymann, Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust, Comput. Secur. 110 (2021) 102436.
[72] David Haddon, Philip Bennett, The emergence of post Covid-19 zero trust security architectures, in: Information Security Technologies for Controlling Pandemics, Springer, 2021, pp. 335–355.
[73] Venkata Naga Satya Surendra Chimakurthi, The challenge of achieving zero trust remote access in multi-cloud environment, ABC J. Adv. Res. 9 (2) (2020) 89–102.
[74] Zillah Adahman, Asad Waqar Malik, Zahid Anwar, An analysis of zero-trust architecture and its cost-effectiveness for organizational security, Comput. Secur. 122 (2022) 102911.
[75] Casimer DeCusatis, Piradon Liengtiraphan, Anthony Sager, Mark Pinelli, Implementing zero trust cloud networks with transport access control and first packet authentication, in: 2016 IEEE International Conference on Smart Cloud, SmartCloud, IEEE, 2016, pp. 5–10.
[76] Zirak Zaheer, Hyunseok Chang, Sarit Mukherjee, Jacobus Van der Merwe, EZTrust: Network-independent zero-trust perimeterization for microservices, in: Proceedings of the 2019 ACM Symposium on SDN Research, SOSR '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 49–61.
[77] Naseer Amara, Huang Zhiqui, Awais Ali, Cloud computing security threats and attacks with their mitigation techniques, in: 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC, 2017, pp. 244–251.
[78] Abu Faisal, Mohammad Zulkernine, A secure architecture for TCP/UDP-based cloud communications, Int. J. Inf. Secur. 20 (2021).
[79] Fatima Hussain, Weiyue Li, Brett Noye, Salah Sharieh, Alexander Ferworn, Intelligent service mesh framework for api security and management, in: 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON, IEEE, 2019, pp. 0735–0742.
[80] Luca Ferretti, Federico Magnanini, Mauro Andreolini, Michele Colajanni, Survivable zero trust for cloud computing environments, Comput. Secur. 110 (2021) 102419.
[81] Zirak Zaheer, Hyunseok Chang, Sarit Mukherjee, Jacobus Van der Merwe, Eztrust: Network-independent zero-trust perimeterization for microservices, in: Proceedings of the 2019 ACM Symposium on SDN Research, 2019, pp. 49–61.
[82] Saima Mehraj, M. Tariq Banday, Establishing a zero trust strategy in cloud computing environment, in: 2020 International Conference on Computer Communication and Informatics, ICCCI, IEEE, 2020, pp. 1–6.
[83] Koshi Ishide, Satoshi Okada, Mariko Fujimoto, Takuho Mitsunaga, ML detection method for malicious operation in hybrid zero trust architecture, in: 2022 IEEE International Conference on Computing, ICOCO, 2022, pp. 264–269.
[84] Tao Chuan, Yao Lv, Zhenfei Qi, Linjiang Xie, Wei Guo, An implementation method of zero-trust architecture, in: Journal of Physics: Conference Series, Vol. 1651, IOP Publishing, 2020, 012010.
[85] Na Zhang, Tongjun Wang, Jingzhou Ji, Analysis of the US military's tactical cloud application based on zero trust, in: ICMLCA 2021; 2nd International Conference on Machine Learning and Computer Application, VDE, 2021, pp. 1–5.
[86] Dayna Eidle, Si Ya Ni, Casimer DeCusatis, Anthony Sager, Autonomic security for zero trust networks, in: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON, IEEE, 2017, pp. 288–293.
[87] Nabeel Sheikh, Mayur Pawar, Victor Lawrence, Zero trust using network micro segmentation, in: IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, IEEE, 2021, pp. 1–6.
[88] Dongyu Yang, Yue Zhao, Kaijun Wu, Xiaoyu Guo, Haiyang Peng, An efficient authentication scheme based on Zero Trust for UAV swarm, in: 2021 International Conference on Networking and Network Applications, NaNA, IEEE, 2021, pp. 356–360.
[89] Vivin Krishnan, C.S. Sreeja, Zero trust-based adaptive authentication using composite attribute set, in: 2021 IEEE 3rd PhD Colloquium on Ethically Driven Innovation and Technology for Society, PhD EDITS, IEEE, 2021, pp. 1–2.
[90] Theo Dimitrakos, Tezcan Dilshener, Alexander Kravtsov, Antonio La Marra, Fabio Martinelli, Athanasios Rizos, Alessandro Rosetti, Andrea Saracino, Trust aware continuous authorization for zero trust in consumer internet of things, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom, IEEE, 2020, pp. 1801–1812.
[91] Shanshan Zhao, Shancang Li, Fuzhong Li, Wuping Zhang, Muddesar Iqbal, Blockchain-enabled user authentication in zero trust internet of things, in: Security and Privacy in New Computing Environments: Third EAI International Conference, SPNCE 2020, Lyngby, Denmark, August 6-7, 2020, Proceedings 3, Springer, 2021, pp. 265–274.
[92] Binanda Sengupta, Anantharaman Lakshminarayanan, Distritrust: Distributed and low-latency access validation in zero-trust architecture, J. Inf. Secur. Appl. 63 (2021) 103023.
[93] Qiuqing Jin, Liming Wang, Zero-trust based distributed collaborative dynamic access control scheme with deep multi-agent reinforcement learning, EAI Endorsed Trans. Secur. Saf. 8 (27) (2020).
[94] Nakul Ghate, Shohei Mitani, Taniya Singh, Hirofumi Ueda, Advanced zero trust architecture for automating fine-grained access control with generalized attribute relation extraction, IEICE Proc. Ser. 68 (C1-5) (2021).
[95] Koudai Hatakeyama, Daisuke Kotani, Yasuo Okabe, 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, IEEE, 2021, pp. 514–519.
[96] Tian Xiaopeng, Song Haohao, A zero trust method based on BLP and BIBA model, in: 2021 14th International Symposium on Computational Intelligence and Design, ISCID, IEEE, 2021, pp. 96–100.

