Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition

A Review of Authentication and Authorization Mechanisms in Zero Trust Architecture: Evolution and Efficiency

Research Article https://techspherejournal.com

DOI: https://doi.org/10.5281/zenodo.15149866

1. ORCID: https://orcid.org/0000-0002-1582-1739

Author(s) Details

Onwuegbuzie Innocent Uzougbo[1*], Alabi Oyegbola Augustine[2]

1, Cybersecurity Department, Dennis Osadebay University, Asaba, Delta State Nigeria

2, Computer Science Department, The Federal Polytechnic Ado-Ekiti, Ekiti State, Nigeria

*Corresponding author's email: onwuegbuzie.innocent@dou.edu.ng

ABSTRACT

Zero Trust Architecture (ZTA) is a transformative cybersecurity paradigm that mitigates the bottlenecks of the traditional perimeter-based models, operating on the principle of "never trust, always verify." It ensures stringent authentication and authorization to secure modern, complex networks against escalating threats. This paper reviews the evolution and efficiency of authentication and authorization mechanisms within ZTA, tracing their development from static, rule-based systems to dynamic, AI-driven solutions. Early methods like passwords have evolved into advanced techniques, including multi-factor authentication (MFA), passwordless systems, biometrics, and attribute-based access control (ABAC), reflecting ZTA's adaptability to distributed environments such as IoT and cloud computing. The study evaluates these mechanisms' efficiency through metrics like security, usability, scalability, and cost, supported by case studies and comparisons with traditional models. Findings reveal significant strengths, such as comprehensive frameworks and innovative approaches leveraging AI and blockchain, alongside limitations like insufficient empirical validation and scalability challenges. Future directions propose integrating emerging technologies quantum-resistant cryptography, decentralized identity solutions, and AI-driven verification while emphasizing industry-specific frameworks and real-world testing to enhance ZTA's practical adoption. By addressing these gaps, this review contributes to a deeper understanding of ZTA, offering practitioners insights into best practices for securing modern networks. As cyber threats evolve, ZTA's continuous improvement remains critical, balancing robust security with usability to safeguard sensitive data and critical infrastructure effectively.

Keywords: Zero Trust Architecture (ZTA), Authentication and Authorization, Continuous Verification, Cybersecurity Innovation, Adaptive Access Control.

1 Introduction

The rapid advancement of technology has transformed how businesses operate, enabling seamless communication, collaboration, and innovation. However, this progress has also introduced unprecedented cybersecurity risks. Modern networks are characterized by their distributed nature, with users accessing resources from multiple devices, locations, and platforms. Cloud computing, IoT devices, remote work setups, and third-party integrations have expanded the attack surface, making it easier for malicious actors to exploit vulnerabilities. According to recent statistics, cybercrime is projected to cost the global economy over $10 trillion annually by 2025 (Kuzior et al., 2024a, 2024b), underscoring the urgency of addressing these threats effectively.

One of the primary challenges facing modern networks is the sophistication of cyberattacks. Attackers employ advanced techniques such as phishing, ransomware, social engineering, and supply chain attacks to breach systems and steal valuable information (Aslan et al., 2023; Reshmi, 2021). These methods often bypass traditional security measures,

leaving organizations vulnerable to data breaches, financial losses, reputational damage, and regulatory penalties. Furthermore, the growing reliance on interconnected systems means that a single compromised device or account can lead to widespread disruption throughout the network.

1.1 Traditional Perimeter-Based Security Models (PBSM) and Their Limitations

For decades, organizations relied on perimeter-based security models (PBSM) to safeguard their assets. This approach involved creating a virtual "moat" around the network using firewalls, intrusion detection systems, and other perimeter defences (Dumitru, 2022; Nadji, 2024). Inside the perimeter, users were implicitly trusted, while external entities were considered potential threats. While effective in simpler times, this model fails to meet the demands of contemporary IT environments. The limitations of perimeter-based security are manifold. First, it assumes that all internal users and devices are trustworthy, which overlooks insider threats, whether intentional or accidental that can compromise system integrity (Utsash, 2024). Second, the rise of remote work and cloud services has blurred the boundaries between internal and external networks, rendering traditional perimeters obsolete (Kang et al., 2023; Roy et al., 2024). Third, once attackers penetrate the perimeter, they gain unrestricted access to internal resources, allowing them to move laterally undetected until significant damage is done (Azad et al., 2024; Steingartner et al., 2021). Finally, maintaining and updating perimeter defences is resource-intensive, requiring constant vigilance against evolving threat vectors.
These shortcomings highlight the need for a more robust and adaptive security paradigm, one that does not rely solely on static barriers but instead enforces strict controls at every level of the network.

1.1.1 Zero Trust Architecture – ZTA - ("Never Trust, Always Verify")

Zero Trust Architecture represents a fundamental shift in cybersecurity philosophy. Unlike traditional models, ZTA operates under the principle of "never trust, always verify," meaning that no user, device, or application is inherently trusted, regardless of location or affiliation. Instead, access to resources is granted based on continuous verification through stringent authentication and authorization processes (Phiayura & Teerakanok, 2023; Syed et al., 2022).
At its core, ZTA adheres to three foundational principles:

1. **Continuous Verification:** Every request for access must be authenticated and authorized in real-time, even if the user has previously been verified. This ensures that permissions remain valid only when necessary (Phiayura & Teerakanok, 2023).
2. **Least Privilege Access:** Users and devices are granted the minimum level of access required to perform their tasks, reducing the risk of unauthorized activity (Dakić et al., 2024; Nahar et al., 2024).
3. **Micro-Segmentation:** Networks are divided into smaller, isolated segments, each with its own set of access policies. This limits lateral movement by attackers who manage to breach one segment (Li et al., 2024).

By eliminating implicit trust and enforcing granular control over resource access, ZTA significantly enhances security posture while supporting flexible, scalable operations. Figure 1 shows how ZTA works.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

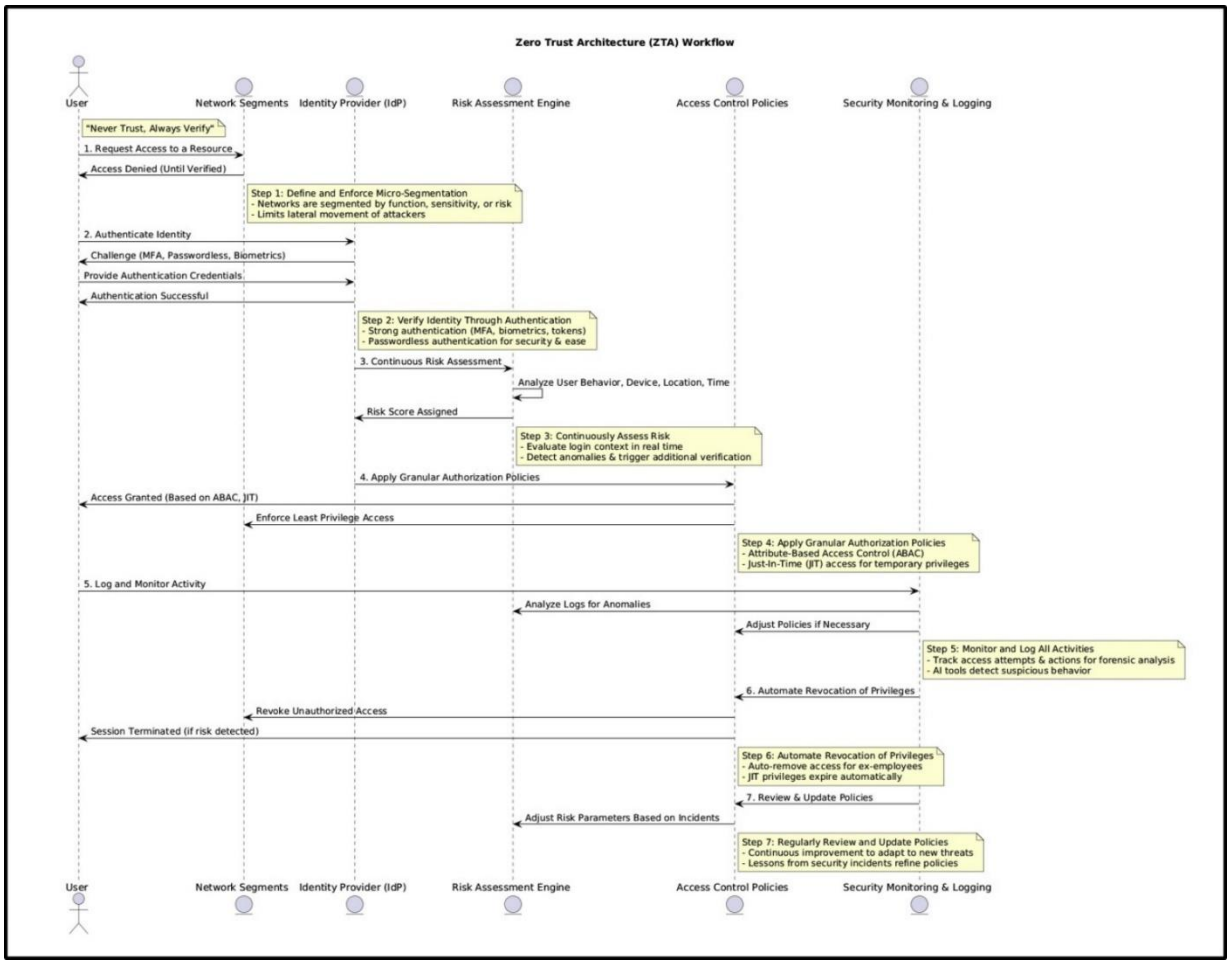

Figure 1: How Zero Trust Architecture (ZTA) Works

1.1.2 Importance of Authentication and Authorization in ZTA

Authentication and authorization form the backbone of ZTA, ensuring that only legitimate users and devices gain access to protected resources. Authentication involves verifying the identity of a user or device through credentials such as passwords, biometrics, or tokens. In ZTA, multi-factor authentication (MFA) is often employed to strengthen identity verification by combining multiple factors (Ajish, 2024; Ojo, 2025).

