GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

A survey of security in zero trust network architectures

Kipkoech Denzel *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo.

GSC Advanced Research and Reviews, 2025, 22(02), 182-214

Publication history: Received on 12 December 2024; revised on 20 February 2025; accepted on 23 February 2025

Article DOI: https://doi.org/10.30574/gscarr.2025.22.2.0036

Abstract

Zero Trust Network Architecture (ZTNA) has emerged as a transformative paradigm in cybersecurity, aiming to address the limitations of traditional perimeter-based security models. By adopting a "never trust, always verify" approach, ZTNA enforces stringent access controls and continuous authentication, regardless of user location or device. This survey provides a comprehensive overview of security challenges, solutions, and advancements in ZTNA. It explores core principles such as least privilege access, micro-segmentation, and contextual identity verification. The paper also examines the integration of emerging technologies like artificial intelligence (AI), blockchain, and secure access service edge (SASE) in ZTNA implementations. Additionally, it discusses the effectiveness of ZTNA in mitigating advanced persistent threats, insider attacks, and lateral movement. Finally, the survey identifies current research gaps, practical deployment challenges, and future directions to enhance security in ZTNA, offering valuable insights for academics and practitioners alike.

Keywords: Security; ZNTA; Privacy; Authentication; Access Control

1. Introduction

In the evolving landscape of cybersecurity, the rapid adoption of cloud services, mobile devices, and remote work has introduced complexities that challenge traditional network security paradigms [1]-[3]. Historically, cybersecurity models have operated on the assumption of a trusted internal network protected by a well-defined perimeter. This approach, often referred to as the "castle-and-moat" model, assumes that threats originate outside the perimeter, while entities within are inherently trusted [4]-[6]. However, the rise of sophisticated cyber threats, such as advanced persistent threats (APTs), insider attacks, and ransomware, has rendered this approach insufficient.

Zero Trust Network Architecture (ZTNA) (shown in Figure 1) has emerged as a transformative paradigm to address these challenges. The core principle of ZTNA is encapsulated in the philosophy of "never trust, always verify." Unlike traditional models, ZTNA assumes that no user, device, or application should be trusted by default, whether inside or outside the network perimeter [7]-[10]. Instead, it enforces continuous authentication, authorization, and validation of security posture for every access request [11], regardless of the requester's location or the resource being accessed.

* Corresponding author: Kipkoech Denzel.

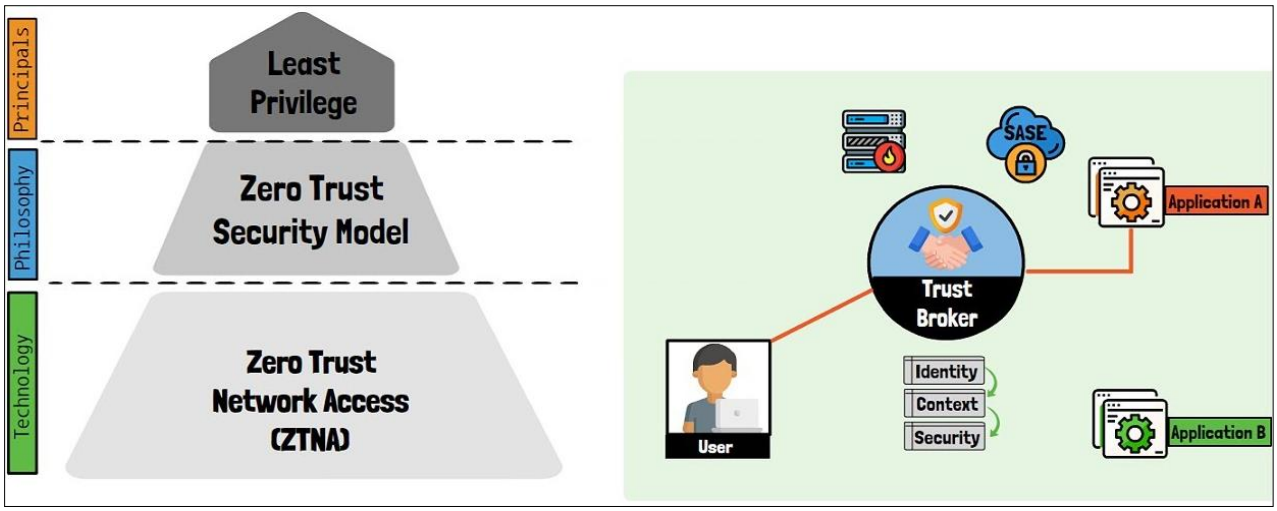

Figure 1 Zero trust network access

ZTNA is not a single technology but rather an architectural framework encompassing a suite of security practices and technologies [12]. These include identity and access management (IAM), multi-factor authentication (MFA), micro-segmentation, endpoint detection and response (EDR), and secure access service edge (SASE) [13], [14]. Together, these components create a robust security posture designed to mitigate lateral movement, reduce attack surfaces, and enhance visibility and control over network interactions.

This survey paper aims to provide a comprehensive exploration of security in ZTNA, highlighting its principles, advancements, and challenges. The objectives are threefold:

- To elucidate the foundational concepts and principles of ZTNA. This includes examining the shift from perimeter-based security to a more dynamic and adaptive security model that aligns with modern organizational needs.
- To survey the state-of-the-art technologies and frameworks that support ZTNA. This encompasses an analysis of existing solutions, their effectiveness in addressing security challenges, and their integration with emerging technologies such as artificial intelligence (AI), blockchain, and machine learning (ML).
- To identify research gaps and practical challenges in ZTNA deployment. This includes exploring issues such as scalability, interoperability, user experience, and cost-effectiveness, as well as proposing future research directions to address these challenges.

The remainder of this paper is structured as follows: Section 2 provides an overview of the key principles and components of ZTNA. Section 3 surveys current technologies and implementations, focusing on their strengths and limitations. Section 4 discusses challenges and open research questions in the field. Section 5 highlights emerging trends and future directions, and Section 6 concludes the survey by summarizing key insights and outlining actionable recommendations. By systematically analyzing security in ZTNA, this survey aims to serve as a valuable resource for researchers, practitioners, and decision-makers seeking to enhance their understanding of this critical domain in modern cybersecurity.

2. Key principles and components of zero trust network architecture

The ZTNA is a modern cybersecurity framework designed to protect systems, users, and data by assuming no entity, whether inside or outside the network, is inherently trustworthy [15]. The guiding principle of ZTNA is "never trust, always verify." This means that access to resources is granted only after stringent identity verification, and every access attempt is continuously monitored and validated.

2.1. Key principles of zero trust network architecture

The key principles of ZTNA are centered around the concept of "never trust, always verify," which challenges the traditional perimeter-based security model, as illustrated in Figure 2. Least privilege access ensures that users, devices,

and applications are granted only the minimal permissions needed to perform their tasks, thereby reducing the attack surface. Explicit verification mandates rigorous authentication and authorization [16] for every access request, often using multi-factor authentication and contextual data like user behavior and device health.

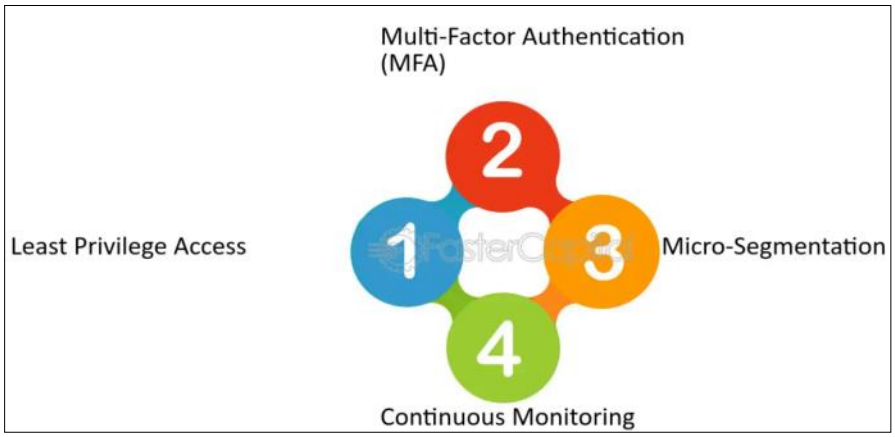

Figure 2 Some of the key principles of ZTNA

Micro-segmentation divides the network into smaller, isolated zones to limit lateral movement in the event of a breach [17]. Continuous monitoring and validation ensure that access permissions are dynamically adjusted based on real-time risk assessments. ZTNA also adopts an assume breach mentality, operating under the assumption that threats may already exist within the network, and focuses on mitigating damage through strict containment. These principles collectively create a robust and adaptive framework to counter evolving cybersecurity threats.

2.1.1. Least privilege access

Least privilege access is a core principle of zero trust network architecture, ensuring that users, devices, and applications are granted only the minimum level of access necessary to perform their tasks [18], [19]. By adhering to this principle, organizations can significantly reduce the attack surface and limit the potential damage in the event of a breach. Access permissions are tightly controlled and continuously evaluated, meaning that users or devices are only authorized to interact with specific resources based on their roles, responsibilities, and current context (e.g., location, device health, or time of access). This principle applies not only to users but also to applications and services, minimizing unnecessary inter-application communication and reducing opportunities for lateral movement [20], [21]. By enforcing granular, context-based access controls and restricting access to sensitive data and systems, ZTNA helps prevent unauthorized access [22] and ensures that security is maintained at all levels, from network perimeter to internal systems, contributing to a more robust defense against both internal and external threats.

2.1.2. Verify explicitly

"Verify explicitly" is a foundational principle of zero trust network architecture that emphasizes the need for continuous and rigorous verification of every access request, regardless of the source or location [23]. Unlike traditional security models that assume trust once a user or device is inside the perimeter, ZTNA requires every access attempt to be validated against strict criteria, such as user identity, device health, location, and behavior patterns [24], [25]. This explicit verification process often involves multi-factor authentication (MFA), real-time risk assessments, and contextual information to determine whether access should be granted or denied. It ensures that no entity is trusted by default, even if they are already within the network, reducing the likelihood of unauthorized access and mitigating the risks associated with compromised credentials or insider threats [26], [27]. By continuously validating the trustworthiness of all entities seeking access, ZTNA reinforces the "never trust, always verify" philosophy and enhances the overall security posture of the organization.

2.1.3. Micro-segmentation

Micro-segmentation in zero trust network architecture is a critical technique for isolating and protecting sensitive resources by dividing the network into smaller, manageable segments [28], [29]. This approach limits the lateral movement of potential attackers within the network, ensuring that even if an attacker compromises one segment, they cannot easily access other parts of the system. Figure 3 gives an illustration of a typical network micro-segmentation.

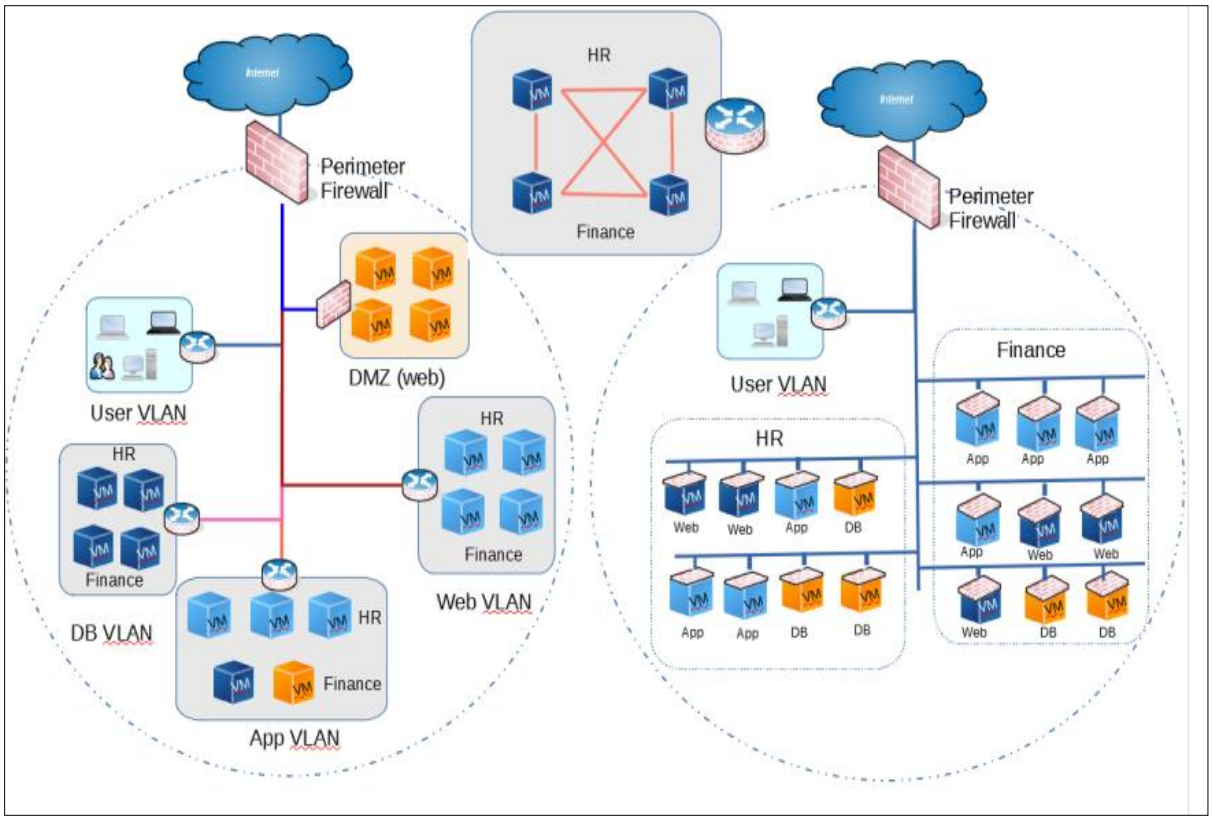

Figure 3 Micro-segmentation

Micro-segmentation involves applying granular security policies to control traffic flow between segments based on factors like user roles, device health, and application behavior [30]. This segmentation is enforced through software-defined networking (SDN) or other network virtualization technologies, allowing for dynamic, policy-driven control over which users or devices can communicate with specific resources [31], [32]. By minimizing trust within the network and controlling access at the most granular level, micro-segmentation strengthens the security model of ZTNA, reduces the attack surface, and enhances the overall resilience of the system against both external and internal threats.