[97] Iftekhar Ahmed, Tahmin Nahar, Shahina Sultana Urmi, Kazi Abu Taher, Protection of sensitive data in zero trust model, in: Proceedings of the International Conference on Computing Advancements, 2020, pp. 1–5.

[98] Wenhua Huang, Xuemin Xie, Ziying Wang, JingYu Feng, Gang Han, Wenbo Zhang, ZT-Access: A combining zero trust access control with attribute-based encryption scheme against compromised devices in power IoT environments, Ad Hoc Netw. 145 (2023) 103161.

[99] Mayra Samaniego, Ralph Deters, Zero-trust hierarchical management in IoT, in: 2018 IEEE International Congress on Internet of Things, ICIOT, IEEE, 2018, pp. 88–95.

[100] Zhang Xiaojian, Chen Liandong, Fan Jie, Wang Xiangqun, Wang Qi, Power IoT security protection architecture based on zero trust framework, in: 2021 IEEE 5th International Conference on Cryptography, Security and Privacy, CSP, IEEE, 2021, pp. 166–170.

[101] G. Anil, A zero-trust security framework for granular insight on blind spot and comprehensive device protection in the Enterprise of Internet of Things (E-IOT), 2021.

[102] Yizhi Liu, Xiaohan Hao, Wei Ren, Ruoting Xiong, Tianqing Zhu, Kim-Kwang Raymond Choo, Geyong Min, A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things, IEEE Trans. Comput. (2022).

[103] Jin Wang, Jiahao Chen, Neal Xiong, Osama Alfarraj, Amr Tolba, Yongjun Ren, S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT, ACM Trans. Internet Technol. (2022) Just Accepted.

[104] Theo Dimitrakos, Tezcan Dilshener, Alexander Kravtsov, Antonio La Marra, Fabio Martinelli, Athanasios Rizos, Alessandro Rosetti, Andrea Saracino, Trust aware continuous authorization for zero trust in consumer internet of things, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom, 2020, pp. 1801–1812.

[105] D. Abhiram, R. Harish, K. Praveen, Zero-trust security implementation using SDP over VPN, in: Inventive Communication and Computational Technologies: Proceedings of ICICCT 2021, Springer, 2022, pp. 267–276.

[106] Pietro Colombo, Elena Ferrari, Engin Deniz Tümer, 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, IEEE, 2021, pp. 159–166.