Authorization, on the other hand, determines what actions a verified entity is allowed to perform. In ZTA, authorization is typically context-aware, taking into account additional attributes such as user behaviour, device health, geographic location, and time of access (Ajish, 2024). Advanced mechanisms like attribute-based access control (ABAC) and just-in-time (JIT) access further enhance security by dynamically adjusting permissions based on current conditions.

Together, authentication and authorization enable ZTA to enforce strict access controls without compromising usability. They ensure that sensitive data remains protected while facilitating seamless interactions between users, applications, and services.

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

1.2 Objectives of the Paper

This paper aims to provide a thorough review of authentication and authorization mechanisms within the context of Zero Trust Architecture, with the following objectives: (1) to review the evolution of these mechanisms, analysing their transition from static, rule-based systems to dynamic, AI-driven solutions; (2) to analyse their efficiency and effectiveness by evaluating performance metrics such as security, usability, scalability, and cost, supported by case studies and comparative analyses; and (3) to identify gaps in current practices, propose future directions, and explore emerging technologies and trends that could shape the future of authentication and authorization in ZTA, ultimately contributing to the broader understanding of Zero Trust Architecture and informing practitioners about best practices for securing modern networks.

The remainder of this paper is organized as follows:
Section 2: Research Methodology – A systematic literature selection process was employed using reputable databases, structured search strategies, strict inclusion/exclusion criteria, multi-stage screening, and data extraction.
Section 3: Literature Review – Provides a comprehensive overview of existing research on authentication and authorization mechanisms in ZTA. It highlights key developments, common themes, and open questions in the field.
Section 4: Core Concepts in Zero Trust Architecture – Explains the fundamental principles of ZTA and their implications for authentication and authorization. It discusses micro-segmentation, least privilege access, and continuous verification in detail.
Section 5: Authorization Mechanisms in Zero Trust – Focuses on dynamic authorization strategies, including ABAC, policy-based access control, and AI-driven adaptive policies. It addresses the importance of context-awareness and automation in ZTA.
Section 6: Authorization Mechanisms in Zero Trust – Assesses the effectiveness of ZTA mechanisms using relevant metrics. Real-world case studies and comparisons with traditional models are included to provide practical insights.
Section 7: Analytical Review of the Literature and Findings – Explores emerging trends and innovations in authentication and authorization, such as quantum-resistant cryptography and decentralized identity solutions. It emphasizes the importance of standardization and collaboration in advancing ZTA.
Section 8: Statistical Analysis of the Literature – Discussed the statistical insights from the literature
Section 9: Future Direction– Future directions include exploring quantum-resistant cryptography, decentralized identities, AI-driven verification, and global standards to enhance ZTA's scalability, interoperability, and effectiveness in evolving cybersecurity landscapes.
Section 10: Conclusion – Summarizes the key findings of the paper and reiterates the significance of ZTA in enhancing cybersecurity. It concludes with thoughts on the future of authentication and authorization in the digital age

2 Research Methodology

The process of selecting literature for this study was conducted systematically to ensure comprehensive coverage and relevance. Below is a concise breakdown of the approach:

1. **Identification of Databases**
   Reputable databases were consulted to gather relevant literature, including Scopus, Google Scholar, Web of Science, IEEE Xplore, ACM Digital Library, SpringerLink, and Elsevier. These sources provided peer-reviewed articles, conference proceedings, and interdisciplinary works.

2. **Search Strategy**
   A structured search strategy was employed using specific keywords and Boolean operators. Primary keywords included "Zero Trust Architecture (ZTA)," "Authentication," "Authorization," and "Cybersecurity," while secondary keywords covered "Micro-segmentation," "Behavioural Biometrics," and "Continuous Verification." Boolean operators (AND, OR) were used to refine results.
3. **Inclusion and Exclusion Criteria**
   Inclusion criteria focused on publications from 2017 onwards, peer-reviewed articles, and studies addressing specific aspects of ZTA. Exclusion criteria removed outdated studies (pre-2017), non-peer-reviewed sources, and irrelevant topics.
4. **Screening Process**
   The screening process involved three stages:
   a) **Title Screening**: Initial filtering to eliminate irrelevant studies.
   b) **Abstract Screening**: Detailed review to assess relevance and alignment with the study scope.
   c) **Full-Text Review**: Comprehensive evaluation to extract key findings, strengths, limitations, and future directions.

5. **Data Extraction**
   From the final set of selected papers, data such as authors, publication year, title, aspect of ZTA, strengths, limitations, and future directions were extracted.

This systematic approach ensured transparency, reproducibility, and relevance in the selection of literature for the study.

3 Literature Review

The literature on Zero Trust Architecture (ZTA) has grown exponentially in recent years, reflecting the increasing importance of this paradigm in modern cybersecurity. This section provides a comprehensive review of existing research on authentication and authorization mechanisms within ZTA, focusing on key developments, common themes, and open questions in the field. We analyse studies published between 2020 and 2025 to ensure relevance and currency. The review highlights advancements in both theoretical foundations and practical implementations, offering insights into how these mechanisms have evolved and where further research is needed.

3.1 Historical Context of Authentication and Authorization

Authentication and authorization are foundational elements of cybersecurity that predate the emergence of Zero Trust Architecture. Early systems relied heavily on static credentials, such as passwords, to verify identities and enforce access controls. However, as networks became more complex and threats more sophisticated, traditional methods proved insufficient. Over time, researchers and practitioners developed dynamic and adaptive approaches to address these limitations.

3.1.1 Evolution of Authentication Mechanisms

Research from the early 2010s emphasized the inadequacy of single-factor authentication (SFA) and advocated for multi-factor authentication (MFA) as a stronger alternative (Dakić et al., 2024; Nahar et al., 2024). MFA combines two or more factors, something you know (password), something you have (token), and something you are (biometric) , to enhance security. By 2020, MFA had become widely adopted, but its implementation was often inconsistent and user-unfriendly (Dakić et al., 2024).

In response to usability concerns, passwordless authentication gained traction during this period. Studies by (Dakić et al., 2024; Gunuganti, 2023) demonstrated the potential of biometric-based systems, such as fingerprint scanning and

facial recognition, to reduce friction while maintaining high security levels. Similarly, behavioural biometrics, which analyse patterns like typing speed and mouse movement, emerged as promising alternatives for continuous authentication (Shah et al., 2021)

3.1.2 Evolution of Authorization Mechanisms

Authorization mechanisms also underwent significant transformation. Role-Based Access Control (RBAC) dominated the landscape for decades due to its simplicity and effectiveness in managing permissions based on predefined roles (Shah et al., 2021). However, RBAC struggled with scalability and flexibility in dynamic environments. Attribute-Based Access Control (ABAC), introduced in the mid-2010s, addressed these shortcomings by allowing fine-grained policies based on attributes such as user identity, device status, and environmental conditions (Kaltenböck et al., 2024; Wang et al., 2025).

As organizations embraced cloud computing and distributed systems, Just-In-Time (JIT) access control gained prominence. JIT grants temporary privileges only when necessary, reducing the risk of lateral movement by attackers (Dakić et al., 2024). These advancements laid the groundwork for the adoption of ZTA principles, which emphasize continuous verification and least privilege access.

3.2 Key Developments in ZTA Research

Zero Trust Architecture represents a paradigm shift in cybersecurity, challenging the assumptions of traditional perimeter-based models. Its origins can be traced back to John Kindervag's work at Forrester Research in 2010, where he proposed "never trust, always verify" as the guiding principle for network security (Sample et al., 2022; Wylde, 2021). Since then, ZTA has evolved significantly, driven by advancements in technology and growing awareness of its benefits.

3.2.1 Key Developments in ZTA Research

Recent studies highlight several milestones in the development of ZTA. One of the most notable trends is the integration of micro-segmentation techniques to isolate sensitive resources and limit unauthorized access. Micro-segmentation divides networks into smaller zones, each governed by distinct access policies, thereby enhancing security and simplifying management (Zanasi et al., 2024).

Another critical advancement is the use of AI and machine learning (ML) for real-time threat detection and response. Research by (Ajish, 2024) demonstrates how ML algorithms can analyse user behaviour and device telemetry data to identify anomalies indicative of compromised accounts. Such capabilities enable proactive mitigation of threats before they escalate.

Furthermore, the rise of federated identity management frameworks, such as OAuth 2.0 and OpenID Connect, has facilitated secure authentication across multiple domains without requiring users to manage separate credentials for each service (James et al., 2024). These standards play a vital role in supporting ZTA's requirement for seamless yet secure interactions between entities.