2.1.4. Continuous monitoring and validation

Continuous monitoring and validation are fundamental to zero trust network architecture, ensuring that security policies are enforced dynamically and in real-time [33]. Unlike traditional models that assume a one-time verification of trust, ZTNA mandates that every user, device, and application is constantly monitored for compliance with security policies throughout their entire session [34], [35]. This ongoing process involves tracking user behavior, device health, network traffic, and environmental conditions to detect potential security risks or anomalies. If any deviation from expected behavior occurs, such as an unusual access pattern or compromised device, the system can trigger immediate responses, including re-authentication, access denial, or adjustment of privileges [36], [37]. This continuous vigilance enables ZTNA to adapt to emerging threats and evolving network conditions, providing a proactive security model that reduces the window of opportunity for attackers and ensures that all access remains valid and secure at all times.

2.1.5. Assume breach mentality

The "assume breach" mentality is a cornerstone of ZTNA, operating under the premise that threats may already exist within the network, whether from external attackers or insiders [38], [39]. Rather than assuming the network perimeter is secure, ZTNA assumes that any user, device, or system could be compromised and, therefore, treats all access requests as potentially malicious. This approach leads to a more proactive and defensive posture, where security measures are designed to minimize the damage of a breach by preventing unauthorized access, containing potential threats, and limiting lateral movement within the network [40], [41]. By assuming breach, ZTNA focuses on continuous validation, strict access controls, micro-segmentation, and real-time monitoring to mitigate the impact of any attack and ensure that any unauthorized activity is quickly detected and contained. This mentality shifts the focus from preventing breaches entirely to detecting and responding swiftly, thereby reducing risk and enhancing resilience.

2.1.6. Device and endpoint security

Device and endpoint security are critical components of zero trust network architecture, as they ensure that all devices accessing the network meet security standards [42] before being granted access to sensitive resources. In a Zero Trust model, every device—whether it's a laptop, smartphone, IoT device, or server—is treated as potentially compromised, and thus must be continuously verified for compliance with security policies. This includes checking device health, ensuring up-to-date software and security patches, and validating the integrity of device configurations [43], [44]. Endpoint Detection and Response (EDR) tools are often employed to monitor device activities and detect suspicious behaviors, while Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) systems help enforce security policies on mobile devices. Additionally, devices must pass authentication checks, such as multi-factor authentication, and be subject to continuous monitoring for any deviations that might indicate a security risk [45]-[47]. By focusing on securing devices and endpoints, ZTNA ensures that unauthorized or compromised devices cannot access critical resources, further reducing the attack surface and reinforcing the architecture's "never trust, always verify" philosophy.

2.1.7. Identity-centric security

Identity-centric security is a key principle in ZTNA, where the focus shifts from securing the network perimeter to securing individual identities—whether users, devices, or applications [48]. In this approach, the identity of each entity is continuously verified and authenticated before being granted access to resources, ensuring that only authorized individuals or systems can interact with sensitive data [49], [50]. Identity and Access Management (IAM) systems, often integrated with multi-factor authentication and single sign-on (SSO) solutions, play a pivotal role in managing these identities and ensuring secure authentication. Access decisions are based on a combination of factors such as the user's role, device health, location, and behavior, creating a context-aware, dynamic access model [51]. Identity-centric security also involves continuous monitoring to detect any anomalous or unauthorized behavior, ensuring that access permissions remain aligned with real-time risks. By making identity the central pillar of security, ZTNA reduces the risk of unauthorized access [52], insider threats, and credential-based attacks, thereby strengthening overall cybersecurity posture.

2.1.8. Data protection

Data protection in zero trust network architecture is a crucial element of its security model, ensuring that sensitive information is safeguarded from unauthorized access or breaches throughout its lifecycle [53]. In a Zero Trust environment, data is protected through a combination of encryption, access control policies, and continuous monitoring, irrespective of its location—whether on-premises, in the cloud, or in transit [54]. End-to-end encryption ensures that data is secure both at rest and in transit, preventing unauthorized users from intercepting or accessing it [55]. Additionally, ZTNA enforces granular access controls that limit data access based on the principle of least privilege, ensuring that only those with explicit authorization can view or manipulate sensitive information [56], [57].

Table 1 Key principles

Principle	**Discussion**
Least Privilege Access	Access is granted based on a strict "need-to-know" and "need-to-access" basis. Users, devices, and applications are given the minimum level of access required to perform their tasks, reducing the attack surface.
Verify Explicitly	Authentication and authorization are required for every access request. Verification is based on multiple factors such as user identity, device status, geolocation, and time of access.
Micro-Segmentation	The network is divided into smaller, isolated segments, limiting lateral movement of attackers. Access to each segment is controlled and monitored independently.
Continuous Monitoring and Validation	Security does not end after authentication; it is an ongoing process. User behaviors, device health, and network activity are constantly evaluated to detect anomalies.
Assume Breach Mentality	Organizations operate under the assumption that breaches will happen or may have already occurred.

	Security measures focus on minimizing the impact of a breach through containment and rapid incident response.
Device and Endpoint Security	Every device accessing the network is verified for compliance with security policies. This includes checking for proper patching, anti-malware software, and encryption.
Identity-Centric Security	Identity becomes the primary perimeter of security, replacing traditional network perimeters. Multi-factor authentication (MFA) and identity governance are critical components.
Data Protection	Data is classified and protected both at rest and in transit. Encryption, rights management, and strict access controls are applied to sensitive data.

Continuous monitoring allows for real-time detection of potential data breaches or misuse, while Data Loss Prevention (DLP) systems prevent unauthorized sharing or leakage of data. By embedding these data protection mechanisms into its core, ZTNA minimizes the risk of data exposure, ensuring that organizations can maintain confidentiality, integrity, and availability [58] while complying with regulatory requirements such as GDPR or HIPAA.

2.2. Components of zero trust network architecture

As shown in Figure 4, the zero trust network architecture comprises several interconnected components that work together to enforce its "never trust, always verify" approach [59]. Identity and Access Management plays a central role, ensuring secure authentication and authorization through mechanisms like single sign-on and multi-factor authentication. Endpoint security monitors and protects devices accessing the network, using tools such as Endpoint Detection and Response (EDR) and Mobile Device Management (MDM) [60].

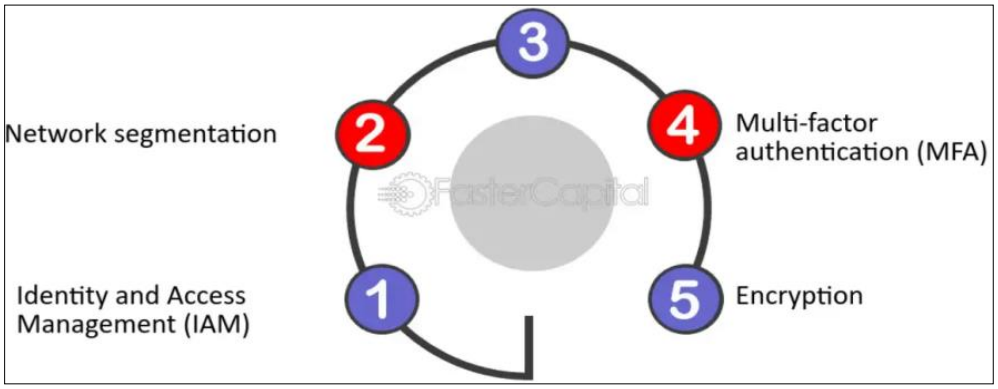

Figure 4 Components of ZTNA

Network segmentation isolates resources using software-defined perimeters and micro-segmentation to prevent lateral movement [61]. Security Information and Event Management (SIEM) and real-time analytics provide visibility into threats, while Data Loss Prevention (DLP) safeguards sensitive data. A Zero Trust policy engine enforces granular access controls based on context, such as user roles and device health. Additional components include Cloud Access Security Brokers (CASB) for extending ZTNA to cloud environments, encryption for secure communication [62], and behavioral analytics to detect anomalies. Together, these components create a dynamic and resilient security framework.

2.2.1. Identity and Access Management (IAM)

Identity and Access Management (IAM) is a fundamental component of ZTNA, enabling organizations to control and manage who can access their resources based on verified identities [63], as illustrated in Figure 5. IAM ensures that only authorized users, devices, or applications are granted access to specific data or services by using robust authentication and authorization mechanisms [64]-[66]. This typically includes the use of multi-factor authentication (MFA) to add an extra layer of security and single sign-on (SSO) to streamline user access while maintaining security.

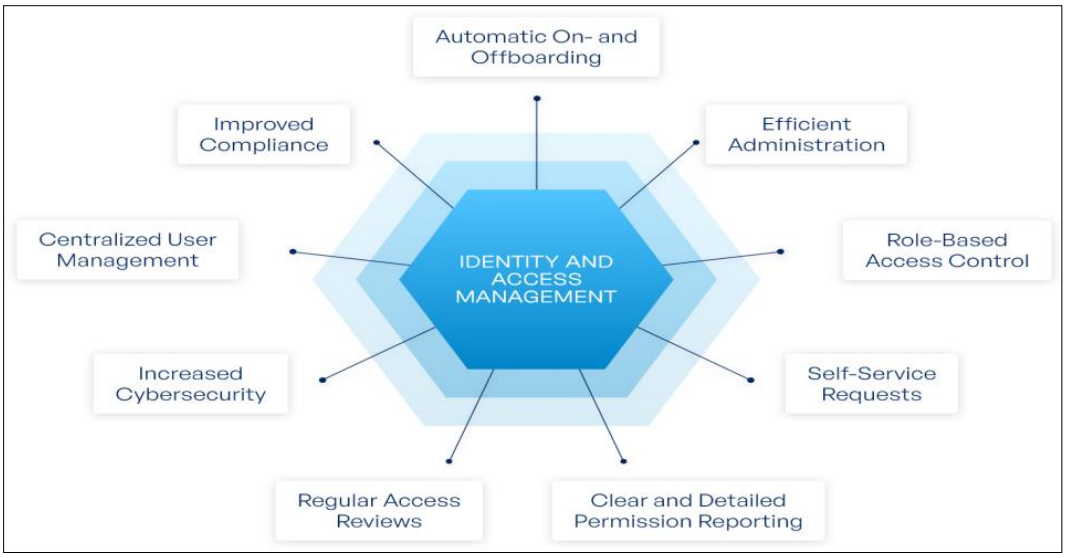

Figure 5 Identity and Access Management

IAM solutions continuously evaluate access requests in real time, taking into account various contextual factors such as user behavior, device health, location, and role within the organization. By integrating role-based access control (RBAC) or attribute-based access control (ABAC), IAM systems enforce the principle of least privilege, granting only the minimal permissions necessary for users to perform their tasks. This dynamic and adaptive approach to identity and access management [67] strengthens the Zero Trust model by ensuring that all access is explicitly verified, reducing the risk of unauthorized access, insider threats, and credential misuse.

2.2.2. Endpoint security

Endpoint security focuses on ensuring that every device—whether a workstation, mobile phone, or IoT device—meets security standards before it is allowed to access network resources [68], [69]. In ZTNA, each endpoint is considered potentially compromised, and therefore must be continuously monitored and validated for compliance with security policies. This involves checking the health and security posture of the device, such as ensuring it has the latest software updates, active antivirus protection, and no signs of malicious activity. Endpoint Detection and Response (EDR) tools are often deployed to detect, investigate, and respond to any suspicious behavior on the device [70]-[72]. Additionally, multi-factor authentication is commonly used to verify the identity of users accessing the network through these endpoints. By integrating endpoint security into the Zero Trust model, organizations can enforce strict access controls, prevent unauthorized devices from connecting, and ensure that compromised or non-compliant devices are quickly identified and isolated [73], thus reducing the overall attack surface and strengthening the network's security posture.

2.2.3. Network segmentation

Network segmentation is a fundamental security strategy that involves dividing the network into distinct segments or zones, each with its own security policies and access controls [74]. This approach limits the scope of potential attacks by preventing unauthorized users or compromised devices from freely moving across the entire network [75]. With micro-segmentation, ZTNA enforces strict identity-based access controls, ensuring that only authenticated and authorized users or devices can access specific segments, even within the same network [76]. By segmenting the network based on sensitivity and business needs, ZTNA enhances visibility and containment, allowing for more precise monitoring and quicker identification of potential threats. This segmentation also supports the principle of least privilege, ensuring users and systems can only access the resources they require. Overall, network segmentation in ZTNA strengthens security by reducing the attack surface [77], improving compliance, and minimizing the impact of a potential breach.

2.2.4. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) plays a critical role in providing real-time monitoring, analysis, and response to security events across the entire network [78]. SIEM systems aggregate and correlate data from various sources—such as endpoints, network devices, identity management systems, and applications—to detect unusual patterns, potential threats, or security breaches [79]. In the context of ZTNA, SIEM enhances the "never trust, always verify" approach by continuously monitoring every user, device, and access request, and evaluating them against

security policies [80], [81]. This enables the rapid detection of anomalies, such as unauthorized access attempts or deviations from normal behavior, which can trigger immediate responses like alerts, access revocation, or further investigation. By integrating SIEM with ZTNA's identity-based and context-aware security controls, organizations can achieve a comprehensive, proactive security posture [82] that not only helps prevent breaches but also accelerates incident response and supports compliance with regulatory requirements.

2.2.5. Data Loss Prevention (DLP)

Data loss prevention is a key component of zero trust network architecture, designed to protect sensitive data from being leaked, stolen, or improperly accessed [83]. In a ZTNA environment, DLP solutions enforce strict data handling policies across the network by continuously monitoring and analyzing data flows, both within the organization and at the network perimeter [84]. These solutions prevent unauthorized access or sharing of confidential information by blocking or restricting the movement of data based on predefined rules, such as file type, content, or user permissions. DLP systems can also detect anomalous behaviors, such as attempts to transfer large volumes of sensitive data or access from non-compliant devices, and trigger real-time alerts or preventive actions [85], [86]. By integrating DLP with the ZTNA model, organizations can ensure that sensitive data is only accessible to authorized individuals and devices, effectively mitigating the risk of data breaches, insider threats [87], and regulatory violations, while maintaining a secure and compliant environment.