[107] Syed W Shah, Naeem F Syed, Arash Shaghaghi, Adnan Anwar, Zubair Baig, Robin Doss, LCDA: lightweight continuous device-to-device authentication for a zero trust architecture (ZTA), Comput. Secur. 108 (2021) 102351.

[108] Andreas Gutmann, Karen Renaud, Joseph Maguire, Peter Mayer, Melanie Volkamer, Kanta Matsuura, Jörn Müller-Quade, Zeta-zero-trust authentication: Relying on innate human ability, not technology, in: 2016 IEEE European Symposium on Security and Privacy, Euro S&P, IEEE, 2016, pp. 357–371.

[109] Giovanni R. da Silva, Daniel F. Macedo, Aldri L. dos Santos, Zero trust access control with context-aware and behavior-based continuous authentication for smart homes, in: Anais Do XXI Simpósio Brasileiro Em Segurança Da Informação e de Sistemas Computacionais, SBC, 2021, pp. 43–56.

[110] Ling Wei, Huimin She, Chuanwei Li, Lele Zhang, Zero trust: Distributed and light-weight authentication for wormhole attacks in low-power and lossy networks, 2020.

[111] Sudakshina Mandal, Danish Ali Khan, Sarika Jain, Cloud-based zero trust access control policy: an approach to support work-from-home driven by COVID-19 pandemic, New Gener. Comput. 39 (3–4) (2021) 599–622.

[112] Thomas Lukaseder, Maya Halter, Frank Kargl, Context-based access control and trust scores in zero trust campus networks, in: SICHERHEIT 2020, Gesellschaft für Informatik eV, 2020.

[113] Taisho Sasada, Yuto Masuda, Yuzo Taenaka, Youki Kadobayashi, Doudou Fall, Zero-trust access control focusing on imbalanced distribution in browser clickstreams, in: 2021 Eighth International Conference on Software Defined Systems, SDS, IEEE, 2021, pp. 1–8.

[114] Ya Guang Wu, Wen Hao Yan, Jin Zhi Wang, Real identity based access control technology under zero trust architecture, in: 2021 International Conference on Wireless Communications and Smart Grid, ICWCSG, IEEE, 2021, pp. 18–22.

[115] Wengao Fang, Xiaojuan Guan, Research on ios remote security access technology based on zero trust, in: 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference, ITOEC, Vol. 6, IEEE, 2022, pp. 238–241.

[116] Romans Vanickis, Paul Jacob, Sohelia Dehghanzadeh, Brian Lee, Access control policy enforcement for zero-trust-networking, in: 2018 29th Irish Signals and Systems Conference, ISSC, IEEE, 2018, pp. 1–6.

[117] Brian Lee, Roman Vanickis, Franklin Rogelio, Paul Jacob, Situational awareness based risk-adapatable access control in enterprise networks, 2017, arXiv preprint arXiv:1710.09696.

[118] Chenchen Han, Gwang-Jun Kim, Osama Alfarraj, Amr Tolba, Yongjun Ren, ZT-BDS: A secure blockchain-based zero-trust data storage scheme in 6G edge IoT, J. Internet Technol. 23 (2) (2022) 289–295.

[119] Peirong Li, Wei Ou, Haozhe Liang, Wenbao Han, Qionglu Zhang, Guang Zeng, A zero trust and blockchain-based defense model for smart electric vehicle chargers, J. Netw. Comput. Appl. 213 (2023) 103599.

[120] Mukesh Soni, Dileep Kumar Singh, Blockchain-based group authentication scheme for 6G communication network, Phys. Commun. 57 (2023) 102005.

[121] Annapurna P Patil, Gaurav Karkal, Jugal Wadhwa, Meer Sawood, K Dhanush Reddy, Design and implementation of a consensus algorithm to build zero trust model, in: 2020 IEEE 17th India Council International Conference, INDICON, IEEE, 2020, pp. 1–5.

[122] Suparna Dhar, Indranil Bose, Securing IoT devices using zero trust and blockchain, J. Org. Comput. Electron. Commer. 31 (1) (2021) 18–34.