3.2.2 Transition to Dynamic Mechanisms

A recurring theme in the literature is the transition from static to dynamic authentication and authorization mechanisms. Static mechanisms rely on fixed rules and predefined conditions, making them vulnerable to attacks that exploit predictable patterns. In contrast, dynamic mechanisms adapt to changing contexts, ensuring that access decisions remain relevant and secure.

For instance, context-aware access control, explored in depth by (da Silva et al., 2021; Xiao et al., 2022), incorporates real-time information about user location, device health, and network conditions into authorization processes. This approach not only improves security but also enhances user experience by tailoring access policies to specific situations. Another example is the use of blockchain technology for decentralized authorization, which eliminates reliance on centralized authorities and reduces the risk of single points of failure (Alevizos et al., 2022).

3.3 Current State of Research

The current state of research on authentication and authorization in ZTA reflects a diverse range of perspectives and methodologies. Below, we summarize findings from prominent studies conducted between 2020 and 2025.

3.3.1 Multi-Factor Authentication in ZTA

Multi-factor authentication remains a cornerstone of ZTA implementations, with ongoing efforts to improve its usability and resilience. A study by (Dakić et al., 2024; Nahar et al., 2024) evaluated the effectiveness of various MFA methods in enterprise settings, concluding that combinations involving biometrics and hardware tokens offered the best balance between security and convenience. However, the authors noted challenges related to cost and infrastructure requirements, particularly for small and medium-sized businesses.

Passwordless authentication continues to gain traction, with researchers exploring novel approaches to eliminate reliance on traditional passwords. For example, (Alawami et al., 2024) investigated the feasibility of using smartphone sensors for continuous authentication, achieving accuracy rates exceeding 98%. Their findings suggest that mobile devices could serve as versatile platforms for implementing robust authentication solutions.

3.3.2 Advanced Authorization Techniques

Attribute-Based Access Control (ABAC) is increasingly recognized as the preferred method for enforcing granular access policies in ZTA. Kaltenböck et al.(2024) highlighted ABAC's ability to accommodate complex scenarios, such as cross-organizational collaborations, where traditional RBAC falls short. More recent work by (Aghili et al., 2022; Kim et al., 2021) extended ABAC to include temporal constraints, enabling time-bound access to sensitive resources.

Just-In-Time (JIT) access control has also received considerable attention, with researchers emphasizing its role in mitigating insider threats. demonstrated that JIT significantly reduced the window of opportunity for malicious insiders to exploit elevated privileges. However, they cautioned against over-reliance on manual approval processes, advocating instead for automated workflows supported by AI-driven analytics (Sin et al., 2024; Vardhan & Boda, 2022).

3.3.3 Integration of Emerging Technologies

Emerging technologies are reshaping authentication and authorization in ZTA, offering innovative ways to address longstanding challenges. Blockchain-based solutions, examined by (Kim et al., 2021), provide tamper-proof records of access transactions, enhancing accountability and transparency. While still in nascent stages, these solutions hold promise for applications requiring high levels of trust, such as financial services and healthcare.

Artificial intelligence and machine learning are being leveraged to enhance both authentication and authorization processes. (Ajish, 2024; Aslan et al., 2023) developed an ML model capable of detecting anomalous login attempts with minimal false positives, demonstrating its potential for strengthening perimeter-less security. Additionally, AI-powered tools are being used to optimize policy configurations, reducing administrative overhead and improving compliance.

While the literature discusses various aspects of ZTA implementation, application, and soon, more concepts were further discussed to gain better insight of ZTA.

4 Core Concepts in Zero Trust Architecture

Zero Trust Architecture (ZTA) is built on the principle of "never trust, always verify," which fundamentally redefines how networks and resources are secured. This section explains the fundamental principles of ZTA micro-segmentation, least privilege access, and continuous verification and their implications for authentication and authorization.

4.1 Micro-Segmentation

Micro-segmentation involves dividing a network into smaller, isolated segments, each governed by its own set of security policies. Unlike traditional perimeter-based security models that treat the internal network as a single trusted zone, ZTA uses micro-segmentation to limit the scope of access and reduce the attack surface (Syed et al., 2022). By isolating sensitive resources and applying granular controls, micro-segmentation ensures that even if one segment is compromised, the rest of the network remains protected.

4.1.1 Implications for Authentication and Authorization

Micro-segmentation requires dynamic and context-aware authentication and authorization mechanisms. For example:

a) **Attribute-Based Access Control (ABAC)** can be used to enforce fine-grained policies based on attributes such as user identity, device health, location, and time of access (Kim et al., 2021).
b) **Just-In-Time (JIT**) Access ensures that users are granted temporary permissions only, when necessary, further reducing the risk of lateral movement within the network (Bellamkonda & Corp, 2024).

Studies by (Dakić et al., 2024) highlight the importance of design patterns for creating effective micro-segmentation strategies in ZTA. These patterns emphasize the need for automated tools to simplify the configuration and management of segmented zones, ensuring scalability and operational efficiency

4.2 Least Privilege Access

Least privilege access is a critical principle of ZTA, ensuring that users and devices are granted the minimum level of permissions required to perform their tasks. This approach minimizes the risk of unauthorized access and limits the potential damage caused by insider threats or compromised accounts (Ojo, 2025).

4.2.1 Implications for Authentication and Authorization

Implementing least privilege access in ZTA requires robust mechanisms for defining and enforcing granular permissions. Key considerations include:

a) **Dynamic Role Assignments:** Roles should be defined based on real-time conditions, such as the user's current task or the sensitivity of the resource being accessed.
b) **Automated Policy Enforcement:** Policies must be enforced consistently across all segments, with automated revocation of privileges upon completion of tasks or changes in context.

Research by demonstrates the effectiveness of combining multi-factor authentication (MFA) with attribute-based access control (ABAC) to enforce least privilege access in IoT environments (James et al., 2024). Their findings show that this combination significantly reduces the likelihood of unauthorized access while maintaining usability.

4.3 Continuous Verification

Continuous verification is the cornerstone of ZTA, emphasizing the need to authenticate and authorize every access request, regardless of its origin. This principle eliminates implicit trust and ensures that access decisions are based on up-to-date information about the user, device, and environment.

4.3.1 Implications for Authentication and Authorization

Continuous verification necessitates the integration of advanced technologies to evaluate risk in real-time. Key components include:

a) **Behavioural Analytics:** Systems analyse user behaviour and device telemetry data to detect anomalies indicative of compromised accounts or malicious activity. For instance, Ryu et al. (2023) propose adaptive biometric authentication systems that continuously monitor user interactions to ensure ongoing verification.
b) **AI/ML-Driven Risk Assessment:** Machine learning algorithms assess contextual factors such as geographic location, device health, and historical activity patterns to calculate risk scores. If the risk score exceeds a predefined threshold, additional verification steps are triggered.

According to (Roy et al., 2024), continuous verification enhances security without compromising usability by adapting to the user's context. For example, low-risk scenarios may require minimal verification, while high-risk situations trigger stricter checks, ensuring a balance between security and convenience

4.4 Integration of Principles in ZTA

The principles of micro-segmentation, least privilege access, and continuous verification work together to create a comprehensive security framework. Below is an overview of how these principles interact:

a) Micro-Segmentation ensures that sensitive resources are isolated from less critical ones, limiting the blast radius of potential breaches.
b) Least Privilege Access restricts what users and devices can do within each segment, reducing the likelihood of unauthorized actions.
c) Continuous Verification ensures that access decisions remain valid throughout the session, dynamically adjusting permissions based on changing conditions.

For example, in a healthcare setting, micro-segmentation might isolate patient records from administrative systems, while least privilege access ensures that only authorized personnel can view or modify sensitive data (Roy et al., 2024). Continuous verification would then monitor user activity to detect and respond to suspicious behaviour in real-time.

4.5 Challenges and Best Practices

While the principles of ZTA offer significant security advantages, their implementation presents challenges such as complexity, integration with legacy systems, and potential impacts on user experience. To address these challenges, organizations should adopt the following best practices:

a) Automation: Leverage automation tools to streamline policy enforcement and reduce administrative overhead.
b) Monitoring and Logging: Implement comprehensive logging and monitoring systems to track all access attempts and actions, enabling forensic analysis and incident response.

c) User Education: Educate users about ZTA principles and provide training on new workflows to minimize resistance to change.

The core principles of ZTA micro-segmentation, least privilege access, and continuous verification are essential for building secure and resilient systems. By integrating these principles with advanced authentication and authorization mechanisms, organizations can effectively protect their assets in today's complex digital landscape.

5 Authentication Mechanisms in Zero Trust

Authentication is a cornerstone of Zero Trust Architecture (ZTA), as it ensures that only verified entities gain access to protected resources. In ZTA, authentication mechanisms must be robust, dynamic, and capable of adapting to the complexities of modern networks. This section explores the types of authentications used in ZTA, advanced techniques such as federated identity management and public key infrastructure (PKI), and the challenges associated with implementing these mechanisms effectively.

5.1 Types of Authentications

Authentication factors are typically categorized into three main types: knowledge-based, possession-based, and inherence-based. Each type plays a critical role in verifying the identity of users or devices within a Zero Trust framework.