2.2.6. Zero trust policy engine

The zero trust policy engine is responsible for defining, enforcing, and continuously evaluating security policies across the network [88]. It dynamically determines whether a user, device, or application is allowed to access specific resources based on a set of predefined rules that take into account factors such as user identity, device health, location, time, and the sensitivity of the requested resource [89]. The policy engine operates in real-time, ensuring that access decisions are made based on the current context and risk assessment, rather than relying on static, pre-established trust levels. By integrating with identity and access management systems, endpoint security, and other ZTNA components, the policy engine ensures that the "never trust, always verify" principle is applied consistently across the entire network [90], [91]. Additionally, the policy engine is flexible and adaptive, allowing organizations to quickly adjust security measures as new threats emerge or as user and device behaviors evolve. This centralized, dynamic control mechanism is essential for maintaining a secure, granular, and scalable Zero Trust environment.

2.2.7. Continuous Diagnostics and Mitigation (CDM)

Continuous Diagnostics and Mitigation (CDM) in ZTNA is a proactive security approach focused on continuously assessing, identifying, and responding to potential vulnerabilities and threats [92] in real-time. By constantly monitoring the security posture of devices, users, and network traffic, CDM enables organizations to detect emerging risks and automatically apply corrective actions, such as isolating compromised endpoints, adjusting access permissions, or enforcing security policy updates [93], [94]. In ZTNA, CDM integrates with other security systems, such as Identity and Access Management (IAM), Endpoint Detection and Response (EDR), and the Zero Trust Policy Engine, to ensure that every entity accessing the network is continuously verified and complies with security policies. This real-time visibility and response mechanism helps to mitigate potential threats before they can cause damage, ensuring a dynamic, adaptive security posture that evolves as new risks and vulnerabilities arise [95]. CDM enhances ZTNA by ensuring that the network remains resilient, adaptable, and secure, even in the face of constantly changing threats and network environments.

2.2.8. Cloud Access Security Broker (CASB)

A Cloud Access Security Broker (CASB) plays a vital role in zero trust network architecture by providing visibility and control over the use of cloud services [96], ensuring secure access to cloud-based applications and data. CASBs act as an intermediary between users and cloud services, enforcing security policies and protecting against threats [97] by continuously monitoring and evaluating user behaviors, data transfers, and access requests. In a Zero Trust model, CASBs are integrated with identity and access management systems to enforce granular access controls, ensuring that only authenticated and authorized users or devices can access cloud resources, based on predefined policies and contextual factors such as location or device health [98], [99]. Additionally, CASBs can enforce data protection measures, such as encryption, data loss prevention (DLP), and activity monitoring, helping to mitigate risks associated with cloud adoption, such as unauthorized access, data leakage, or shadow IT. By incorporating CASBs into ZTNA, organizations can achieve a secure and compliant environment for cloud resources, while maintaining strict access control and protecting sensitive data.

2.2.9. Encryption and secure communication

As depicted in Figure 6, encryption and secure communication are critical elements in zero trust network architecture, ensuring that data is protected both in transit and at rest, regardless of its location or the entity accessing it [100]-[102]. In a Zero Trust model, all communications, whether between users, devices, or applications, are encrypted to prevent unauthorized access and interception, even within the internal network. End-to-end encryption ensures that sensitive data remains unreadable to anyone without the proper decryption keys [103], while secure communication protocols, such as TLS and IPsec, are used to establish trusted connections and protect data integrity.

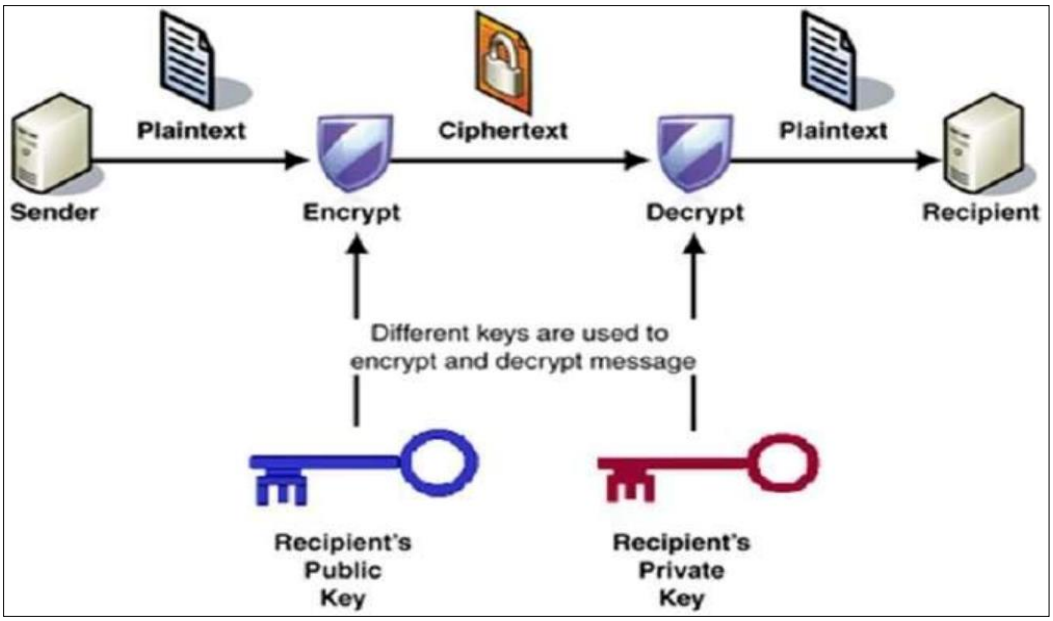

Figure 6 Encryption and secure communication

ZTNA applies encryption at multiple layers, securing both network traffic and application data, and uses mechanisms like public key infrastructure (PKI) and multi-factor authentication MFA to further strengthen the authentication and authorization process [104]. This comprehensive encryption strategy supports the "never trust, always verify" principle by ensuring that only legitimate, authenticated entities can decrypt and access data, reducing the risk of data breaches, man-in-the-middle attacks, and unauthorized access across the network.

2.2.10. Threat intelligence and behavioral analytics

Threat intelligence and behavioral analytics are key components of ZTNA that enhance security by enabling the proactive identification and mitigation of potential threats [105], as illustrated in Figure 7. Threat intelligence involves gathering, analyzing, and sharing data about emerging threats, vulnerabilities, and attack techniques, which helps organizations stay informed about the latest risks and take preventive actions [106], [107]. In a Zero Trust environment, threat intelligence is integrated into the decision-making process, enabling continuous monitoring and real-time threat detection across the network.

Behavioral analytics, on the other hand, focuses on analyzing the normal patterns of user and device activity to identify anomalies that could indicate malicious behavior, such as unauthorized access attempts, lateral movement, or data exfiltration [108], [109]. By leveraging these insights, ZTNA systems can adapt security policies dynamically, ensuring that access requests are continuously evaluated based on the latest threat intelligence and the behavioral context of the requesting entity. This combination of threat intelligence and behavioral analytics strengthens ZTNA's ability to detect and respond to sophisticated attacks, such as advanced persistent threats (APTs), before they can cause significant harm.

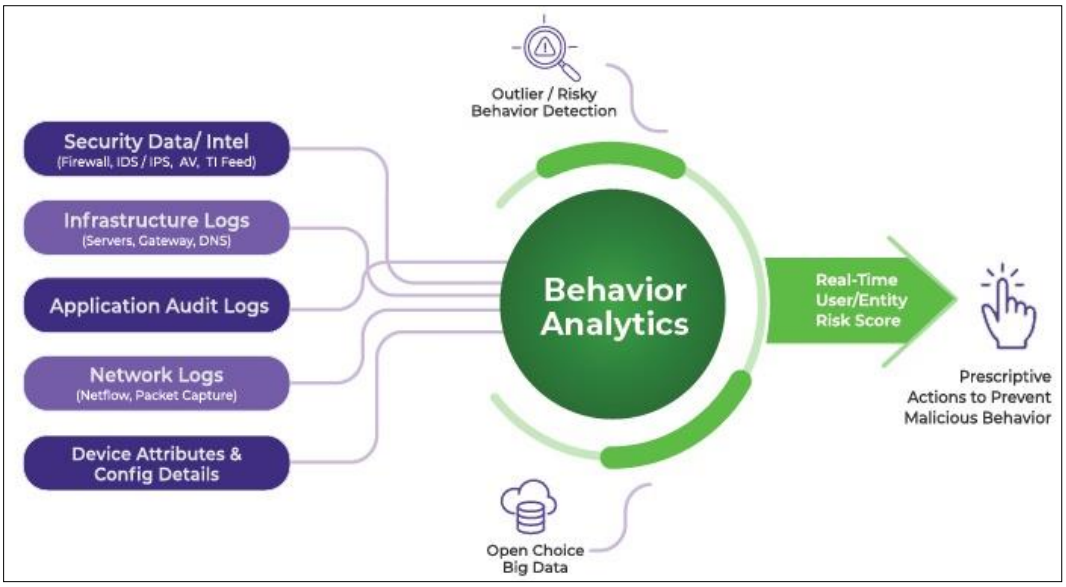

Figure 7 Threat intelligence and behavioral analytics

Table 2 Components of zero trust network architecture

Component	**Explanation**
Identity and Access Management (IAM)	Centralized management of user identities, roles, and permissions. Includes Single Sign-On (SSO), MFA, and adaptive authentication.
Endpoint Security	Continuous monitoring and management of devices accessing the network. Endpoint Detection and Response (EDR) and Mobile Device Management (MDM) solutions ensure device compliance.
Network Segmentation	Implementation of software-defined perimeters (SDP) and micro-segmentation. Controls lateral movement and isolates sensitive resources.
Security Information and Event Management (SIEM)	Aggregates and analyzes security logs from across the network. Provides real-time visibility into potential threats and supports threat hunting.
Data Loss Prevention (DLP)	Tools that prevent unauthorized access, sharing, or exfiltration of sensitive data. Enforces data protection policies across endpoints, emails, and cloud storage.
Zero Trust Policy Engine	Centralized system for defining and enforcing access policies. Evaluates access requests based on context, such as user role, device health, and location.
Continuous Diagnostics and Mitigation (CDM)	Ongoing assessment of vulnerabilities and configuration weaknesses. Automates remediation tasks to maintain a secure posture.
Cloud Access Security Broker (CASB)	Extends ZTNA principles to cloud environments. Provides visibility, compliance enforcement, and data protection for cloud applications.
Encryption and Secure Communication	Ensures that all data in transit and at rest is encrypted. Employs Transport Layer Security (TLS) and other encryption standards.
Threat Intelligence and Behavioral Analytics	Uses machine learning and artificial intelligence to detect and respond to advanced threats. Analyzes patterns in network traffic and user behavior to identify anomalies.

2.3. Benefits of zero trust architecture

Zero Trust Architecture (ZTA) offers several key benefits that significantly enhance an organization's cybersecurity posture [110]. Table 3 gives a summary of these benefits. One of the primary advantages is its reduced attack surface. Traditional perimeter-based security models operate under the assumption that threats exist only outside the network [111], leading to a false sense of security once inside the perimeter. In contrast, ZTA assumes that threats can exist both outside and inside the network, meaning no entity is trusted by default. This approach minimizes the attack surface by continually verifying every access request, regardless of whether the user or device is inside or outside the network perimeter. As a result, attackers who manage to bypass the perimeter defenses are less likely to gain lateral movement or escalate their privileges [112] within the network, making it harder for them to inflict significant damage.

Another major benefit of Zero Trust is improved data protection. ZTA ensures that data is always encrypted and access to sensitive information is tightly controlled, even within the internal network [113], [114]. By applying the principle of least privilege, where users and devices are granted only the minimal level of access necessary to perform their tasks, Zero Trust reduces the risk of unauthorized data access or data breaches. Furthermore, continuous monitoring and behavioral analytics help identify anomalies or unusual access patterns that might indicate potential data leaks or insider threats [115], allowing for immediate response and mitigating the impact of a breach before it escalates.

Table 3 Benefits of zero trust architecture

Merit	Description
Enhanced security	Reduces the risk of insider threats and external attacks by enforcing strict access controls.
Minimized attack surface	Micro-segmentation and least privilege access limit exposure to vulnerabilities.
Regulatory compliance	Helps meet requirements for data protection and privacy laws, such as GDPR and HIPAA.
Improved visibility	Provides granular monitoring of user and device activities across the network.
Scalability	Adaptable to hybrid and multi-cloud environments, ensuring consistent security across diverse infrastructures.

Zero Trust Architecture also enables greater flexibility and scalability, particularly as organizations increasingly adopt cloud environments, remote work, and IoT devices [116]-[118]. Traditional network security models struggle to scale with the growing number of endpoints and decentralized access points, which can lead to security gaps. ZTA, on the other hand, allows organizations to securely extend their network beyond the physical perimeter by applying the same rigorous identity verification and access controls to cloud services, remote users, and mobile devices [119]-[120]. This flexibility ensures that security policies are uniformly applied, regardless of where resources or users are located, facilitating secure collaboration across distributed teams and environments.

Furthermore, Zero Trust enhances visibility and control over network traffic, making it easier for organizations to monitor and audit access to critical resources [121]. With ZTA, every access request is logged, analyzed, and continuously monitored, providing security teams with real-time insights into who is accessing what, from where, and under what conditions. This level of transparency allows for better detection of suspicious activity, quicker identification of compromised credentials [122], and faster incident response times. The granular level of control also ensures that security policies can be tailored to specific users, devices, or applications, enabling organizations to enforce context-aware security measures and adapt to evolving threats.

Finally, Zero Trust Architecture offers improved compliance and regulatory adherence. Many industries are subject to strict regulatory requirements concerning data protection and privacy, such as GDPR, HIPAA, and PCI-DSS [123], [124]. Zero Trust's focus on strict identity verification, access control, data encryption, and audit trails helps organizations meet these compliance standards more effectively. Continuous monitoring and the ability to enforce policies at a granular level ensure that only authorized users can access sensitive data, and any violations or breaches can be quickly detected and addressed [125], [126]. As organizations face increasing pressure to protect sensitive information [127], ZTA provides a robust framework that simplifies compliance management and reduces the risk of non-compliance penalties.