[123] Dawei Li, Enzhun Zhang, Ming Lei, Chunxiao Song, Zero trust in edge computing environment: a blockchain based practical scheme, Math. Biosci. Eng. 19 (4) (2022) 4196–4216.

[124] Abdullah Albuali, Tessema Mengistu, Dunren Che, ZTIMM: A zero-trust-based identity management model for volunteer cloud computing, in: Cloud Computing–CLOUD 2020: 13th International Conference, Held As Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings 13, Springer, 2020, pp. 287–294.

[125] D.M. Chess, C.C. Palmer, S.R. White, Security in an autonomic computing environment, IBM Syst. J. 42 (1) (2003) 107–118.

[126] Simone Rodigari, Donna O'Shea, Pat McCarthy, Martin McCarry, Sean McSweeney, Performance analysis of zero-trust multi-cloud, in: 2021 IEEE 14th International Conference on Cloud Computing, CLOUD, 2021, pp. 730–732.

[127] Shancang Li, Zero trust based internet of things, EAI Endorsed Trans. Internet Things 5 (20) (2019) e1.

[128] Safwa Ameer, Maanak Gupta, Smriti Bhatt, Ravi Sandhu, BlueSky: Towards convergence of zero trust principles and score-based authorization for IoT enabled smart systems, in: Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies, SACMAT '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 235–244.

[129] Yinghong Yang, Fenhua Bai, Zhuo Yu, Tao Shen, Yingli Liu, Bei Gong, An anonymous and supervisory cross-chain privacy protection protocol for zero-trust IoT application, ACM Trans. Sen. Netw. (2023) Just Accepted.

[130] Adel Atieh, Priyadarsi Nanda, Manoranjan Mohanty, A zero-trust framework for industrial internet of things, in: 2023 International Conference on Computing, Networking and Communications, ICNC, 2023, pp. 331–335.

[131] Liang Xue, Jianbing Ni, Dongxiao Liu, Xiaodong Lin, Xuemin Shen, Blockchain-based fair and fine-grained data trading with privacy preservation, IEEE Trans. Comput. (2023) 1–14.

[132] Sairath Bhattacharjya, A Novel Zerotrust Framework to Secure Iot Communications (PhD thesis), University of Kansas, 2020.

[133] Bruno Carneiro da Rocha, Laerte Peotta de Melo, Rafael Timóteo de Sousa, Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model, in: 2021 Workshop on Communication Networks and Power Systems, WCNPS, IEEE, 2021, pp. 1–6.