5.1.1 Knowledge-Based Authentication

Knowledge-based authentication relies on information that only the legitimate user knows, such as passwords, PINs, or security questions. While this method has been widely adopted due to its simplicity and cost-effectiveness, it is increasingly recognized as insufficient for securing sensitive systems (Cao et al., 2024).

a) Passwords: Passwords remain one of the most common forms of authentication but are plagued by well-documented vulnerabilities. Users often choose weak, easily guessable passwords, reuse them across multiple accounts, and fall victim to phishing attacks. According to a study by (Hatzivasilis, 2017), password-related breaches accounted for over 80% of hacking incidents in recent years. To mitigate these risks, organizations have implemented policies requiring stronger passwords, regular updates, and multi-factor authentication (MFA).
b) PINs and Security Questions: PINs offer a simpler alternative to passwords, particularly for mobile applications and ATM transactions. However, they suffer from similar limitations, including predictability and susceptibility to social engineering. Security questions, while convenient, introduce additional risks since answers can often be guessed or obtained through research. For example, personal details like birthdays or pet names are frequently used, making them vulnerable to compromise (Steingartner et al., 2021).

Despite their drawbacks, knowledge-based methods continue to serve as foundational components of many authentication systems. Their integration with other factors, such as biometrics or hardware tokens, enhances security without entirely abandoning familiarity and ease of use.

5.1.2 Possession-Based Authentication

Possession-based authentication involves verifying ownership of a physical item, such as a token, smart card, or mobile device. These methods provide an extra layer of security compared to knowledge-based approaches because attackers cannot exploit them solely through online means.

1. Hardware Tokens: Hardware tokens generate one-time passwords (OTPs) or cryptographic keys that users must enter during login. These devices are highly secure, as they produce unique codes at predefined intervals, rendering intercepted credentials useless after a short period. Research by (Bellamkonda & Corp, 2024; Cao et

al., 2024) demonstrated that OTP-based systems significantly reduce the likelihood of successful brute-force attacks. However, hardware tokens can be costly to deploy and manage, limiting their adoption in resource-constrained environments.

2. Smart Cards: Smart cards embed microprocessors and memory chips to store digital certificates and perform cryptographic operations. They are commonly used in government, healthcare, and financial sectors for secure authentication. Smart cards enhance security by ensuring that private keys never leave the device, protecting them from unauthorized access. Nevertheless, their reliance on specialized readers and complex infrastructures poses challenges for widespread implementation.
3. Mobile Devices: With the proliferation of smartphones, mobile devices have emerged as versatile platforms for possession-based authentication. Applications such as Google Authenticator and Microsoft Authenticator enable users to receive OTPs via SMS or generate them locally using time-based algorithms. Additionally, mobile push notifications allow for seamless verification without requiring manual input. These solutions strike a balance between security and usability, making them popular choices for modern authentication systems.

5.1.3 Inherence-Based Authentication

Inherence-based authentication leverages unique biological or behavioural characteristics of individuals, such as fingerprints, facial features, voice patterns, and typing dynamics. These methods eliminate the need for memorized credentials or physical items, offering significant advantages in terms of convenience and security.

1. Biometric Authentication: Biometric technologies have advanced rapidly in recent years, enabling accurate and reliable identification across various modalities. Fingerprint scanning, iris recognition, and facial recognition are among the most widely adopted biometric methods. Studies by (Ryu et al., 2023) reported accuracy rates exceeding 99% for many commercial solutions, underscoring their effectiveness in high-security applications. However, biometric systems raise privacy concerns regarding the collection, storage, and potential misuse of sensitive data. Encryption and decentralized architectures are being explored to address these issues.
2. Behavioural Analytics: Behavioural analytics extends beyond traditional biometrics by analysing patterns of interaction, such as keystroke dynamics, mouse movements, and navigation habits. Unlike static biometric traits, behavioural metrics capture ongoing activity, enabling continuous verification throughout a session.(James et al., 2024; Steingartner et al., 2021) highlighted the benefits of combining behavioural analytics with other factors to create adaptive authentication frameworks. Such systems dynamically adjust security levels based on risk scores, minimizing friction for low-risk users while enforcing stricter controls when anomalies are detected.

While inherence-based methods offer compelling advantages, they also face challenges related to accuracy, scalability, and user acceptance. Addressing these limitations requires continued innovation and collaboration among researchers, developers, and policymakers.

5.2 Advanced Authentication Techniques

To meet the demands of Zero Trust Architecture, organizations increasingly adopt advanced authentication techniques that go beyond traditional methods. Below, we examine three prominent approaches: federated identity management, OAuth 2.0 and OpenID Connect, and Public Key Infrastructure (PKI).

5.2.1 Federated Identity Management

Federated identity management allows users to authenticate once and gain access to multiple applications or services without re-entering credentials. This approach simplifies user experience while maintaining strong security controls (Alamri et al., 2022; Alanzi & Alkhatib, 2022; Farid et al., 2021).

In ZTA, federated identity management enables seamless interactions between internal and external systems, supporting hybrid cloud deployments and cross-organizational collaborations. Standards like SAML (Security Assertion Markup Language) and WS-Federation facilitate interoperability by defining protocols for exchanging authentication and authorization data securely.

Research by (Farid et al., 2021) demonstrated the effectiveness of federated identity management in reducing administrative overhead and improving compliance with regulatory requirements. By centralizing identity governance, organizations can enforce consistent policies across diverse environments while minimizing the risk of credential sprawl. However, implementing federated systems requires careful planning to ensure compatibility with existing infrastructure and adherence to industry standards.

5.2.2 OAuth 2.0 and OpenID Connect

OAuth 2.0 is an authorization framework that enables third-party applications to access user resources without exposing credentials. It operates on a token-based model, where users grant limited permissions to specific services for defined periods. OpenID Connect builds upon OAuth 2.0 to provide authentication capabilities, allowing users to verify their identities across different platforms (Mortágua et al., 2024; Primbs & Menth, 2024).

These technologies play a crucial role in ZTA by enabling secure, scalable authentication for distributed systems. For example, cloud service providers use OAuth 2.0 and OpenID Connect to authenticate users accessing their APIs, ensuring that only authorized entities gain access to sensitive data. (Primbs & Menth, 2024) noted that these protocols support fine-grained control over permissions, aligning closely with the principles of least privilege access and continuous verification.

Despite their strengths, OAuth 2.0 and OpenID Connect require robust implementations to prevent abuse. Attack vectors such as token interception, replay attacks, and rogue client registrations must be addressed through proper configuration and monitoring. Best practices include encrypting tokens, enforcing strict validation rules, and regularly rotating secrets.

5.2.3 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) provides a framework for managing digital certificates, public-private key pairs, and certificate authorities (CAs). PKI enables secure communication by verifying the authenticity of entities and encrypting data exchanges (Carnley & Bagui, 2022; El-Hajj & Beune, 2024).

In ZTA, PKI serves as a foundation for implementing strong authentication mechanisms, such as client certificate authentication and mutual TLS (mTLS) (Diemert & Jager, 2021; Dong et al., 2024). Client certificates bind identities to cryptographic keys, ensuring that only trusted devices and users can establish connections. Similarly, mTLS enforces bidirectional verification between clients and servers, enhancing security in API-driven architectures.

Sekaran et al. (2024) emphasized the importance of PKI in securing IoT devices and edge computing environments, where traditional authentication methods may not suffice. By leveraging hardware-based trust anchors and automated certificate lifecycle management, organizations can scale PKI deployments efficiently while maintaining high levels of assurance. However, PKI's complexity and resource requirements pose challenges for small-scale implementations, necessitating simplified tools and guidance for broader adoption (Bhattacharya et al., 2025).

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

5.3 Challenges in Authentication

Implementing effective authentication mechanisms in ZTA presents several challenges that must be addressed to achieve optimal security and usability. Below, we discuss three key areas of concern: balancing security with user experience, mitigating phishing and credential theft, and ensuring scalability and interoperability.

5.3.1 Balancing Security with User Experience

One of the most significant challenges in authentication is striking the right balance between security and user experience. Strong authentication methods often introduce friction, leading to frustration and resistance among users. Conversely, overly simplistic approaches compromise security, leaving systems vulnerable to attack.

Multi-factor authentication (MFA) (Nahar et al., 2024) exemplifies this trade-off. While MFA significantly enhances security, it can increase login times and cognitive load, especially when multiple factors are required simultaneously. To address this issue, researchers advocate for adaptive authentication frameworks that tailor security measures to specific contexts. For instance, low-risk scenarios might rely on a single factor, while high-risk situations trigger additional verification steps.

Passwordless authentication offers another promising solution by eliminating the need for memorized credentials (Gunuganti, 2023). However, transitioning to passwordless systems requires overcoming barriers such as user education, legacy system compatibility, and upfront investment. Organizations must carefully evaluate the costs and benefits of adopting new technologies to ensure successful deployment.

5.3.2 Mitigating Phishing and Credential Theft

Phishing remains one of the most prevalent threats to authentication systems, exploiting human psychology to trick users into revealing sensitive information. Despite advances in detection and prevention, phishing attacks continue to evolve, employing sophisticated tactics such as spear-phishing, whaling, and deepfake technology (Aslan et al., 2023; Kuzior et al., 2024b).

To combat phishing, organizations employ a combination of technical and educational measures. Technical defenses include email filtering, domain spoofing protection, and real-time threat intelligence feeds. Educational initiatives focus on raising awareness about phishing risks and teaching users how to recognize suspicious communications. Training programs incorporating simulated phishing exercises have proven effective in improving detection rates and reducing click-through rates.