3. Current technologies and implementations of ZTNA

Zero Trust Network Architecture is a subset of the broader Zero Trust security model, specifically focused on securing network access [128], [129]. As evidenced in Figure 8, it enforces stringent identity verification, continuous monitoring, and adaptive security policies to ensure that no user or device is inherently trusted. Table 4 presents an extensive discussion of the current technologies and implementations of zero trust network architecture, addressing its principles, technologies, deployment models, and applications.

Table 4 Current technologies and implementations

Technology/ implementation	**Discussion**
Core principles	*Least privilege access:* Users and devices are granted only the minimum permissions necessary. *Continuous verification*: Trust is dynamically assessed based on identity, device posture, and context. *Microsegmentation*: Network segments are isolated to restrict lateral movement in case of a breach. *Context-aware access*: Access decisions consider user roles, location, device health, and risk profiles. *Assume breach:* The architecture operates under the assumption that internal and external threats are ever-present.
Core technologies	a) Identity and Access Management (IAM) *Single Sign-On (SSO):* Streamlines authentication while maintaining security. *Multi-Factor Authentication (MFA)*: Adds layers of verification, such as biometrics or time-based one-time passwords. *Adaptive access control*: Grants or denies access based on contextual risk factors. b) Network Segmentation and Software-Defined Perimeters (SDP) *Microsegmentation:* Divides networks into smaller, isolated zones. *Software-Defined Perimeters (SDPs):* Conceal network resources and allow access only after authentication. c) Endpoint and device security *Endpoint Detection and Response (EDR):* Monitors and analyzes endpoint activities. *Mobile Device Management (MDM):* Ensures compliance with security policies on mobile devices. *Zero trust device posture assessment*: Validates device security before granting access. d) Secure Access Service Edge (SASE) *Cloud Access Security Brokers (CASBs):* Control access to cloud services and enforce security policies. *Secure Web Gateways (SWGs):* Protect against web-based threats. *Firewall as a Service (FWaaS):* Cloud-delivered firewalls for perimeter security. e) Encryption and secure communication *TLS/SSL encryption:* Secures data in transit between endpoints. *IPSec tunnels:* Provides secure communication for VPN alternatives in ZTNA. f) Behavioral and threat analytics

	AI-Powered behavioral analytics: Detect anomalies and adapt security policies dynamically. *Threat intelligence feeds:* Enhance ZTNA policies by incorporating real-time threat data.
Deployment models	*a) Agent-Based ZTNA* Requires an agent installed on endpoint devices. Pros: Granular access control, robust security. Cons: Complexity in managing and deploying agents. *Example:* Palo Alto Prisma Access. *b) Agentless ZTNA* Relies on browser-based access or reverse proxies for authentication. Pros: Simpler to deploy, ideal for unmanaged devices. Cons: Limited functionality compared to agent-based models. *Example*: ZScaler Private Access. *c) Cloud-Native ZTNA* Delivered as a cloud service, reducing the need for on-premise infrastructure. *Example:* Google BeyondCorp. *d) On-Premise ZTNA* Fully implemented within an organization's infrastructure. Pros: Full control over security policies. Cons: Requires significant resources and expertise. *Example:* Cisco TrustSec.
Current implementations	*a) Remote work enablement* Provides secure, seamless access to enterprise resources for remote employees. *Example:* Microsoft Azure AD Conditional Access. *b) Third-party and vendor access* Grants restricted access to external users without exposing the broader network. *Example:* Akamai Enterprise Application Access. *c) Multi-cloud and hybrid environments* Ensures consistent security policies across on-premise and cloud environments. *Example:* VMware Workspace ONE. *d) Compliance in regulated industries* Supports stringent security standards (e.g., HIPAA, PCI-DSS). *Example:* Okta Adaptive MFA and Identity Engine.

It is quite evident that current technologies and implementations of ZTNA are reshaping the cybersecurity landscape by prioritizing identity-centric access, device security, and adaptive policy enforcement. Leveraging advancements like multi-factor authentication [130], microsegmentation, software-defined perimeters (SDPs), and Secure Access Service Edge (SASE), ZTNA ensures secure, context-aware access to resources [132].

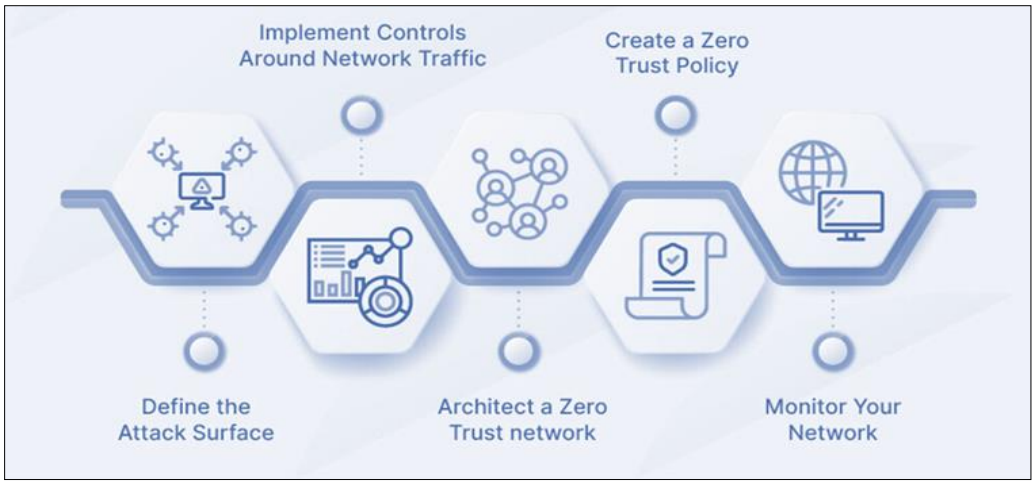

Figure 8 Steps in implementing ZTNA

It is widely deployed in both cloud-native and hybrid environments to address the challenges of remote work, third-party access, and IoT security [133]. Despite its robust capabilities, ZTNA implementations face challenges such as integration with legacy systems, potential performance trade-offs, and the complexity of policy management. However, with growing adoption of AI-driven analytics and edge computing, ZTNA is poised to remain a cornerstone of modern cybersecurity strategies.

4. Challenges and open research questions ZTNA

Implementing Zero Trust Architecture presents several challenges that organizations must navigate to fully realize its security benefits. Table 5 gives a summary of these challenges. One of the primary challenges is the complexity of deployment and integration with existing IT infrastructure [133], [134]. Transitioning from a traditional perimeter-based security model to Zero Trust requires a fundamental shift in how access is managed and monitored [135]. Organizations often have complex and diverse IT environments with legacy systems, third-party applications, and a mix of on-premises and cloud resources [136]. Integrating ZTA across these various environments can be time-consuming, costly, and technically challenging. It may require significant changes to existing network architectures, security tools, and operational processes, as well as coordination across multiple teams and departments.

Another significant challenge is managing and scaling identity and access management (IAM) systems. Zero Trust relies heavily on the concept of continuous identity verification [137], which demands a robust IAM framework to authenticate, authorize, and track users, devices, and applications. Ensuring that all entities are accurately and continuously authenticated can be complex, particularly for organizations with large and dynamic user bases [138], [139]. The challenge intensifies when dealing with third-party vendors, remote workers, or Internet of Things devices, which may not conform to the same standards of identity management. Additionally, implementing multi-factor authentication and other advanced security measures can introduce friction into the user experience [140]-[142], leading to potential resistance from employees or partners.

Table 5 Challenges in implementing ZTNA

Challenge	Explanation
Cultural and operational resistance	Shifting from legacy perimeter-based security to Zero Trust requires significant change management.
Complexity	Implementing micro-segmentation and continuous monitoring can be resource-intensive.
Integration issues	Ensuring compatibility with existing IT infrastructure and applications may pose challenges.
Skill gaps	Requires skilled cybersecurity professionals to design, implement, and manage the architecture.

The cost and resource requirements of implementing a Zero Trust framework can also be prohibitive for some organizations, especially small to medium-sized enterprises [144]. ZTA demands a combination of new technologies, such as advanced endpoint security, data loss prevention tools, security information and event management systems, and cloud access security brokers, which can entail significant upfront costs [146]. Furthermore, organizations must invest in continuous monitoring, threat intelligence, and behavioral analytics capabilities to support real-time access control and response [147]. In addition to the financial costs, implementing ZTA requires skilled cybersecurity professionals to manage and maintain the infrastructure, which can place a strain on existing resources and budgets.

Another challenge in implementing Zero Trust is user adoption and resistance. The core principle of Zero Trust—"never trust, always verify"—often requires significant changes to how users interact with systems and applications [148], [149]. The transition to ZTA involves shifting from traditional login-based access to continuous authentication, contextual access control, and frequent re-authentication [150], [151]. While these measures enhance security, they can create friction and inconvenience for users who are accustomed to more seamless access experiences. Employees may resist the perceived complexity or intrusiveness of continuous monitoring, multi-factor authentication, or restrictive access controls, which could lead to lower productivity or non-compliance [152]. Overcoming this resistance requires effective communication, user training, and possibly the integration of more user-friendly security measures.

Finally, monitoring and managing threats in real-time within a Zero Trust framework can be overwhelming due to the sheer volume of data generated by continuous monitoring and the complexity of real-time decision-making [153], [154]. ZTA demands that every access request be evaluated based on a dynamic risk assessment, considering numerous contextual factors such as user behavior, device health, location, and time of access. While this provides a high level of security, it can also lead to an overwhelming amount of alerts, data, and logs that security teams must analyze and respond to. Effective threat intelligence, machine learning, and behavioral analytics tools are essential to manage this flood of data [155], [156], but they also require substantial resources, expertise, and time to configure and operate efficiently. Balancing the need for detailed monitoring with the ability to respond quickly and appropriately to actual threats can be a significant hurdle for organizations.

Therefore, Zero Trust Network Architecture represents a paradigm shift in cybersecurity. By enforcing strict access controls, leveraging continuous monitoring, and assuming that breaches are inevitable, ZTNA offers robust protection against modern cyber threats [157], [158]. Although implementing ZTNA may be complex, its benefits far outweigh the challenges, making it an essential strategy for organizations aiming to secure their digital ecosystems.

5. Emerging trends and future directions

Zero Trust Network Architecture has emerged as a foundational framework for securing modern IT environments. While it has been widely adopted and researched, significant gaps remain in understanding, implementing, and scaling ZTNA in diverse contexts. Addressing these gaps and exploring future directions will enhance the framework's effectiveness and adaptability.

5.1. Research gaps in ZTNA

Despite its growing adoption, Zero Trust Network Architecture faces several research gaps that hinder its full potential, as summarized in Table 6. A lack of standardization leads to inconsistent implementations, complicating interoperability across organizations and platforms. Scalability challenges arise in large, distributed environments like IoT and multi-cloud systems, where managing granular policies and real-time monitoring becomes complex [159]. Policy management is another concern, as defining, updating, and enforcing detailed access controls across diverse systems is prone to errors.

Table 6 Research gaps

Gap	Explanation
Lack of standardization	*Gap:* Despite its popularity, ZTNA lacks a universally accepted standard or framework, leading to varied interpretations and implementations [160]. *Impact:* Inconsistent implementations can result in vulnerabilities [161], interoperability issues, and inefficiencies. *Example:* Organizations may implement ZTNA differently, complicating integration across supply chains or multi-cloud environments.

Scalability challenges	*Gap:* Scaling ZTNA in large, distributed environments, especially in hybrid and multi-cloud setups, remains complex [162]. *Impact:* The increased number of devices, users, and connections can strain policy engines, authentication systems, and monitoring tools [163]. *Example:* IoT networks with millions of devices face significant challenges in policy enforcement and monitoring [164], [165].
Usability and user experience	*Gap:* Overly stringent access controls [166] can disrupt workflows and negatively impact user experience. *Impact:* Users may seek workarounds, creating new vulnerabilities. *Example:* Excessive reauthentication requirements can frustrate users and reduce productivity [167].
Evolving threat landscape	*Gap:* ZTNA principles are not fully equipped to handle advanced threats like AI-driven attacks, quantum computing-based decryption [168], and zero-day vulnerabilities. *Impact:* These sophisticated attacks can bypass traditional ZTNA defenses. *Example:* AI-powered phishing attacks that impersonate trusted entities to compromise credentials [169].
Integration with emerging technologies	*Gap:* ZTNA integration with emerging technologies such as blockchain, edge computing, and AI/ML remains underexplored [170]. *Impact:* Lack of integration reduces the effectiveness of ZTNA in leveraging these technologies for enhanced security. *Example:* Blockchain could offer decentralized identity verification [171], but its use in ZTNA is limited.
Policy management complexity	*Gap:* Managing and updating granular access policies across diverse systems and user groups is complex [172]. *Impact:* Errors in policy configuration can lead to security gaps or excessive restrictions. *Example:* Defining consistent policies for a workforce spread across multiple geographies and devices.
Real-time monitoring and response	*Gap:* Real-time threat detection [173] and response are critical but challenging to achieve in ZTNA due to the volume and velocity of data. *Impact:* Delayed responses to threats can lead to significant damage. *Example:* A compromised device in a ZTNA framework might not be immediately flagged, allowing lateral movement.

Additionally, usability issues emerge when stringent access requirements disrupt workflows, pushing users toward insecure workarounds. ZTNA's ability to handle the evolving threat landscape, including AI-driven attacks and quantum computing risks, remains underexplored. Furthermore, integrating ZTNA with emerging technologies like blockchain and edge computing is limited, and more work is needed to address privacy concerns when monitoring user activities. Addressing these gaps is critical for enhancing ZTNA’s effectiveness and adaptability in securing modern digital ecosystems.

5.2. Future directions in ZTNA

The future of zero trust network architecture lies in advancing its adaptability, scalability, and integration with emerging technologies, as illustrated in Table 7. Developing universal standards is essential to ensure consistent implementation and interoperability across diverse environments [174], [175]. AI and machine learning will play a pivotal role in automating threat detection, behavioral analysis, and dynamic policy enforcement, reducing reliance on manual processes. As quantum computing threatens traditional encryption, adopting quantum-resistant cryptography will enhance the resilience of ZTNA. Efforts to secure IoT and edge computing environments will involve lightweight authentication mechanisms [176] and localized analytics for real-time threat mitigation. Enhancing privacy-preserving technologies like differential privacy and secure multi-party computation will address concerns about user data monitoring [177]-[181]. Additionally, context-aware access control will enable richer decision-making by factoring in real-time user behavior, device health, and environmental conditions [182]. Collaborative efforts in threat intelligence

sharing and extending ZTNA principles to supply chains and federated ecosystems will further strengthen its impact, making ZTNA a cornerstone of future cybersecurity strategies.