[134] Rong Zeng, Nige Li, Xiaoming Zhou, Yuanyuan Ma, Building a zero-trust security protection system in the environment of the power Internet of Things, in: 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology, AINIT, IEEE, 2021, pp. 557–560.
[135] Geir M. Køien, Zero-trust principles for legacy components: 12 rules for legacy devices: An antidote to chaos, Wirel. Pers. Commun. 121 (2) (2021) 1169–1186.
[136] Debashis Das, Sourav Banerjee, Kousik Dasgupta, Pushpita Chatterjee, Uttam Ghosh, Utpal Biswas, Blockchain enabled SDN framework for security management in 5G applications, in: Proceedings of the 24th International Conference on Distributed Computing and Networking, ICDCN '23, Association for Computing Machinery, New York, NY, USA, 2023, pp. 414–419.
[137] Mizna Khalid, Sufian Hameed, Abdul Qadir, Syed Attique Shah, Dirk Draheim, Towards SDN-based smart contract solution for IoT access control, Comput. Commun. 198 (2023) 1–31.
[138] Mikhail Zolotukhin, Timo Hämäläinen, Pyry Kotilainen, Intelligent solutions for attack mitigation in zero-trust environments, in: Cyber Security: Critical Infrastructure Protection, Springer, 2022, pp. 403–417.
[139] Deepak Puthal, Saraju P. Mohanty, Priyadarsi Nanda, Uma Choppali, Building security perimeters to protect network systems against cyber threats [future directions], IEEE Consum. Electron. Mag. 6 (4) (2017) 24–27.
[140] Antonio López Martínez, Manuel Gil Pérez, Antonio Ruiz-Martínez, A comprehensive review of the state-of-the-art on security and privacy issues in healthcare, ACM Comput. Surv. 55 (12) (2023).
[141] Sarah Qahtan, Khaironi Yatim, Hazura Zulzalil, Mohd Hafeez Osman, A.A. Zaidan, H.A. Alsattar, Review of healthcare industry 4.0 application-based blockchain in terms of security and privacy development attributes: Comprehensive taxonomy, open issues and challenges and recommended solution, J. Netw. Comput. Appl. 209 (2023) 103529.
[142] Rui Zhang, Rui Xue, Ling Liu, Security and privacy for healthcare blockchains, IEEE Trans. Serv. Comput. 15 (6) (2022) 3668–3686.
[143] Jigna J. Hathaliya, Sudeep Tanwar, An exhaustive survey on security and privacy issues in Healthcare 4.0, Comput. Commun. 153 (2020) 311–335.
[144] Shancang Li, Editorial: Zero trust based internet of things, EAI Endorsed Trans. Internet Things 5 (20) (2019) e1.
[145] Baozhan Chen, Siyuan Qiao, Jie Zhao, Dongqing Liu, Xiaobing Shi, Minzhao Lyu, Haotian Chen, Huimin Lu, Yunkai Zhai, A security awareness and protection system for 5G smart healthcare based on zero-trust architecture, IEEE Internet Things J. 8 (13) (2020) 10248–10263.
[146] Belal Ali, Mark A. Gregory, Shuo Li, Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model, in: 2021 31st International Telecommunication Networks and Applications Conference, Itnac, IEEE, 2021, pp. 192–197.
[147] Y. Bevish Jinila, S. Prayla Shyry, A. Christy, A multi-component-based zero trust model to mitigate the threats in internet of medical things, in: Data Engineering for Smart Systems: Proceedings of SSIC 2021, Springer, 2022, pp. 605–613.
[148] Dan Tyler, Thiago Viana, Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture, Appl. Sci. 11 (16) (2021) 7499.
[149] Lewis Golightly, Paolo Modesti, Rémi Garcia, Victor Chang, Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN, Cyber Secur. Appl. (2023) 100015.
[150] Xueping Liang, Charalambos Konstantinou, Sachin Shetty, Eranga Bandara, Ruimin Sun, Decentralizing cyber physical systems for resilience: An innovative case study from a cybersecurity perspective, Comput. Secur. 124 (2023) 102953.
[151] Thien Huynh-The, Thippa Reddy Gadekallu, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa, Madhusanka Liyanage, Blockchain for the metaverse: A review, Future Gener. Comput. Syst. 143 (2023) 401–419.
[152] Suparna Dhar, Indranil Bose, Securing IoT devices using zero trust and blockchain, J. Org. Comput. Electron. Commer. 31 (1) (2021) 18–34.
[153] Samia Masood Awan, Muhammad Ajmal Azad, Junaid Arshad, Urooj Waheed, Tahir Sharif, A blockchain-inspired attribute-based zero-trust access control model for IoT, Information 14 (2) (2023).
[154] Erikson Júlio De Aguiar, Bruno S. Faiçal, Bhaskar Krishnamachari, Jó Ueyama, A survey of blockchain-based strategies for healthcare, ACM Comput. Surv. 53 (2) (2020).
[155] Fei Tang, Shuai Ma, Yong Xiang, Changlu Lin, An efficient authentication scheme for blockchain-based electronic health records, IEEE Access 7 (2019) 41678–41689.
[156] Mohammed Shuaib, Shadab Alam, Mohammad Shabbir Alam, Mohammad Shahnawaz Nasir, Self-sovereign identity for healthcare using blockchain, Mater. Today: Proc. (2021).
[157] Sourav Saha, Anil Kumar Sutrala, Ashok Kumar Das, Neeraj Kumar, Joel J. P. C. Rodrigues, On the design of blockchain-based access control protocol for IoT-enabled healthcare applications, in: ICC 2020 - 2020 IEEE International Conference on Communications, ICC, 2020, pp. 1–6.
[158] Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi, Access control and privacy-preserving blockchain-based system for diseases management, IEEE Trans. Comput. Soc. Syst. (2022) 1–13.
[159] Maliha Sultana, Afrida Hossain, Fabiha Laila, Kazi Abu Taher, Muhammad Nazrul Islam, Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology, BMC Med. Inform. Decis. Mak. 20 (1) (2020) 1–10.
[160] Javier Junquera-Sánchez, Carlos Cilleruelo, Luis De-Marcos, José-Javier Martinez-Herráiz, Access control beyond authentication, Secur. Commun. Netw. 2021 (2021) 1–11.
[161] Li Zhao, Meng Sun, Binbin Yang, Junpeng Xie, Jiqiang Feng, Zero trust access authorization and control of network boundary based on cloud sea big data fuzzy clustering, J. Intell. Fuzzy Systems (Preprint) (2022) 1–13.
[162] Hany F. Atlam, Muhammad Ajmal Azad, Madini O. Alassafi, Abdulrahman A. Alshdadi, Ahmed Alenezi, Risk-based access control model: A systematic literature review, Future Internet 12 (6) (2020).
[163] 2022 Cyber safety insights report global results, 2023, bit.ly/43ez8kz. (Accessed 31 March 2023).
[164] New data shows FTC received 2.8 million fraud reports from consumers in 2021, 2023, http://bit.ly/413FelT. (Accessed 31 March 2023).
[165] Fei Tang, Chunliang Ma, Kefei Cheng, Privacy-preserving authentication scheme based on zero trust architecture, Digit. Commun. Netw. (2023).
[166] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, Dawn Song, Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication, IEEE Trans. Inf. Forensics Secur. 8 (1) (2013) 136–148.
[167] Arsalan Mosenia, Susmita Sur-Kolay, Anand Raghunathan, Niraj K. Jha, CABA: Continuous authentication based on BioAura, IEEE Trans. Comput. 66 (5) (2017) 759–772.
[168] Ingo Deutschmann, Peder Nordström, Linus Nilsson, Continuous authentication using behavioral biometrics, IT Prof. 15 (4) (2013) 12–15.
[169] Shivam Saxena, Bharat Bhushan, Mohd Abdul Ahad, Blockchain based solutions to secure IoT: Background, integration trends and a way forward, J. Netw. Comput. Appl. 181 (2021) 103050.
[170] Eman M. Abou-Nassar, Abdullah M. Iliyasu, Passent M. El-Kafrawy, Oh-Young Song, Ali Kashif Bashir, Ahmed A. Abd El-Latif, DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems, IEEE Access 8 (2020) 111223–111238.
[171] Dongxing Li, Wei Peng, Wenping Deng, Fangyu Gai, A blockchain-based authentication and security mechanism for IoT, in: 2018 27th International Conference on Computer Communication and Networks, ICCCN, 2018, pp. 1–6.
[172] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, Ahmed Serhrouchni, Bubbles of Trust: A decentralized blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) 126–142.