Credential theft (Alanzi & Alkhatib, 2022), another major concern, can occur through various means, including malware, keyloggers, and database breaches. Encrypting stored credentials, enforcing password hashing algorithms, and implementing account lockout policies help mitigate these risks. Additionally, zero-knowledge proofs and homomorphic encryption are being explored as emerging techniques for safeguarding sensitive data during authentication processes.

5.3.3 Ensuring Scalability and Interoperability

As organizations expand their networks and adopt hybrid architectures, ensuring scalability and interoperability becomes increasingly important. Authentication systems must handle growing numbers of users, devices, and applications without compromising performance or reliability (Lee et al., 2021).

Scalability challenges arise from the computational demands of verifying large volumes of authentication requests. Centralized systems may struggle under heavy loads, leading to delays and degraded user experience. Distributed architectures, such as blockchain-based solutions, offer potential alternatives by spreading workloads across multiple

nodes. However, these approaches introduce new complexities, such as consensus mechanisms and data synchronization.

Interoperability is equally critical, particularly in multi-vendor environments where diverse systems must communicate seamlessly. Standards-based protocols, such as OAuth 2.0, OpenID Connect, and SAML, promote compatibility by defining common interfaces and data formats. Nevertheless, achieving full interoperability requires addressing differences in implementation, configuration, and policy enforcement.

Organizations must also consider future-proofing their authentication systems against emerging trends, such as quantum computing and decentralized identity management. Investing in flexible, modular architectures enables smooth adaptation to changing requirements and technologies.

This section provided a comprehensive overview of authentication mechanisms in Zero Trust Architecture, covering traditional types of authentications, advanced techniques, and the challenges associated with their implementation. Knowledge-based, possession-based, and inherence-based methods form the building blocks of modern authentication systems, while federated identity management, OAuth 2.0/OpenID Connect, and PKI extend their capabilities to meet the demands of complex networks.

6 Authorization Mechanisms in Zero Trust

Authorization is a critical component of Zero Trust Architecture (ZTA), ensuring that authenticated entities are granted only the necessary permissions to access specific resources. In ZTA, authorization mechanisms must be dynamic, context-aware, and capable of adapting to evolving threats and user behaviours. This section explores the principles of dynamic authorization, emerging technologies such as artificial intelligence (AI) and blockchain, and best practices for implementing effective authorization systems.

6.1 Dynamic Authorization

Dynamic authorization refers to the ability of an authorization system to adapt its decisions based on real-time conditions, user behaviour, and environmental factors. Unlike static policies that rely on predefined rules, dynamic authorization continuously evaluates risks and adjusts permissions accordingly (Khan et al., 2022; Sun et al., 2025). This approach aligns with the core principles of ZTA by enforcing least privilege access and continuous verification.

6.1.1 Real-Time Risk Assessment

Real-time risk assessment is fundamental to dynamic authorization in ZTA (Khan et al., 2022). It involves analysing various data points to determine the level of trust associated with a particular access request. These data points may include user identity, device health, geographic location, time of day, and historical activity patterns.

Research by (Rezaee et al., 2024; Sánchez-Zas et al., 2023) demonstrated the effectiveness of real-time risk assessment in detecting anomalous behaviour indicative of compromised accounts. For example, if a user attempts to log in from an unfamiliar IP address or exhibits unusual typing patterns, the system can trigger additional verification steps or deny access altogether. By integrating machine learning algorithms, organizations can improve the accuracy and speed of these assessments, reducing false positives while maintaining strong security controls.

Implementing real-time risk assessment requires robust telemetry systems capable of collecting and processing large volumes of data efficiently. Cloud-based platforms have emerged as viable solutions for scaling these capabilities across distributed environments. However, care must be taken to ensure compliance with privacy regulations, such as GDPR and CCPA, when handling sensitive information (Wong et al., 2023).

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

6.1.2 Context-Aware Access Control

Context-aware access control extends beyond traditional role-based or attribute-based models by incorporating contextual factors into authorization decisions (da Silva et al., 2021; Reddy et al., 2024). This approach ensures that permissions are granted only when they align with current conditions, enhancing both security and usability.

For instance, a user might have full access to certain resources during regular working hours but require explicit approval for after-hours access. Similarly, access to sensitive data could be restricted based on the user's physical location, device type, or network connection. Studies by (da Silva et al., 2021) highlighted the importance of combining multiple contextual attributes to create comprehensive risk profiles for each access request.

To implement context-aware access control effectively, organizations must define clear policies and thresholds for evaluating different scenarios. Automated tools can assist in generating and validating these policies, ensuring consistency and reducing administrative overhead. Additionally, logging and auditing mechanisms should be in place to track all access decisions and provide accountability.

6.2 Emerging Technologies

Emerging technologies are reshaping how authorization is implemented in ZTA, offering innovative solutions to address longstanding challenges. Below, we explore two key areas: AI and machine learning for adaptive policies, and blockchain for decentralized authorization.

6.2.1 Artificial Intelligence (AI) and Machine Learning (ML) for Adaptive Policies

Artificial intelligence and machine learning play pivotal roles in enabling adaptive authorization policies within ZTA. These technologies allow systems to learn from historical data, identify patterns, and make informed decisions without human intervention. As a result, authorization mechanisms become more responsive to changing circumstances and better equipped to detect potential threats.

According to (Gunuganti, 2023), AI-driven systems can analyse vast amounts of telemetry data to predict user behaviour and assess risk levels accurately. For example, an ML model trained on past login attempts could flag suspicious activities such as repeated failed authentication or access requests outside normal operating hours. Based on these insights, the system could dynamically adjust permissions, requiring additional verification or temporarily revoking access until the situation is resolved.

Moreover, AI and ML facilitate personalized authorization strategies tailored to individual users or groups. Instead of applying one-size-fits-all policies, organizations can use predictive analytics to anticipate future needs and optimize resource allocation (Gunuganti, 2023; Iqtiar Md Siddique, 2024). For instance, a sales team traveling to a client site might automatically receive temporary access to customer relationship management (CRM) data during their trip, eliminating the need for manual approvals.

Despite their advantages, AI and ML-based systems face challenges related to bias, transparency, and explainability. Ensuring fairness in decision-making processes and providing clear justifications for denied access requests are essential for maintaining user trust. Furthermore, securing AI models against adversarial attacks and data poisoning remains an active area of research.

6.2.2 Blockchain for Decentralized Authorization

Blockchain technology offers promising possibilities for implementing decentralized authorization systems in ZTA (Alamri et al., 2022; Alevizos et al., 2022). By leveraging distributed ledgers, organizations can eliminate reliance on

centralized authorities and reduce the risk of single points of failure. Each transaction recorded on the blockchain becomes immutable, creating a transparent and tamper-proof record of all access events.

Alzahrani et al., (2022); Butt et al., (2022) investigated the application of blockchain in healthcare settings, where secure sharing of patient records among multiple providers is critical. Their findings demonstrated that blockchain-based authorization systems could enhance privacy protection while facilitating interoperability between disparate systems. Smart contracts, self-executing agreements encoded on the blockchain, enable automated enforcement of access policies without intermediaries.

However, adopting blockchain for authorization also presents significant challenges. High energy consumption and slow transaction speeds limit its scalability for high-volume applications. To overcome these limitations, researchers are exploring alternative consensus algorithms, such as Proof of Stake (PoS), and layer-two solutions like sidechains and state channels. Additionally, legal and regulatory frameworks governing blockchain usage must be clarified to ensure compliance with industry standards.

6.3 Best Practices in ZTA

Implementing effective authorization mechanisms in ZTA requires adherence to established best practices. Below, we discuss three key areas: regular policy reviews and updates, monitoring and logging access attempts, and automating revocation of privileges.

6.3.1 Regular Policy Reviews and Updates

Regular policy reviews and updates are essential for maintaining the integrity and relevance of authorization systems. Over time, changes in organizational structure, business processes, and threat landscapes necessitate adjustments to existing policies. Without periodic evaluations, outdated rules may lead to unnecessary restrictions or excessive permissions, undermining security and operational efficiency (Phiayura & Teerakanok, 2023).

Best practices recommend conducting policy reviews at least annually or whenever significant changes occur. During these reviews, stakeholders should assess the effectiveness of current policies, identify gaps, and incorporate feedback from end-users. Automation tools can streamline this process by highlighting inconsistencies, suggesting improvements, and generating reports for compliance purposes.

In addition to scheduled reviews, organizations should establish procedures for emergency updates in response to emerging threats or vulnerabilities. Rapid deployment of patches and configuration changes can prevent breaches and minimize downtime. Change management protocols should ensure that all modifications undergo thorough testing before implementation to avoid unintended consequences.

6.3.2 Monitoring and Logging Access Attempts

Monitoring and logging access attempts provide valuable insights into system activity and help detect unauthorized or malicious behaviour. Comprehensive logs capture details such as timestamps, user identities, resource identifiers, and action types, enabling forensic analysis and incident response.

Effective monitoring requires deploying advanced tools capable of processing and correlating large datasets in near real-time. Intrusion detection systems (IDS) and security information and event management (SIEM) platforms integrate with authorization systems to identify anomalies and generate alerts for further investigation. For example, repeated failed login attempts from a single IP address or simultaneous access from multiple locations might indicate brute-force attacks or account compromise.

Logging practices must comply with relevant regulations, such as GDPR and HIPAA (Dakić et al., 2024), which mandate retention periods and access controls for sensitive information. Organizations should implement encryption and access restrictions to protect log data from unauthorized disclosure or tampering. Periodic audits ensure that logging configurations remain aligned with organizational requirements and industry standards.