5.3. Development of universal standards

The development of universal standards in Zero Trust Network Architecture is crucial to ensuring consistency, interoperability, and scalability across diverse environments and organizations [183], [184]. Currently, the lack of universally accepted guidelines leads to fragmented implementations of ZTNA, which can result in security gaps, inefficiencies, and integration challenges [185]. Establishing standardized frameworks would enable organizations to adopt ZTNA more effectively, facilitating seamless communication and trust management across multi-cloud, hybrid, and cross-organizational infrastructures. These standards would cover critical aspects such as identity verification, access controls [186], and policy enforcement, ensuring a unified approach to security across different systems and technologies. Collaborative efforts among industry groups, government agencies, and standards organizations (e.g., NIST, ISO) are needed to define these standards and promote best practices, ultimately enabling organizations to implement ZTNA with confidence and improving the overall cybersecurity posture across industries.

5.4. Integration with artificial intelligence and machine learning

Integrating Artificial Intelligence and Machine Learning into Zero Trust Network Architecture holds the potential to significantly enhance security by automating threat detection, policy enforcement, and decision-making processes [187], [188]. AI and ML can analyze vast amounts of network traffic, user behavior, and device health data to identify anomalies and predict potential security threats in real-time [189]-[191]. These technologies enable adaptive authentication by adjusting access permissions based on evolving risk factors, such as changes in user behavior, device compliance, or environmental conditions. AI/ML-powered systems can also automate the creation and adjustment of access policies [192], reducing human error and ensuring more dynamic, context-aware security decisions. Furthermore, machine learning algorithms can continuously improve their ability to recognize sophisticated threats, such as AI-driven attacks or zero-day vulnerabilities, by learning from historical data and emerging patterns. The integration of AI and ML into ZTNA will thus enable more proactive, efficient, and adaptive security solutions in increasingly complex and dynamic digital ecosystems**.**

5.5. Quantum-resistant cryptography

Quantum-resistant cryptography is becoming an essential component of Zero Trust Network Architecture as the advent of quantum computing threatens to undermine traditional encryption methods [193], [194]. Quantum computers, with their ability to perform complex calculations at unprecedented speeds, have the potential to break widely used cryptographic algorithms such as RSA and ECC (Elliptic Curve Cryptography) [195], [196]. To mitigate this risk, quantum-resistant algorithms (also known as post-quantum cryptography) are being developed to ensure the continued security of communications, data, and authentication processes within a Zero Trust framework. These algorithms, which are designed to be secure even against the capabilities of quantum computers, must be integrated into ZTNA to protect sensitive data and maintain the integrity of identity and access management systems. Implementing quantum-resistant cryptography will be crucial for future-proofing ZTNA and ensuring that security remains robust as quantum computing evolves [197], [198]. This integration will involve adopting new cryptographic standards, updating legacy systems, and ensuring that ZTNA solutions are resilient to both classical and quantum threats.

5.6. Enhanced IoT and Edge Security

Enhanced IoT and edge security in zero trust network architecture is crucial due to the growing number of interconnected devices and the decentralized nature of edge computing environments [199]. IoT devices, often resource-constrained and distributed across various locations, present unique security challenges, such as weak authentication, limited monitoring capabilities, and susceptibility to attacks [200], [201]. In a Zero Trust framework, every device—whether IoT or edge-based—must be authenticated and continuously validated for compliance with security policies before being granted access to the network. Micro-segmentation and context-aware access control play a key role in isolating and securing IoT devices and edge nodes [202], ensuring that even if one device is compromised, the rest of the network remains protected. Additionally, lightweight authentication mechanisms, such as device certificates and behavioral analytics, are essential for validating devices in real-time without degrading performance [203]-[206]. Edge-based security solutions, including local threat detection and policy enforcement, enable faster responses to security incidents, reducing reliance on centralized systems. By integrating ZTNA principles with robust IoT and edge security strategies, organizations can ensure that their decentralized and rapidly expanding networked environments remain secure, resilient, and compliant.

5.7. Privacy-preserving technologies

Privacy-preserving technologies are essential in ensuring that stringent security measures do not compromise user privacy [207]. As ZTNA requires continuous monitoring of user behavior, device health, and access requests, it is crucial to implement privacy-enhancing techniques that protect sensitive data while maintaining robust security [208]. Technologies such as differential privacy, homomorphic encryption, and secure multi-party computation can be used to anonymize and encrypt data, ensuring that user information is not exposed during verification processes or data analysis [209]-[211]. These methods allow organizations to enforce strict access controls and monitor activities without violating privacy regulations or undermining user trust. Furthermore, adopting data minimization practices [212], where only essential information is collected and retained, helps balance security with privacy. By integrating these privacy-preserving technologies into ZTNA, organizations can safeguard sensitive data, comply with privacy regulations like GDPR, and maintain a high level of user confidence while enforcing a secure, zero-trust environment.

5.8. Automated policy management

Automated policy management in zero trust network architecture plays a critical role in simplifying and streamlining the creation, enforcement, and adjustment of security policies across dynamic and complex environments [213]. Figure 9 presents a typical policy management lifecycle. Traditional manual policy management can be error-prone, time-consuming, and difficult to scale, particularly in large organizations with diverse systems, user roles, and access requirements [214]. By leveraging automation, ZTNA can dynamically generate, update, and enforce access policies based on real-time factors such as user identity, device health, location, and behavior [215].

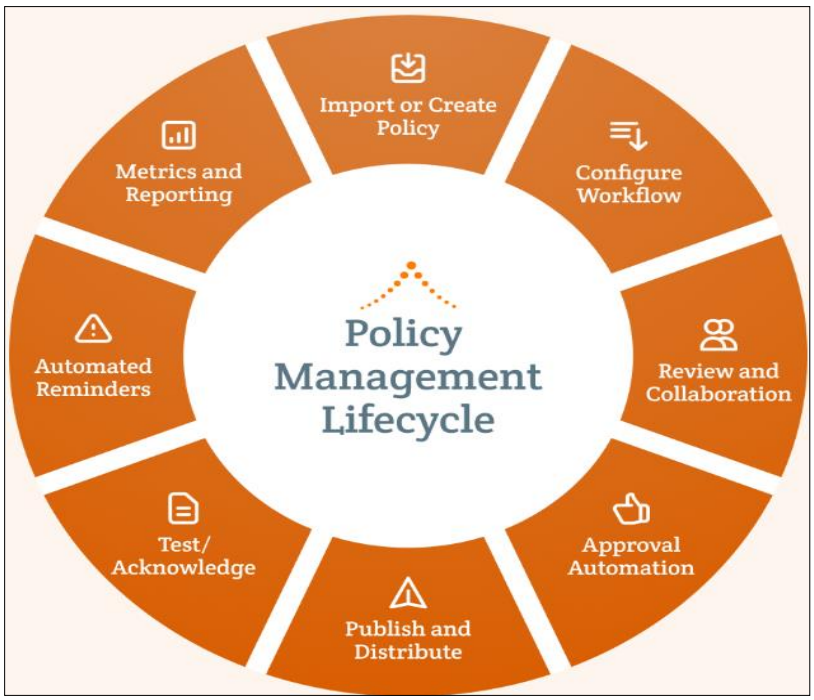

Figure 9 Policy management lifecycle

Policy-as-code frameworks and machine learning models can be used to automatically assess risk and adjust policies accordingly, ensuring that security measures remain consistent and effective even as the network evolves. Additionally, automated tools can integrate with existing identity and access management systems [216] to maintain a continuous, adaptive security posture. This automation not only reduces the administrative burden but also minimizes human error, making it easier to enforce least-privilege access and adapt to changing security needs, thereby enhancing the overall efficiency and effectiveness of ZTNA implementations.

5.9. Context-aware access control

Context-aware access control is a fundamental aspect of zero trust network architecture, as it enables more granular and dynamic decision-making for granting access to resources [217]. As shown in Figure 10, rather than relying solely on static rules or a simple user-password validation, context-aware access control evaluates multiple factors—such as the user's role, device health, location, time of access, and the sensitivity of the requested resource—to determine

whether access should be granted [218], [219]. By continuously assessing the risk associated with each access request in real-time, ZTNA can enforce adaptive policies that reflect the current security context, making it harder for attackers to bypass defenses [220]. For example, if a user attempts to access a critical resource from an unrecognized device or a location outside their usual pattern, the system may trigger additional authentication [221] steps or deny access altogether. This dynamic, context-sensitive approach ensures that access decisions are tailored to the situation at hand, improving both security and user experience by aligning access permissions with actual risk levels.

5.10. Collaboration across ecosystems

Collaboration across ecosystems is essential for securing multi-organizational environments, where trust and security must be maintained between different partners, suppliers, and stakeholders [222]. In such interconnected ecosystems, traditional perimeter-based security models are insufficient, as data and resources often need to be shared across multiple entities with varying security postures.

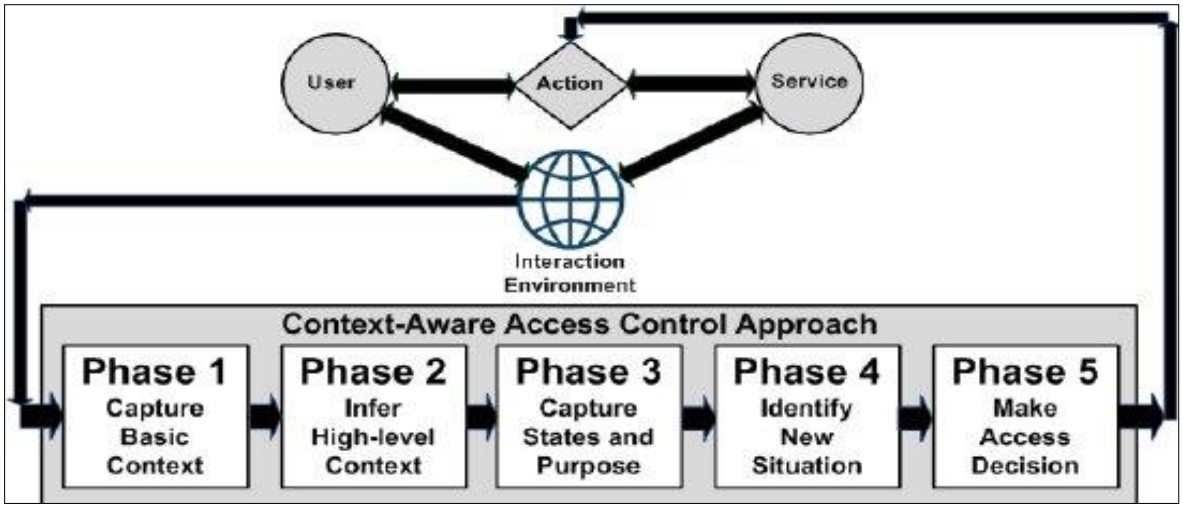

Figure 10 Context-aware access control

ZTNA enables secure collaboration by applying consistent, policy-driven access controls and continuous verification across organizational boundaries [223]. This is achieved through federated identity systems, which allow secure and seamless user authentication across disparate environments, and secure communication protocols that protect data in transit. Moreover, shared threat intelligence and common security frameworks can enhance the collective defense by allowing organizations to respond to emerging threats more effectively [224], [225]. By ensuring that all entities within the ecosystem adhere to the same stringent Zero Trust principles—regardless of their internal security measures—ZTNA fosters secure, collaborative interactions while minimizing the risk of external breaches or data leaks.

5.11. Improved threat intelligence sharing

Improved threat intelligence sharing is a crucial aspect of enhancing collective cybersecurity defense across organizations and ecosystems. Given the dynamic and evolving nature of cyber threats [226], sharing real-time threat intelligence enables organizations to rapidly detect, understand, and mitigate attacks before they escalate [227]. ZTNA fosters secure and controlled sharing of threat data through secure communication channels, anonymized data exchanges, and trusted third-party platforms that ensure privacy and confidentiality. By integrating threat intelligence with ZTNA's continuous monitoring and adaptive access controls, organizations can more effectively anticipate and respond to emerging threats, such as advanced persistent threats (APTs) or zero-day vulnerabilities [228]-[233]. Collaborative intelligence sharing allows for faster identification of attack patterns, improved detection capabilities, and the rapid dissemination of threat insights across different entities, strengthening the overall security posture of the broader network. In this way, ZTNA creates a dynamic, proactive approach to cybersecurity where shared knowledge significantly enhances resilience and mitigates the impact of potential security breaches.

Table 7 Future directions

Research direction	Discussion
Development of universal standards	*Goal:* Create standardized frameworks and guidelines for ZTNA implementation. *Approach:* Collaborate among industry groups, governments, and standards organizations like NIST to establish best practices. *Outcome:* Improved interoperability, consistency, and security across implementations.
Integration with AI and ML	*Goal:* Leverage AI/ML to enhance threat detection, behavioral analysis, and automated policy management. *Approach:* Use ML models to identify anomalous behaviors and adapt policies dynamically. Employ AI to optimize resource allocation for authentication and monitoring systems. *Outcome:* Improved threat detection, reduced manual effort, and dynamic adaptation to changing conditions.
Quantum-resistant cryptography	*Goal:* Prepare ZTNA for a future where quantum computing may render traditional cryptographic methods obsolete. *Approach:* Research and adopt quantum-resistant encryption algorithms for securing communications and data. *Outcome:* Enhanced resilience against quantum computing threats.
Enhanced IoT and edge security	*Goal:* Extend ZTNA principles to secure IoT and edge computing environments. *Approach:* Develop lightweight authentication and monitoring mechanisms for resource-constrained IoT devices. Use edge-based analytics for localized threat detection and policy enforcement. *Outcome:* Improved security for distributed and resource-constrained environments.
Privacy-preserving technologies	*Goal:* Ensure user privacy while implementing ZTNA, especially in data-sensitive industries like healthcare and finance. *Approach:* Employ technologies such as homomorphic encryption and differential privacy. Limit data collection to the minimum necessary for security. *Outcome:* Enhanced trust and compliance with privacy regulations.
Automated policy management	*Goal:* Simplify policy creation, management, and updates. *Approach:* Develop tools for automated policy generation based on user roles, behaviors, and environmental conditions. Use policy-as-code frameworks for consistency and scalability. *Outcome:* Reduced errors and administrative overhead in policy management.
Context-aware access control	*Goal:* Incorporate richer context into access control decisions. *Approach:* Use geolocation, device health, time of access, and user activity patterns to determine access levels. Continuously evaluate and adapt access permissions based on real-time context. *Outcome:* More accurate and adaptive access control.
Collaboration across ecosystems	*Goal:* Enable seamless ZTNA adoption across organizational boundaries, supply chains, and ecosystems. *Approach:*

	Develop federated identity systems for secure collaboration between organizations. Standardize APIs and protocols for interoperability. *Outcome:* Streamlined and secure inter-organization interactions.
Improved threat intelligence sharing	*Goal:* Foster collaboration among organizations for sharing threat intelligence. *Approach:* Establish platforms and frameworks for secure and anonymized intelligence sharing. Use AI to aggregate and analyze shared intelligence for actionable insights. *Outcome:* Enhanced collective defense against evolving threats.