[173] Abbas Yazdinejad, Gautam Srivastava, Reza M. Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, Mohammed Aledhari, Decentralized authentication of distributed patients in hospital networks using blockchain, IEEE J. Biomed. Health Inf. 24 (8) (2020) 2146–2156.
[174] Sanjay Kak, Zero Trust Evolution & Transforming Enterprise Security (PhD thesis), California State University San Marcos, 2022.
[175] Bhabendu Kumar Mohanta, Debasish Jena, Utkalika Satapathy, Srikanta Patnaik, Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology, Internet Things 11 (2020) 100227.
[176] Seraphin B. Calo, Maroun Touna, Dinesh C. Verma, Alan Cullen, Edge computing architecture for applying AI to IoT, in: 2017 IEEE International Conference on Big Data, Big Data, 2017, pp. 3012–3016.
[177] Bimal Ghimire, Danda B. Rawat, Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things, IEEE Internet Things J. 9 (11) (2022) 8229–8249.
[178] Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, Aruna Seneviratne, Jun Li, H. Vincent Poor, Federated learning for internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor. 23 (3) (2021) 1622–1658.
[179] Latif U. Khan, Walid Saad, Zhu Han, Ekram Hossain, Choong Seon Hong, Federated learning for internet of things: Recent advances, taxonomy, and open challenges, IEEE Commun. Surv. Tutor. 23 (3) (2021) 1759–1799.