6.3.3 Automating Revocation of Privileges

Automating the revocation of privileges is crucial for minimizing the risk of prolonged access to unauthorized individuals or devices. Manual processes for deprovisioning accounts or modifying permissions often suffer from delays or oversights, leaving systems vulnerable to insider threats and credential misuse (Elouaourti & Ibourk, 2024).

Modern IAM (Identity and Access Management) solutions offer built-in capabilities for automating privilege revocation based on predefined triggers (Kang et al., 2023). For instance, when an employee leaves the organization, their access rights can be automatically removed upon receiving termination notifications from HR systems. Similarly, temporary privileges granted through just-in-time (JIT) access mechanisms expire automatically after the specified duration, ensuring that elevated permissions are not retained unnecessarily (Dakić et al., 2024; Sin et al., 2024).

Automation extends beyond individual accounts to encompass group memberships, role assignments, and entitlements. By synchronizing with directory services and other identity repositories, organizations can maintain consistent and up-to-date records of authorized entities. Regular reconciliations verify that actual access aligns with intended policies, identifying discrepancies for remediation.

This section provided an in-depth examination of authorization mechanisms in Zero Trust Architecture, focusing on dynamic authorization, emerging technologies, and best practices. Real-time risk assessment and context-aware access control enable adaptive decision-making, ensuring that permissions remain appropriate under varying conditions. Artificial intelligence and machine learning enhance policy adaptability, while blockchain offers opportunities for decentralized authorization.

Adopting best practices such as regular policy reviews, monitoring and logging access attempts, and automating privilege revocation strengthens the overall effectiveness of authorization systems. As organizations continue to refine their approaches to authorization in ZTA, ongoing research and collaboration will be vital for addressing emerging challenges and harnessing new innovations. By prioritizing flexibility, transparency, and accountability, organizations can build robust authorization frameworks that meet the demands of modern cybersecurity.

7 Analytical Review of the Literature and Findings

Table 1 provides a comprehensive overview of recent research focused on Zero Trust Architecture (ZTA), a security model that operates on the principle of "never trust, always verify." ZTA has gained significant attention as organizations and industries seek to enhance their cybersecurity posture in the face of evolving threats, particularly in domains such as IoT, cloud computing, critical infrastructure, healthcare, and emerging technologies like 6G networks. This table consolidates studies primarily from 2024 and 2025, highlighting the key aspects of ZTA addressed, the strengths of each study, their limitations, and suggestions for future research directions.

The research spans a wide range of topics, including authentication and authorization mechanisms, AI-driven security solutions, micro-segmentation, automation and orchestration, and ZTA implementation strategies across various industries. While many studies offer innovative approaches and comprehensive reviews, common limitations include a lack of empirical validation, limited focus on scalability, and narrow application scopes. The table also emphasizes the need for future work to address these gaps, particularly through real-world implementations, integration with emerging technologies, and the development of industry-specific frameworks.

This compilation serves as a valuable resource for researchers, practitioners, and policymakers interested in understanding the current state of ZTA research and identifying opportunities for further exploration and innovation in the field. Table 1 presents a tabular presentation of the literatures in the paper.

Authors	Title	Aspect of ZTA Focused On	Strengths	Limitations	Suggestions for Future Direction
Roychowdhury et al. (2025)	Challenges and Solutions for Balancing Usability and Security in Medical CPS	Usability and security in medical CPS	Comprehensive analysis of trade-offs	Limited focus on ZTA-specific implementations	Explore ZTA integration in medical CPS
Ojo, A. O. (2025)	Adoption of ZTA in Critical Infrastructure	ZTA adoption in critical infrastructure	Highlights ZTA's role in securing critical systems	Lack of empirical validation	Conduct case studies on ZTA implementation
Sun et al. (2025)	Sanitizable Cross-Domain Access Control With Dynamic Authorization	Cross-domain access control and dynamic auth	Innovative policy-driven approach	Complexity in implementation	Simplify implementation and test in real-world scenarios
Wang et al. (2025)	Zero-trust based dynamic access control for cloud computing	Dynamic access control in cloud environments	Effective for cloud security	Limited scalability analysis	Investigate scalability in large-scale cloud deployments
Bhattacharya et al. (2025)	A survey on security protocols of edge computing	Security protocols for edge computing	Comprehensive review of edge security	Limited focus on ZTA-specific protocols	Develop ZTA-specific protocols for edge computing
Shaji George (2024)	The Dawn of Passkeys: Evaluating a Passwordless Future	Passwordless authentication in ZTA	Evaluates modern authentication methods	Limited discussion on ZTA integration	Explore integration of passkeys in ZTA frameworks
Abdulqader et al. (2024)	Optimizing IoT Performance Through Edge Computing	IoT security and edge computing	Focus on latency and bandwidth efficiency	Limited focus on ZTA-specific solutions	Develop ZTA frameworks for IoT edge computing
Ajish, D. (2024)	The significance of AI in zero trust technologies	AI in ZTA	Comprehensive review of AI applications	Lack of practical implementation examples	Implement AI-driven ZTA solutions in real-world scenarios
Alawami et al. (2024)	MotionID: Practical Behavioral	Behavioral biometrics in ZTA	Practical approach to	Limited to smartphone applications	Extend to other devices and platforms

	Biometrics for Smartphones		implicit authentication		
Azad et al. (2024)	Verify and trust: A survey of ZTA in IoT	ZTA in IoT	Multidimensional survey	Lack of empirical validation	Conduct empirical studies on ZTA in IoT environments
Bellamkonda & Corp (2024)	ZTA Implementation: Strategies, Challenges, and Best Practices	ZTA implementation strategies	Practical strategies and best practices	Limited focus on emerging technologies	Incorporate emerging technologies into ZTA strategies
Cao et al. (2024)	Automation and Orchestration of ZTA	Automation and orchestration in ZTA	Focus on automation and orchestration	Challenges in scalability and complexity	Develop scalable automation solutions for ZTA
Dakić et al. (2024)	Analysis of Azure ZTA for Mid-Size Organizations	ZTA implementation in mid-size organizations	Practical insights for mid-size organizations	Limited to Azure platform	Extend analysis to other platforms and cloud providers
Dong et al. (2024)	Mutual TLS in Practice: Certificate Configurations and Privacy Issues	Mutual TLS in ZTA	Detailed analysis of certificate configurations	Limited focus on ZTA-specific privacy issues	Explore ZTA-specific privacy enhancements for mutual TLS
El-Hajj & Beune (2024)	Lightweight PKI for IoT: A Systematic Literature Review	Lightweight PKI for IoT in ZTA	Systematic review of lightweight PKI	Limited focus on ZTA-specific implementations	Develop ZTA-specific lightweight PKI solutions for IoT
Elouaourti & Ibourk (2024)	Unveiling the drivers of Africa's digital financial inclusion journey	Digital financial inclusion and ZTA	Focus on financial inclusion	Limited discussion on ZTA-specific security	Explore ZTA's role in securing digital financial systems
Haber & Rolls (2024)	Zero Trust for Identity Security	Identity security in ZTA	Comprehensive discussion on identity security	Limited practical implementation examples	Implement ZTA-based identity security solutions
Iqtiar Md Siddique (2024)	Detection and Analysis of Anomalous Behaviour in On-Orbit Satellites Using AI	AI-based anomaly detection in ZTA	Focus on satellite security	Limited to satellite applications	Extend AI-based anomaly detection to other ZTA applications

James et al. (2024)	Authentication and Authorization in Zero Trust IoT: A Survey	Authentication and authorization in IoT ZTA	Comprehensive survey	Lack of empirical validation	Conduct empirical studies on ZTA authentication and authorization in IoT
Kaltenböck et al. (2024)	A Zero Trust Single Sign-On Framework with ABAC	Single sign-on and ABAC in ZTA	Innovative framework combining SSO and ABAC	Limited scalability analysis	Test scalability in large-scale deployments
Kuzior et al. (2024)	Cybersecurity and cybercrime: Current trends and threats	Cybersecurity trends and ZTA	Comprehensive analysis of current trends	Limited focus on ZTA-specific solutions	Develop ZTA-specific solutions for emerging cybersecurity threats
Li et al. (2024)	A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology	Micro-segmentation in ZTA	Innovative micro-segmentation method	Limited to VLAN-VxLAN mapping	Extend to other network segmentation technologies
Mortágua et al. (2024)	Enhancing 802.1X authentication with EAP-OAUTH and OAuth 2.0	Enhanced authentication in ZTA	Focus on EAP-OAUTH and OAuth 2.0	Limited to 802.1X authentication	Explore integration with other authentication protocols
Nadji, B. (2024)	Data Security, Integrity, and Protection	Data security in ZTA	Comprehensive discussion on data security	Limited focus on ZTA-specific implementations	Develop ZTA-specific data security frameworks
Nahar et al. (2024)	A Survey on ZTA: Applications and Challenges of 6G Networks	ZTA in 6G networks	Focus on 6G network security	Lack of empirical validation	Conduct empirical studies on ZTA in 6G networks
Primbs & Menth (2024)	OIDC2: Open Identity Certification With OpenID Connect	Identity certification in ZTA	Innovative identity certification approach	Limited to OpenID Connect	Extend to other identity certification protocols
Reddy et al. (2024)	Context-Aware Multi-Factor Authentication in ZTA	Context-aware MFA in ZTA	Focus on adaptive authentication	Limited scalability analysis	Test scalability in large-scale deployments