While Zero Trust Network Architecture has established itself as a critical cybersecurity framework, research gaps and implementation challenges hinder its full potential. Addressing these gaps through standardization, integration with emerging technologies, and enhanced automation will pave the way for a more secure and adaptive ZTNA. As organizations increasingly embrace digital transformation, the evolution of ZTNA will remain a cornerstone in building resilient and future-ready cybersecurity architectures.

6. Conclusion

Zero Trust Network Architecture (ZTNA) has emerged as a transformative paradigm in modern cybersecurity, challenging traditional perimeter-based approaches. Its principles—such as "never trust, always verify," least privilege access, and continuous monitoring—provide a robust framework to address evolving threats in hybrid, multi-cloud, and distributed environments. This survey has examined the core concepts, implementation strategies, and key components of ZTNA while highlighting its benefits, challenges, and diverse applications across industries. Despite its advantages, the adoption of ZTNA is not without challenges. Issues such as lack of standardization, scalability concerns, and the complexity of policy management remain significant hurdles. Moreover, the evolving threat landscape, driven by advancements in AI, IoT, and quantum computing, demands continuous innovation in ZTNA strategies. Research gaps in areas such as real-time monitoring, seamless integration with emerging technologies, and privacy-preserving mechanisms present opportunities for future exploration. Looking ahead, the future of ZTNA lies in the convergence of advanced technologies such as AI/ML, blockchain, and quantum-resistant cryptography to enhance threat detection, policy automation, and data protection. Collaborative efforts among researchers, industry leaders, and policymakers will be critical to establishing standardized frameworks and addressing interoperability challenges. By bridging these gaps, ZTNA can evolve into a more adaptive, resilient, and universally applicable architecture. In a nutshell, ZTNA represents a paradigm shift in cybersecurity, offering a proactive and comprehensive approach to securing digital ecosystems. As organizations navigate an increasingly complex and interconnected world, ZTNA's principles will play a pivotal role in shaping the future of secure, efficient, and scalable network architectures.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that he holds no conflict of interest.

References

[1] Hussain SM, Tummalapalli SR, Chakravarthy AS. Cyber Security Education: Enhancing Cyber Security Capabilities, Navigating Trends and Challenges in a Dynamic Landscape. Advances in Cyber Security and Digital Forensics. 2024:9-33.

[2] Daniel SA, Victor SS. Emerging Trends in Cybersecurity for Critical Infrastructure Protection: A Comprehensive Review. Computer Science & IT Research Journal. 2024 Mar 10;5(3):576-93.

[3] Obi OC, Dawodu SO, Daraojimba AI, Onwusinkwue S, Akagha OV, Ahmad IA. Review of evolving cloud computing paradigms: security, efficiency, and innovations. Computer Science & IT Research Journal. 2024 Feb 2;5(2):270-92.

[4] Nadji B. Data Security, Integrity, and Protection. InData, Security, and Trust in Smart Cities 2024 Jun 27 (pp. 59-83). Cham: Springer Nature Switzerland.

[5] Daah C, Qureshi A, Awan I, Konur S. Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. Electronics. 2024 Feb 23;13(5):865.

[6] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. A Review on IoTs Applications and Security Threats via Data Transfer over Networks. InComputer Science On-line Conference 2024 Apr 25 (pp. 562-579). Cham: Springer Nature Switzerland.

[7] Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H. Security of zero trust networks in cloud computing: A comparative review. Sustainability. 2022 Sep 7;14(18):11213.

[8] Qazi FA. Study of zero trust architecture for applications and network security. In2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET) 2022 Dec 19 (pp. 111-116). IEEE.

[9] Fernandez EB, Brazhuk A. A critical analysis of Zero Trust Architecture (ZTA). Computer Standards & Interfaces. 2024 Apr 1;89:103832.

[10] Indran S, Alwi NH. Systematic Literature Review on Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA) Implementation to Ensure Secure Access. Journal of Advanced Research in Applied Sciences and Engineering Technology. 2024 Oct 8:182-95.

[11] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[12] Nahar N, Andersson K, Schelén O, Saguna S. A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks. IEEE Access. 2024 Jul 9.

[13] Dakić V, Morić Z, Kapulica A, Regvart D. Analysis of Azure Zero Trust Architecture implementation for mid-size organizations. Journal of cybersecurity and privacy. 2024 Dec 30;5(1):2.

[14] Batan A. Investigating the Efficacy of Zero-Trust Security Models in Mitigating Insider Threats in Enterprise Environments. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications. 2024 Dec 7;8(12):10-9.

[15] Ajish D. The significance of artificial intelligence in zero trust technologies: a comprehensive review. Journal of Electrical Systems and Information Technology. 2024 Aug 5;11(1):30.

[16] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[17] Daniel C. Building a More Secure Network: A Comprehensive Guide to Network Segmentation Strategies and Best Practices. Revista de Inteligencia Artificial en Medicina. 2024 Sep 9;15(1):959-68.

[18] Syed NF, Shah SW, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero trust architecture (zta): A comprehensive survey. IEEE access. 2022 May 12;10:57143-79.

[19] Azad MA, Abdullah S, Arshad J, Lallie H, Ahmed YH. Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. Internet of Things. 2024 Oct 1;27:101227.

[20] Chinamanagonda S. Zero Trust Security Models in Cloud Infrastructure-Adoption of zero-trust principles for enhanced security. Academia Nexus Journal. 2022 May 13;1(2).

[21] Chen B, Qiao S, Zhao J, Liu D, Shi X, Lyu M, Chen H, Lu H, Zhai Y. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. IEEE internet of things journal. 2020 Nov 30;8(13):10248-63.

[22] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[23] Alquwayzani AA, Albuali AA. A Systematic Literature Review of Zero Trust Architecture for Military UAV Security Systems. IEEE Access. 2024 Nov 20.

[24] AlMarshoud M, Sabir Kiraz M, H. Al-Bayatti A. Security, privacy, and decentralized trust management in VANETs: a review of current research and future directions. ACM Computing Surveys. 2024 Jun 22;56(10):1-39.

[25] Sharma H. Behavioral Analytics and Zero Trust. International Journal of Computer Engineering and Technology. 2021 Jun 25;12(1):63-84.

[26] Soltani S, Amanloo A, Shojafar M, Tafazolli R. Intelligent Control in 6G Open RAN: Security Risk or Opportunity?. IEEE Open Journal of the Communications Society. 2025 Jan 6.

[27] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[28] Ahmadi S. Zero trust architecture in cloud networks: application, challenges and future opportunities. Ahmadi, S.(2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports. 2024 Feb 13;26(2):215-28.

[29] A Al-Ofeishat H, Alshorman R. Build a secure network using segmentation and micro-segmentation techniques. International Journal of Computing and Digital Systems. 2023 Sep 20;16(1):1499-508.

[30] Roy A, Dhar A, Tinny SS. Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review. Journal of Computer Science and Information Technology. 2024 Sep 3;1(1):25-50.

[31] Kim Y, Sohn SG, Jeon HS, Lee SM, Lee Y, Kim J. Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. KSII Transactions on Internet and Information Systems (TIIS). 2024;18(9):2665-91.

[32] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[33] Ike CC, Ige AB, Oladosu SA, Adepoju PA, Amoo OO, Afolabi AI. Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. Magna Scientia Advanced Research and Reviews. 2021;2(1):074-86.

[34] Patel N. Secure access service edge (SASE): evaluating the impact of convereged network security architectures in cloud computing. Journal of Emerging Technologies and Innovative Research. 2024;11(3):12.

[35] Shen Q, Shen Y. Endpoint security reinforcement via integrated zero-trust systems: A collaborative approach. Computers & Security. 2024 Jan 1;136:103537.

[36] Stanco G, Navarro A, Frattini F, Ventre G, Botta A. A comprehensive survey on the security of low power wide area networks for the Internet of Things. ICT Express. 2024 Mar 18.

[37] Jawad M, Yassin AA, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Towards Building Multi-factor Authentication Scheme for Users in the Healthcare Sector Based on Blockchain Technology. InComputer Science On-line Conference 2024 Apr 25 (pp. 694-713). Cham: Springer Nature Switzerland.

[38] Lazarovitz L. Deconstructing the solarwinds breach. Computer Fraud & Security. 2021 Jun;2021(6):17-9.

[39] Taylor C. Improving your company's cyber security training. Network Security. 2023 Jun;2023(6).

[40] Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the internet of things. IEEE communications surveys & tutorials. 2018 Oct 11;21(2):1636-75.

[41] Mughal AA. The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection. International Journal of Intelligent Automation and Computing. 2018 Mar 11;1(1):1-20.

[42] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[43] Dissanayake N, Jayatilaka A, Zahedi M, Babar MA. Software security patch management-A systematic literature review of challenges, approaches, tools and practices. Information and Software Technology. 2022 Apr 1;144:106771.

[44] Makhdoom I, Abolhasan M, Franklin D, Lipman J, Zimmermann C, Piccardi M, Shariati N. Detecting compromised IoT devices: Existing techniques, challenges, and a way forward. Computers & Security. 2023 Sep 1;132:103384.

[45] Wang C, Wang Y, Chen Y, Liu H, Liu J. User authentication on mobile devices: Approaches, threats and trends. Computer Networks. 2020 Apr 7;170:107118.

[46] Mahmood RK, Mahameed AI, Lateef NQ, Jasim HM, Radhi AD, Ahmed SR, Tupe-Waghmare P. Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection. Journal of Robotics and Control (JRC). 2024 Aug 8;5(5):1502-24.

[47] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Aldarwish AJ, Neamah HA. Smart Grid and Renewable Energy Security Challenges: A Review. InComputer Science On-line Conference 2024 Apr 25 (pp. 805-825). Cham: Springer Nature Switzerland.

[48] Al-Tamimi S, Al-Haija QA, Alrawashdeh K. Zero-Trust Architecture for Securing Internet of Things (IoT) Networks: A Review. In2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES) 2024 Nov 20 (pp. 1-6). IEEE.

[49] Manoj T, Makkithaya K, VG N. A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records. Cogent Engineering. 2022 Jan 1;9(1).

[50] Indu I, Anand PR, Bhaskar V. Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal. 2018 Aug 1;21(4):574-88.

[51] Indu I, Anand PR, Bhaskar V. Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal. 2018 Aug 1;21(4):574-88.

[52] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[53] Muhammad T, Munir MT, Munir MZ, Zafar MW. Integrative cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. International Journal of Computer Science and Technology. 2022 Nov 30;6(4):99-135.

[54] Oladosu SA, Ike CC, Adepoju PA, Afolabi AI, Ige AB, Amoo OO. Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises integrations. Magna Scientia Advanced Research and Reviews. 2021.

[55] Swanzy PN, Abukari AM, Ansong ED. Data Security Framework for Protecting Data in Transit and Data at Rest in the Cloud. Current Journal of Applied Science and Technology. 2024 May 13;43(6):61-77.

[56] Ataullah M, Chauhan N. Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review. Security and Privacy. 2024 Nov;7(6):e448.

[57] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[58] Zohaib SM, Sajjad SM, Iqbal Z, Yousaf M, Haseeb M, Muhammad Z. Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work. Information. 2024 Nov 17;15(11):734.

[59] Annabi M, Zeroual A, Messai N. Towards zero trust security in connected vehicles: A comprehensive survey. Computers & Security. 2024 Jul 26:104018.

[60] Lekkala S, Gurijala P. Endpoint and Mobile Security Imperatives. InSecurity and Privacy for Modern Networks: Strategies and Insights for Safeguarding Digital Infrastructures 2024 Oct 8 (pp. 155-165). Berkeley, CA: Apress.

[61] Baligodugula VV, Ghimire A, Amsaad F. An Overview of Secure Network Segmentation in Connected IIoT Environments. Computing&AI Connect. 2024 Aug 28;1(1):1-0.

[62] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[63] Ganesh SS, Rajaram G, Anusuya V, Thirumalaikumari T, Navaz K, Sobia MC. Next-Generation Threat Detection and Mitigation in 6G Wireless Networks Using IAM, ZTNA and Advanced Security Mechanisms. Journal of Electrical Systems. 2024;20(5s):2034-41.

[64] Khan MZ, Nisa KU, Quasim MT, Khalifa MA, Mobarak MM. Cloud-based Data Protection: A Framework for Authorizing Data Movement. In2024 International Conference on Expert Clouds and Applications (ICOECA) 2024 Apr 18 (pp. 271-275). IEEE.

[65] Kokila M, Reddy S. Authentication, Access Control and Scalability models in Internet of Things Security-A Review. Cyber Security and Applications. 2024 Apr 14:100057.

[66] Alsayaydeh JA, Ali MF, Al-Andoli MN, Herawan SG. Improving the Robustness of IoT-Powered Smart City Applications Through Service-Reliant Application Authentication Technique. IEEE Access. 2024 Feb 1.

[67] Alshuraify NA, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Monitoring and surveillance systems based IoTs with Blockchain: Literature Review. Basrah Researches Sciences. 2024 Dec 31;50(2):42-63.