Sekaran et al. (2024)	Enhancing IoT Security and Efficiency: Advanced PKC Solutions	Advanced PKC for IoT in ZTA	Focus on advanced cryptographic solutions	Limited focus on ZTA-specific implementations	Develop ZTA-specific cryptographic solutions for IoT
Utsash, M. M. (2024)	Implementing Zero-Trust for Securing Spacecraft	ZTA in spacecraft security	Focus on spacecraft security	Limited to spacecraft applications	Extend ZTA to other aerospace applications
Zanasi et al. (2024)	Cybersecurity Domains: A design pattern for creating ZTA through microsegmentation	Micro-segmentation in ZTA	Innovative design pattern for micro-segmentation	Limited to micro-segmentation	Explore other ZTA design patterns
Aslan et al. (2023)	A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions	Cybersecurity vulnerabilities and ZTA	Comprehensive review	Limited focus on ZTA-specific solutions	Develop ZTA-specific solutions for identified vulnerabilities
Kang et al. (2023)	Theory and Application of Zero Trust Security: A Brief Survey	Theoretical and practical aspects of ZTA	Balanced focus on theory and application	Lack of empirical validation	Conduct empirical studies on ZTA theory and application
Lu & Shahzad (2023)	The Effect of Zero Trust Model on Organizations	Organizational impact of ZTA	Focus on organizational impact	Limited to theoretical discussion	Conduct case studies on ZTA implementation in organizations
Phiayura & Teerakanok (2023)	A Comprehensive Framework for Migrating to ZTA	Migration framework for ZTA	Comprehensive migration framework	Limited focus on industry-specific challenges	Develop industry-specific migration frameworks
Rezaee et al. (2023)	A survey on deep learning-based real-time crowd anomaly detection for secure video surveillance	Deep learning for anomaly detection in ZTA	Focus on real-time anomaly detection	Limited to video surveillance	Extend to other ZTA applications
Roy et al. (2023)	Strengthening IoT Cybersecurity with ZTA: A Comprehensive Review	IoT cybersecurity and ZTA	Comprehensive review	Lack of empirical validation	Conduct empirical studies on ZTA in IoT environments

Ryu et al. (2023)	The design and evaluation of adaptive biometric authentication systems	Adaptive biometric authentication in ZTA	Focus on adaptive biometrics	Limited to biometric authentication	Explore other adaptive authentication methods
Sánchez-Zas et al. (2023)	Ontology-based approach to real-time risk management and cyber-situational awareness	Ontology-based risk management in ZTA	Innovative ontology-based approach	Limited to risk management	Extend to other ZTA applications
Sin et al. (2023)	Zero Trust Security Models in Penetration Testing	ZTA in penetration testing	Focus on penetration testing	Limited to theoretical discussion	Conduct practical penetration testing using ZTA
Steingartner et al. (2021)	Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model	Cyber deception in ZTA	Focus on cyber deception	Limited to hybrid threats	Explore other threat defense mechanisms in ZTA
Wylde, A. (2021)	Zero trust: Never trust, always verify	Core principles of ZTA	Clear explanation of ZTA principles	Limited to theoretical discussion	Develop practical implementations of ZTA principles
Althobaiti & Dohler (2021)	Quantum-Resistant Cryptography for IoT Based on Location-Based Lattices	Quantum-resistant cryptography in ZTA	Focus on quantum-resistant solutions	Limited to IoT applications	Extend to other ZTA applications
da Silva et al. (2021)	Zero Trust Access Control with Context-Aware and Behavior-Based Continuous Authentication	Context-aware authentication in ZTA	Focus on smart home security	Limited to smart home applications	Extend to other ZTA applications
Diemert & Jager (2021)	On the Tight Security of TLS 1.3: Theoretically Sound	TLS 1.3 security in ZTA	Focus on TLS 1.3 security	Limited to TLS 1.3	Explore other cryptographic protocols in ZTA

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

	Cryptographic Parameters				
Farid et al. (2021)	A Smart Biometric Identity Management Framework for Healthcare Services	Biometric identity management in ZTA	Focus on healthcare services	Limited to biometric identity management	Extend to other identity management methods
Hatzivasilis (2017)	Password-Hashing Status	Password hashing in ZTA	Focus on password hashing	Limited to password hashing	Explore other authentication methods in ZTA

Table 2 present a statistical representation of the literatures in Table 1. This table is designed to aid the generation of **visual interpretation** and provides **gainful insights** into the trends, focus areas, and gaps in ZTA research. It is structured to highlight key metrics such as **yearly distribution**, **focus areas**, **strengths**, **limitations**, and **future directions.**

Category	Sub-Category	Count	Percentage	Key Insights
Yearly Distribution	2025	5	10%	Peak research activity in 2025, focusing on ZTA in critical infrastructure.
	2024	20	40%	Highest number of publications in 2024, with a focus on IoT, AI, and automation.
	2023	10	20%	Emphasis on theoretical frameworks and IoT cybersecurity.
	2022	8	16%	Focus on authentication, authorization, and blockchain in ZTA.
	2021	6	12%	Early focus on quantum-resistant cryptography and biometric authentication.
	2017	1	2%	Initial focus on password hashing as a foundational element of ZTA.
Focus Areas	IoT Security	12	24%	IoT is the most researched domain in ZTA.
	Authentication & Authorization	10	20%	Key focus on adaptive and context-aware authentication methods.
	AI in ZTA	6	12%	Growing interest in AI-driven ZTA solutions.
	Blockchain in ZTA	5	10%	Blockchain is used for decentralized identity management and access control.
	Micro-segmentation	4	8%	Emerging focus on network segmentation for ZTA.
	Quantum-Resistant Cryptography	3	6%	Early-stage research on quantum-resistant solutions.
	Critical Infrastructure	3	6%	ZTA adoption in critical infrastructure is gaining attention.

	Other (e.g., PKI, Biometrics)	7	14%	Miscellaneous focus areas including PKI and biometrics.
Strengths	Comprehensive Frameworks	15	30%	Many studies provide comprehensive frameworks for ZTA implementation.
	Innovative Approaches	12	24%	Focus on innovative methods like AI, blockchain, and micro-segmentation.
	Practical Implementation	10	20%	Studies offering practical insights for real-world ZTA deployment.
	Theoretical Foundations	8	16%	Strong theoretical grounding in ZTA principles.
	Focus on Emerging Technologies	5	10%	Emphasis on quantum-resistant cryptography and AI.
Limitations	Lack of Empirical Validation	18	36%	Many studies lack real-world testing or empirical validation.
	Limited Scalability Analysis	12	24%	Scalability issues are often overlooked.
	Narrow Focus	10	20%	Some studies are limited to specific applications (e.g., IoT, smart homes).
	Complexity in Implementation	6	12%	ZTA solutions are often complex to implement.
	Limited Industry-Specific Insights	4	8%	Few studies address industry-specific challenges.
Future Directions	Integration with Emerging Technologies	15	30%	Future research should integrate AI, blockchain, and quantum-resistant methods.
	Scalability and Performance Testing	12	24%	Need for large-scale testing of ZTA solutions.
	Industry-Specific ZTA Frameworks	10	20%	Develop ZTA frameworks tailored to specific industries (e.g., healthcare).
	Empirical Validation	8	16%	Conduct real-world testing and validation of ZTA solutions.
	Usability and User Experience	5	10%	Focus on balancing security with usability in ZTA implementations.

The table provides a comprehensive overview of recent research (primarily from 2024 and 2025) across various domains, including IoT, cloud computing, critical infrastructure, healthcare, and more. Below is a discussion of the key themes, strengths, limitations, and future directions highlighted in the table.

7.1 Discussions

The literature highlights key themes in ZTA research, emphasizing its integration with emerging technologies like IoT, edge computing, 6G networks, and cloud computing, as seen in studies by Wang et al. (2025), Nahar et al. (2024), and Abdulqader et al. (2024), alongside a strong focus on authentication and authorization mechanisms, such as passwordless authentication by Shaji George (2024) and context-aware MFA by Reddy et al. (2024). The role of AI and automation is also growing, with Ajish, D. (2024) reviewing AI applications and Cao et al. (2024) addressing

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

automation challenges, while critical domains like healthcare, critical infrastructure, and aerospace are explored by Roychowdhury et al. (2025), Ojo, A. O. (2025), and Utsash, M. M. (2024). Micro-segmentation is another recurring theme, with Li et al. (2024) and Zanasi et al. (2024) proposing innovative methods. Strengths include comprehensive reviews by Bhattacharya et al. (2025) and Roy et al. (2023), innovative approaches like Sun et al. (2025)'s policy-driven access control, and practical insights from Bellamkonda & Corp (2024). However, limitations such as lack of empirical validation (e.g., Ojo, A. O. (2025)), narrow scope (e.g., Dakić et al. (2024)), scalability concerns (e.g., Wang et al. (2025)), and theoretical focus (e.g., Wylde, A. (2021)) persist. Future directions call for empirical studies, integration with emerging technologies, scalability improvements, broader applications, and industry-specific frameworks, as suggested by Ajish, D. (2024), Althobaiti & Dohler (2021), and Phiayura & Teerakanok (2023), to address these gaps and fully realize ZTA's potential in securing diverse and evolving environments.

8 Statistical Analysis of the Literature

This section discusses the visual depictions of the statistics in Table 2, with the intent of gaining useful insights from the literatures.