[68] Kamruzzaman A, Ismat S, Brickley JC, Liu A, Thakur K. A comprehensive review of endpoint security: Threats and defenses. In2022 International Conference on Cyber Warfare and Security (ICCWS) 2022 Dec 7 (pp. 1-7). IEEE.

[69] Acton T, Datta PM. Endpoint cybersecurity: When smart devices turn stupid. Journal of Information Technology Teaching Cases. 2024 Mar 27:20438869241242142.

[70] Kaur H, SL DS, Paul T, Thakur RK, Reddy KV, Mahato J, Naveen K. Evolution of endpoint Detection and Response (EDR) in cyber security: A comprehensive review. InE3S Web of Conferences 2024 (Vol. 556, p. 01006). EDP Sciences.

[71] Yusof ZB. Effectiveness of Endpoint Detection and Response Solutions in Combating Modern Cyber Threats. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures. 2024 Dec 4;8(12):1-9.

[72] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[73] Ahn G, Jang J, Choi S, Shin D. Research on Improving Cyber Resilience by Integrating the Zero Trust security model with the MITRE ATT&CK matrix. IEEE Access. 2024 Jun 21.

[74] Edwards DJ. Network Security. InMastering Cybersecurity: Strategies, Technologies, and Best Practices 2024 Jul 1 (pp. 103-138). Berkeley, CA: Apress.

[75] Mallick MA, Nath R. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News. 2024;190(1):1-69.

[76] Ravidas S, Lekidis A, Paci F, Zannone N. Access control in Internet-of-Things: A survey. Journal of Network and Computer Applications. 2019 Oct 15;144:79-101.

[77] Abdali HK, Hussain MA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. Comprehensive Challenges to E-government in Iraq. InComputer Science On-line Conference 2024 Apr 25 (pp. 639-657). Cham: Springer Nature Switzerland.

[78] Sania NS, Gigras Y, Mahajan S. Gatividhi Guard: The Activity Guardian—Revolutionizing Security Information and Event Management (SIEM) Technology. Journal of Operating Systems Development & Trends. 2024;11(1):29-44p.

[79] Sashwin K, Nithika KS, Priyadharshini S, Maduvant SP. Analysis, Trends, and Utilization of Security Information and Event Management (SIEM) in Critical Infrastructures. In2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS) 2024 Mar 14 (Vol. 1, pp. 1980-1984). IEEE.

[80] Veeramachaneni V. Integrating Zero Trust Principles into IAM for Enhanced Cloud Security. Recent Trends in Cloud Computing and Web Engineering. 2025;7(1):78-92.

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

[82] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[83] He Y, Huang D, Chen L, Ni Y, Ma X. A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing. 2022;2022(1):6476274.

[84] Edwards DJ. Data Protection. InCritical Security Controls for Effective Cyber Defense: A Comprehensive Guide to CIS 18 Controls 2024 Sep 29 (pp. 57-96). Berkeley, CA: Apress.

[85] Henriques J, Caldeira F, Cruz T, Simões P. A survey on forensics and compliance auditing for critical infrastructure protection. IEEE Access. 2024 Jan 1.

[86] Waqas M, Tu S, Halim Z, Rehman SU, Abbas G, Abbas ZH. The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. Artificial Intelligence Review. 2022 Oct;55(7):5215-61.

[87] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[88] Dhiman P, Saini N, Gulzar Y, Turaev S, Kaur A, Nisa KU, Hamid Y. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. Sensors. 2024 Feb 19;24(4):1328.

[89] Ali B, Hijjawi S, Campbell LH, Gregory MA, Li S. A maturity framework for zero-trust security in multiaccess edge computing. Security and Communication Networks. 2022;2022(1):3178760.

[90] Buck C, Olenberger C, Schweizer A, Völter F, Eymann T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security. 2021 Nov 1;110:102436.

[91] Lin J, Jiang Q, Zhang W, Lin Z, Du X. Quantum-Enhanced Zero Trust Security: Evolution, Implementation, and Application. In2024 International Conference on Quantum Communications, Networking, and Computing (QCNC) 2024 Jul 1 (pp. 211-215). IEEE.

[92] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[93] Ray PP. Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. Internet of Things and Cyber-Physical Systems. 2023 Jan 1;3:213-48.

[94] Obi OC, Akagha OV, Dawodu SO, Anyanwu AC, Onwusinkwue S, Ahmad IA. Comprehensive review on cybersecurity: modern threats and advanced defense strategies. Computer Science & IT Research Journal. 2024 Feb 2;5(2):293-310.

[95] Abdelkader S, Amissah J, Kinga S, Mugerwa G, Emmanuel E, Mansour DE, Bajaj M, Blazek V, Prokop L. Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks. Results in engineering. 2024 Jul 30:102647.

[96] Vidhyasagar BS, Arvindhan M, Arulprakash A, Kannan BB, Kalimuthu S. The Crucial Function that Clouds Access Security Brokers Play in Ensuring the Safety of Cloud Computing. In2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI) 2023 Nov 23 (pp. 98-102). IEEE.

[97] Abdali HK, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Implementing Blockchain for Enhancing Security and Authentication in Iraqi E-Government Services. Engineering, Technology & Applied Science Research. 2024 Dec 2;14(6):18222-33.

[98] Zandesh Z. Privacy, Security, and Legal Issues in the Health Cloud: Structured Review for Taxonomy Development. JMIR Formative Research. 2024 Feb 12;8:e38372.

[99] Mostafa AM, Ezz M, Elbashir MK, Alruily M, Hamouda E, Alsarhani M, Said W. Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. Applied Sciences. 2023 Sep 30;13(19):10871.

[100] Colomb Y, White P, Islam R, Alsadoon A. Applying Zero Trust Architecture and Probability-Based Authentication to Preserve Security and Privacy of Data in the Cloud. InEmerging Trends in Cybersecurity Applications 2022 Nov 19 (pp. 137-169). Cham: Springer International Publishing.

[101] Federici F, Martintoni D, Senni V. A zero-trust architecture for remote access in industrial IoT infrastructures. Electronics. 2023 Jan 22;12(3):566.

[102] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[103] Pureti N. Encryption 101: How to Safeguard Your Sensitive Information. International Journal of Advanced Engineering Technologies and Innovations. 2023 Nov 23;1(01):242-70.

[104] Tanque M, Foxwell HJ. Cyber risks on IoT platforms and zero trust solutions. InAdvances in Computers 2023 Jan 1 (Vol. 131, pp. 79-148). Elsevier.

[105] Nagamalla V, Sanapala RK. Integrating Predictive Big Data Analytics with Behavioral Machine Learning Models for Proactive Threat Intelligence in Industrial IoT Cybersecurity. International Journal of Wireless & Ad Hoc Communication. 2023 Oct 1;7(2).

[106] Aminu M, Akinsanya A, Dako DA, Oyedokun O. Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. International Journal of Computer Applications Technology and Research. 2024;13(8):11-27.

[107] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[108] Vemula VR, Yarraguntla T. Mitigating Insider Threats through Behavioural Analytics and Cybersecurity Policies. International Meridian Journal. 2021 Apr 30;3(3):1-20.

[109] Alzaabi FR, Mehmood A. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access. 2024 Feb 26;12:30907-27.

[110] Bashir T. Zero Trust Architecture: Enhancing cybersecurity in enterprise networks. Journal of Computer Science and Technology Studies. 2024 Sep 23;6(4):54-9.

[111] Anjum I, Kostecki D, Leba E, Sokal J, Bharambe R, Enck W, Nita-Rotaru C, Reaves B. Removing the reliance on perimeters for security using network views. InProceedings of the 27th ACM on Symposium on Access Control Models and Technologies 2022 Jun 7 (pp. 151-162).

[112] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[113] Gupta A, Gupta P, Pandey UP, Kushwaha P, Lohani BP, Bhati K. ZTSA: Zero Trust Security Architecture a Comprehensive Survey. In2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE) 2024 May 9 (pp. 378-383). IEEE.

[114] Tsai M, Lee S, Shieh SW. Strategy for implementing of zero trust architecture. IEEE Transactions on Reliability. 2024 Jan 5.

[115] Liu L, De Vel O, Han QL, Zhang J, Xiang Y. Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys & Tutorials. 2018 Feb 1;20(2):1397-417.

[116] Chimakurthi VN. The challenge of achieving zero trust remote access in multi-cloud environment. ABC Journal of Advanced Research. 2020 Dec 31;9(2):89-102.

[117] Al-Maliki H, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Reliable Vehicular Ad Hoc Networks for Intelligent Transportation Systems based on the Snake Optimization Algorithm. Engineering, Technology & Applied Science Research. 2024 Dec 2;14(6):18631-9.

[118] Ferretti L, Magnanini F, Andreolini M, Colajanni M. Survivable zero trust for cloud computing environments. Computers & Security. 2021 Nov 1;110:102419.

[119] Stefanidou M, Maraslidis GS, Antoniadis I, Fragulis GF. Cloud-driven network security: A survey of methods, challenges, and innovations. InAIP Conference Proceedings 2024 Oct 8 (Vol. 3220, No. 1). AIP Publishing.

[120] Alevizos L, Ta VT, Hashem Eiza M. Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. Security and privacy. 2022 Jan;5(1):e191.

[121] Itodo C, Ozer M. Multivocal Literature Review on Zero-Trust Security Implementation. Computers & Security. 2024 Mar 29:103827.

[122] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[123] Sargiotis D. Legal and Regulatory Considerations in Data Governance. InData Governance: A Guide 2024 Sep 12 (pp. 445-466). Cham: Springer Nature Switzerland.

[124] Herath HM, Herath HM, Madhusanka BG, Guruge LG. Data Protection Challenges in the Processing of Sensitive Data. InData Protection: The Wake of AI and Machine Learning 2024 Dec 24 (pp. 155-179). Cham: Springer Nature Switzerland.

[125] Amirah S. Policy-Based Encryption Models and Their Role in Enforcing Granular Data Security for E-Marketplace Customers. Perspectives on Next-Generation Cloud Computing Infrastructure and Design Frameworks. 2022 Feb 4;6(10):1-9.

[126] Murthy JS, Kar R. Collaborative Cloud: Safeguarding Sensitive Information through Innovative Secure Data-Sharing Practices. InCloud Security 2024 Aug 28 (pp. 1-16). Chapman and Hall/CRC.

[127] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[128] Simpson WR, Foltz KE. Resolving network defense conflicts with zero trust architectures and other end-to-end paradigms. International Journal of Network Security & Its Applications (IJNSA) Vol. 2021;13.

[129] Coronado E, Behravesh R, Subramanya T, Fernàndez-Fernàndez A, Siddiqui MS, Costa-Pérez X, Riggio R. Zero touch management: A survey of network automation solutions for 5G and 6G networks. IEEE Communications Surveys & Tutorials. 2022 Oct 6;24(4):2535-78.

[130] Aburbeian AM, Fernández-Veiga M. Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. AI. 2024 Jan 10;5(1):177-94.

[131] Yoon HJ, Zolkipli MF. Conceptual Model for Remote Access Security Using Zero-Trust Network Access (ZTNA). Borneo International Journal eISSN 2636-9826. 2024 Nov 28;7(4):28-34.

[132] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[133] Joshi H. Emerging Technologies Driving Zero Trust Maturity Across Industries. IEEE Open Journal of the Computer Society. 2024 Nov 22.

[134] Zanasi C, Russo S, Colajanni M. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc Networks. 2024 Apr 1;156:103414.

[135] Fitria N. Comparing Software-Defined Perimeter and Zero-Trust Architectures for Secure, Cloud-Native Online Retail Infrastructures. International Journal of Applied Business Intelligence. 2021 Dec 7;1(12):12-22.

[136] Ali A, Laghari AA, Kandhro IA, Kumar K, Younus S. Systematic analysis of on-premise and cloud services. International Journal of Cloud Computing. 2024;13(3):214-42.

[137] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[138] Trnka M, Cerny T, Stickney N. Survey of Authentication and Authorization for the Internet of Things. Security and Communication Networks. 2018;2018(1):4351603.

[139] Abdullah N, Hakansson A, Moradian E. Blockchain based approach to enhance big data authentication in distributed environment. In2017 Ninth international conference on ubiquitous and future networks (ICUFN) 2017 Jul 4 (pp. 887-892). IEEE.

[140] Kamaruddin NH, Zolkipli MF. The Role of Multi-Factor Authentication in Mitigating Cyber Threats. Borneo International Journal eISSN 2636-9826. 2024 Dec 16;7(4):35-42.

[141] Khadka M. A Systematic Appraisal of Multi-Factor Authentication Mechanisms for Cloud-Based E-Commerce Platforms and Their Effect on Data Protection. Journal of Emerging Cloud Technologies and Cross-Platform Integration Paradigms. 2022 Dec 7;6(12):12-21.

[142] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[143] Chitra M, Surianarayanan R, Mahamuni VS, Mohammed S, Keno MT, Boopathi S. Study on Cloud Computing-Empowered Small and Medium Enterprises. InEssential Information Systems Service Management 2025 (pp. 189-220). IGI Global.

[144] Konar S, Mukherjee G, Dutta G. Understanding the Relationship Between Trust and Faith in Micro-Enterprises to Cyber Hygiene: An Empirical Review. Strengthening Industrial Cybersecurity to Protect Business Intelligence. 2024:125-48.

[145] Gupta A, Gupta R, Jadav D, Tanwar S, Kumar N, Shabaz M. Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications. Computer Communications. 2023 Jun 1;206:10-21.

[146] Pavana B, Prasad SK. Zero trust model: A compelling strategy to strengthen the security posture of IT organizations. InAIP Conference Proceedings 2022 Oct 3 (Vol. 2519, No. 1). AIP Publishing.

[147] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[148] Lund BD, Lee TH, Wang Z, Wang T, Mannuru NR. Zero Trust Cybersecurity: Procedures and Considerations in Context. Encyclopedia. 2024 Oct 11;4(4):1520-33.

[149] Alawneh M, Abbadi IM. Integrating trusted computing mechanisms with trust models to achieve zero trust principles. In2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) 2022 Nov 29 (pp. 1-6). IEEE.

[150] Thomas PA, Preetha Mathew K. A broad review on non-intrusive active user authentication in biometrics. Journal of Ambient Intelligence and Humanized Computing. 2023 Jan;14(1):339-60.

[151] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Secure and Fast Remote Application–Based Authentication Dragonfly Using an LED Algorithm in Smart Buildings. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 509-517). IEEE.

[152] Vignesh R, Mohana Prasad K. Blockchain assisted AHMFA authentication in employee performance assessment system. Multimedia Tools and Applications. 2024 Jan;83(2):5131-64.

[153] Gudala L, Shaik M, Venkataramanan S. Leveraging Machine Learning for Enhanced Threat Detection and Response in Zero Trust Security Frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies. Journal of Artificial Intelligence Research. 2021 Nov 26;1(2):19-45.

[154] Nookala G. Adaptive Data Governance Frameworks for Data-Driven Digital Transformations. Journal of Computational Innovation. 2024 Feb 13;4(1).

[155] Gupta R, Tanwar S, Tyagi S, Kumar N. Machine learning models for secure data analytics: A taxonomy and threat model. Computer Communications. 2020 Mar 1;153:406-40.

[156] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[157] Deshpande A. A study on rapid adoption of zero trust network architectures by global organizations due to COVID-19 pandemic. New Visions in Science and Technology. 2021 Aug 11;1:26-33.

[158] Ansarullah SI, Kirmani MM, Mushtaq Z, ud din Dar GM. Cyber Security: Future Trends and Solutions. InCyber Security for Next-Generation Computing Technologies 2024 (pp. 1-15). CRC Press.

[159] Putri A. Multi-Cloud Strategies for Managing Big Data Workflows and AI Applications in Decentralized Government Systems. Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks. 2025 Jan 4;9(1):1-1.

[160] Syrotynskyi R, Tyshyk I, Kochan O, Sokolov V, Skladannyi P. Methodology of network infrastructure analysis as part of migration to zero-trust architecture. Cyber Security and Data Protection 2024. 2024(3800):97-105.

[161] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11; 2(3): 399-406.

[162] Dash B. Zero-Trust Architecture (ZTA): Designing an AI-Powered Cloud Security Framework for LLMs' Black Box Problems. Available at SSRN 4726625. 2024 Feb 10.

[163] Liang Y, Samtani S, Guo B, Yu Z. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. IEEE Internet of Things Journal. 2020 Jun 22;7(9):9128-43.

[164] Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials. 2020 Jan 6;22(2):1191-221.

[165] Douglass R. Use and Abuse of IoT: Challenges and Recommendations. IoT for Defense and National Security. 2022 Dec 28:397-465.

[166] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[167] Huh JH, Kwag S, Kim I, Popov A, Park Y, Cho G, Lee J, Kim H, Lee CH. On the long-term effects of continuous keystroke authentication: Keeping user frustration low through behavior adaptation. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 2023 Jun 12;7(2):1-32.

[168] Gill SS, Kumar A, Singh H, Singh M, Kaur K, Usman M, Buyya R. Quantum computing: A taxonomy, systematic review and future directions. Software: Practice and Experience. 2022 Jan;52(1):66-114.

[169] Prince NU, Faheem MA, Khan OU, Hossain K, Alkhayyat A, Hamdache A, Elmouki I. AI-Powered Data-Driven Cybersecurity Techniques: Boosting Threat Identification and Reaction. Nanotechnology Perceptions. 2024;20:332-53.

[170] Alsadie D. Artificial Intelligence Techniques for Securing Fog Computing Environments: Trends, Challenges, and Future Directions. IEEE Access. 2024 Sep 19.

[171] Alshuraify NA, Yassin AA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. Blockchain-Based CCTV Surveillance Cameras for Oil and Gas Industry Pipelines. InComputer Science On-line Conference 2024 Apr 25 (pp. 730-744). Cham: Springer Nature Switzerland.

[172] Punia A, Gulia P, Gill NS, Ibeke E, Iwendi C, Shukla PK. A systematic review on blockchain-based access control systems in cloud environment. Journal of Cloud Computing. 2024 Sep 30;13(1):146.

[173] Ofoegbu KD, Osundare OS, Ike CS, Fakeyede OG, Ige AB. Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. Journal name if available. 2024.

[174] Rodriguez Müller AP, Martin Bosch J, Tangi L. Interoperability for Emerging Technologies: A Systematic Scoping Review. InInternational Conference on Electronic Government 2024 (pp. 387-401). Springer, Cham.

[175] Tsampoulatidis I, Komninos N, Syrmos E, Bechtsis D. Universality and interoperability across smart city ecosystems. InInternational Conference on Human-Computer Interaction 2022 Jun 16 (pp. 218-230). Cham: Springer International Publishing.

[176] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[177] Sahinbas K, Catak FO. Secure multi-party computation-based privacy-preserving data analysis in healthcare IoT systems. InInterpretable Cognitive Internet of Things for Healthcare 2023 Jun 27 (pp. 57-72). Cham: Springer International Publishing.

[178] Gowda SD. Secure Multiparty Computation: Protocols, Collaborative Data Processing, and Real-World Applications in Industry. InCloud Security 2024 Aug 28 (pp. 160-182). Chapman and Hall/CRC.

[179] Jiang R, Long C, Yang M, Liang Z. Application of Multi-Party Computation in Data Security and Privacy Protection under the Context of Blockchain. In2024 Second International Conference on Inventive Computing and Informatics (ICICI) 2024 Jun 11 (pp. 683-688). IEEE.

[180] Zhou I, Tofigh F, Piccardi M, Abolhasan M, Franklin D, Lipman J. Secure Multi-Party Computation for Machine Learning: A Survey. IEEE Access. 2024 Apr 15.

[181] Alzaidi ZS, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2247-2252). IEEE.

[182] Kayes AS, Kalaria R, Sarker IH, Islam MS, Watters PA, Ng A, Hammoudeh M, Badsha S, Kumara I. A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. Sensors. 2020 Apr 27;20(9):2464.

[183] Pooja S, Chandrakala CB. Secure Reviewing & Data Sharing in Scientific Collaboration: Leveraging Blockchain and Zero Trust Architecture. IEEE Access. 2024 Jul 4.

[184] Hazra A, Adhikari M, Amgoth T, Srirama SN. A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. ACM Computing Surveys (CSUR). 2021 Nov 23;55(1):1-35.

[185] Hanif M, Munir EU, Rehan MM, Ahmad SG, Iqbal T, Kirn N, Ayyub K, Ramzan N. Adaptive Secure Multi-modal Telehealth Patient-Monitoring System. Multimodal Intelligent Sensing in Modern Applications. 2024 Dec 13:201-25.

[186] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[187] Ramezanpour K, Jagannath J. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. Computer Networks. 2022 Nov 9;217:109358.

[188] Chokkanathan K, Karpagavalli SM, Priyanka G, Vanitha K, Anitha K, Shenbagavalli P. AI-Driven Zero Trust Architecture: Enhancing Cyber-Security Resilience. In2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS) 2024 Nov 7 (pp. 1-6). IEEE.

[189] Maddireddy BR, Maddireddy BR. Real-Time Data Analytics with AI: Improving Security Event Monitoring and Management. Unique Endeavor in Business & Social Sciences. 2022 Jun 30;1(2):47-62.

[190] Nassar A, Kamal M. Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. Journal of Artificial Intelligence and Machine Learning in Management. 2021 Feb 6;5(1):51-63.

[191] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[192] Camacho NG. Unlocking the Potential of AI/ML in DevSecOps: Effective Strategies and Optimal Practices. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023. 2024 Mar 6;3(1):106-15.

[193] Baseri Y, Chouhan V, Hafid A. Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. Computers & Security. 2024 May 1:103883.

[194] Zornetta A. Quantum-safe global encryption policy. International Journal of Law and Information Technology. 2024;32(1):eaae020.

[195] Zhang Z, Zhao Y. Enhanced Elliptic Curve Cryptography (EECC). Procedia Computer Science. 2024 Jan 1;247:1324-30.

[196] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[197] Chahar S. Exploring the future trends of cryptography. InNext Generation Mechanisms for Data Encryption 2025 Jan 24 (pp. 234-257). CRC Press.

[198] Khan MA, Javaid S, Mohsan SA, Tanveer M, Ullah I. Future-Proofing Security for UAVs With Post-Quantum Cryptography: A Review. IEEE Open Journal of the Communications Society. 2024 Oct 28.

[199] Ali B, Gregory MA, Li S. Multi-access edge computing architecture, data security and privacy: A review. IEEE Access. 2021 Jan 21;9:18706-21.

[200] Samaila MG, Neto M, Fernandes DA, Freire MM, Inácio PR. Challenges of securing Internet of Things devices: A survey. Security and Privacy. 2018 Mar;1(2):e20.

[201] Xu X, Patibandla RL, Arora A, Al-Razgan M, Awwad EM, Nyangaresi VO. An Adaptive Hybrid (1D-2D) Convolution-based ShuffleNetV2 Mechanism for Irrigation Levels Prediction in Agricultural Fields with Smart IoTs. IEEE Access. 2024 Apr 3.

[202] Ragothaman K, Wang Y, Rimal B, Lawrence M. Access control for IoT: A survey of existing research, dynamic policies and future directions. Sensors. 2023 Feb 6;23(4):1805.

[203] Tahir M, Sardaraz M, Muhammad S, Saud Khan M. A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. Sustainability. 2020 Aug 26;12(17):6960.

[204] Bagga P, Das AK, Wazid M, Rodrigues JJ, Park Y. Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. Ieee Access. 2020 Mar 17;8:54314-44.

[205] Munir A, Sumra IA, Naveed R, Javed MA. Techniques for Authentication and Defense Strategies to Mitigate IoT Security Risks. Journal of Computing & Biomedical Informatics. 2024 Jun 1;7(01).

[206] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[207] Domingo-Ferrer J, Blanco-Justicia A. Privacy-preserving technologies. The Ethics of Cybersecurity. 2020:279-97.

[208] Farayola OA, Olorunfemi OL, Shoetan PO. Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal. 2024 Mar 27;5(3):606-15.

[209] Hossam AT. Enhancing Privacy in Big Data Analytics Through Encrypted Computational Techniques and Secure Multi-Party Computation Strategies. Journal of Industrial IoT Technologies. 2024 Feb 13;14(2):1-8.

[210] Nookala G. Secure Multiparty Computation (SMC) for Privacy-Preserving Data Analysis. Journal of Big Data and Smart Systems. 2023 Mar 9;4(1).

[211] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[212] Staab R, Jovanović N, Balunović M, Vechev M. From principle to practice: Vertical data minimization for machine learning. In2024 IEEE Symposium on Security and Privacy (SP) 2024 May 19 (pp. 4733-4752). IEEE.

[213] El Rajab M, Yang L, Shami A. Zero-touch networks: Towards next-generation network automation. Computer Networks. 2024 Apr 1;243:110294.

[214] Nookala G. Automation of Privileged Access Control as Part of Enterprise Control Procedure. Journal of Big Data and Smart Systems. 2020 Mar 25;1(1).

[215] Ashfaq F, Ahad A, Hussain M, Shayea I, Pires IM. Enhancing Zero Trust Security in Edge Computing Environments: Challenges and Solutions. InWorld Conference on Information Systems and Technologies 2024 Mar 26 (pp. 433-444). Cham: Springer Nature Switzerland.

[216] Nyangaresi VO, Yenurkar GK. Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks. High-Confidence Computing. 2023 Nov 24:100178.

[217] Xiao S, Ye Y, Kanwal N, Newe T, Lee B. SoK: context and risk aware access control for zero trust systems. Security and Communication Networks. 2022;2022(1):7026779.

[218] Bellavista P, Montanari R. Context awareness for adaptive access control management in IoT environments. Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications. 2017 Nov 13:157-78.

[219] Kalaria R, Kayes AS, Rahayu W, Pardede E, Salehi Shahraki A. Adaptive context-aware access control for IoT environments leveraging fog computing. International Journal of Information Security. 2024 Aug;23(4):3089-107.

[220] Shandilya SK, Datta A, Kartik Y, Nagar A. Advancing Security and Resilience. InDigital Resilience: Navigating Disruption and Safeguarding Data Privacy 2024 Jan 2 (pp. 459-529). Cham: Springer Nature Switzerland.

[221] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[222] Kandanaarachchi TB, Nelson JD, Ho CQ. Conceptualising trust and collaboration among stakeholders in MaaS ecosystems. Transport Policy. 2024 Oct 1;157:98-110.

[223] Gunawardena RS. Dynamic Access Control Techniques and Their Role in Preserving Data Confidentiality in Multi-Cloud Retail Solutions. Journal of Computational Intelligence for Hybrid Cloud and Edge Computing Networks. 2022 Dec 7;6(12):12-22.

[224] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security. 2018 Jan 1;72:212-33.

[225] Mavroeidis V, Bromander S. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In2017 European Intelligence and Security Informatics Conference (EISIC) 2017 Sep 11 (pp. 91-98). IEEE.

[226] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[227] Tahmasebi M. Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises. Journal of Information Security. 2024 Feb 27;15(2):106-33.

[228] Sharma A, Gupta BB, Singh AK, Saraswat VK. Advanced persistent threats (apt): evolution, anatomy, attribution and countermeasures. Journal of Ambient Intelligence and Humanized Computing. 2023 Jul;14(7):9355-81.

[229] Nicho M, McDermott CD. Dimensions of 'socio'vulnerabilities of advanced persistent threats. In2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) 2019 Sep 19 (pp. 1-5). IEEE.

[230] Saurabh K, Sharma V, Singh U, Khondoker R, Vyas R, Vyas OP. HMS-IDS: Threat intelligence integration for zero-day exploits and advanced persistent threats in IIoT. Arabian Journal for Science and Engineering. 2024 Jul 10:1-21.

[231] Zengeni IP, fadli Zolkipli M. Zero-Day Exploits and Vulnerability Management. Borneo International Journal eISSN 2636-9826. 2024 Sep 1;7(3):26-33.

[232] Yusof ZB. Exploration of Advanced Persistent Threats: Techniques, Mitigation Strategies, and Impacts on Critical Infrastructure. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications. 2024 Dec 4;8(12):1-9.

[233] Karim SS, Afzal M, Iqbal W, Al Abri D. Advanced Persistent Threat (APT) and intrusion detection evaluation dataset for linux systems 2024. Data in Brief. 2024 Jun 1;54:110290.