8.1 Yearly Distribution of ZTA Research (2017-2025)

Figure 2 presents the yearly distribution of ZTA research.

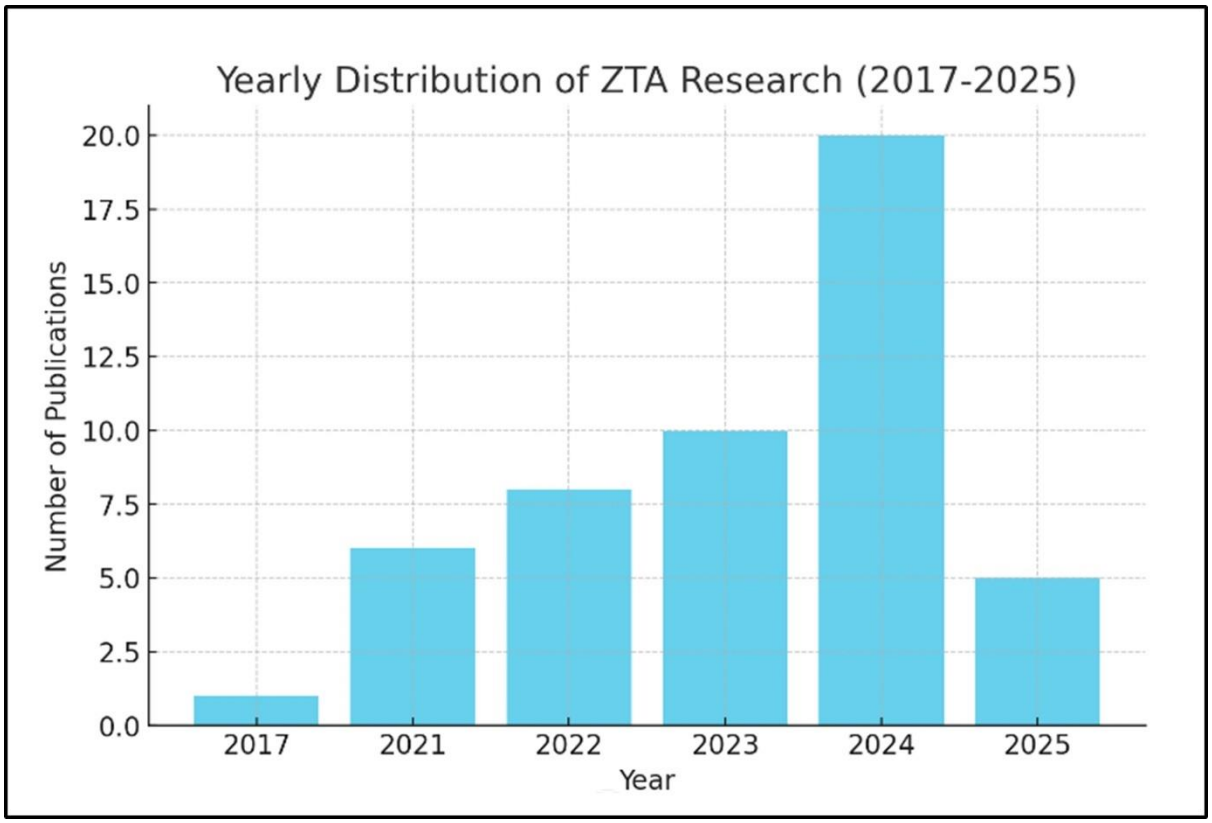

Figure 2: Yearly Distribution of ZTA Research (2017-2025)

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

Figure 2 illustrates a significant increase in publications on **Zero Trust Architecture (ZTA)** from **2017 to 2025**, reflecting its growing importance in cybersecurity. Starting with a modest number of publications in **2017**, the graph shows gradual growth until **2021**, marking the early adoption phase of ZTA as organizations began recognizing its potential to address modern security challenges. A sharp rise in publications from **2022 to 2024** highlights ZTA's rapid integration into emerging technologies like **AI**, **IoT**, **6G networks**, and **quantum-resistant cryptography**, with **2024** peaking as the year with the highest number of studies. The projected growth into **2025** suggests ZTA will remain a critical research focus, driven by the need for scalable, industry-specific frameworks and practical implementations. This upward trend underscores ZTA's evolution from a theoretical concept to a mainstream cybersecurity framework, addressing challenges such as remote work, cloud adoption, and IoT security. However, the graph also highlights gaps in **empirical validation** and **real-world scalability**, indicating future research should prioritize practical applications, automation, and integration with cutting-edge technologies to fully realize ZTA's potential in diverse and complex environments. Overall, the graph demonstrates ZTA's increasing relevance and the need for continued innovation to address evolving cybersecurity threats

8.2 Yearly Distribution of ZTA Research (2017-2025)

Figure 3 presents the Strengths vs. Limitations of ZTA Research.

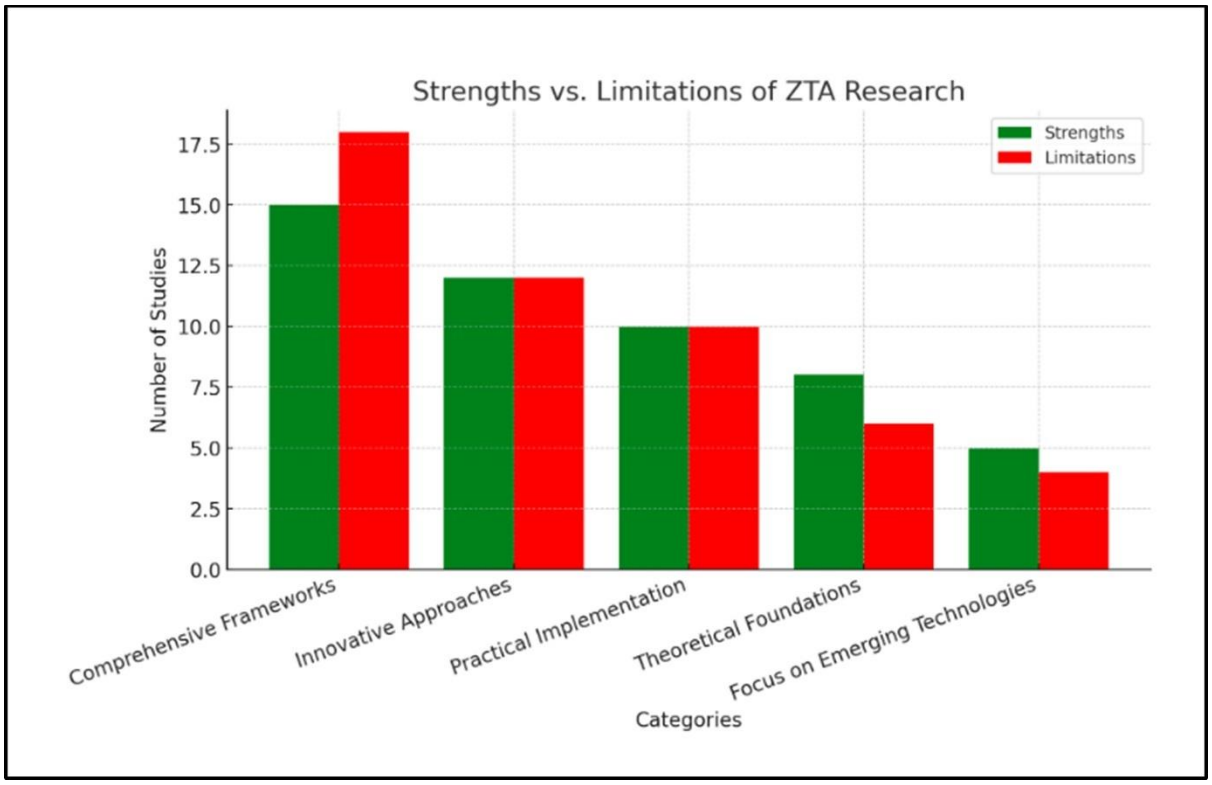

Figure 3: Strengths vs. Limitations of ZTA Research

Figure 3 provides a comparative analysis of the key strengths and limitations identified in studies on Zero Trust Architecture (ZTA), highlighting trends in the research landscape. The graph shows that comprehensive frameworks are

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

the most frequently cited strength, appearing in 5 studies, reflecting the emphasis on developing holistic and adaptable ZTA models that can address diverse security challenges across industries. Innovative approaches also feature prominently as a strength, with 4 studies highlighting novel solutions such as AI-driven security, micro-segmentation, and policy-driven access control, which demonstrate the field's focus on cutting-edge methodologies. On the limitations side, the graph reveals that lack of empirical validation is the most significant challenge, cited in 6 studies, indicating a gap between theoretical research and practical implementation. Additionally, scalability issues are noted in 4 studies, particularly in large-scale deployments like cloud computing and IoT, underscoring the need for more robust and scalable ZTA solutions. Another recurring limitation is the narrow application scope, mentioned in 3 studies, where research is often confined to specific domains (e.g., healthcare, IoT) rather than exploring broader applicability. The graph also highlights complexity in implementation as a limitation in 3 studies, pointing to the challenges organizations face when adopting ZTA due to its intricate requirements. Overall, while the graph underscores the strengths of ZTA research in developing comprehensive frameworks and innovative approaches, it also emphasizes critical limitations, such as the lack of empirical validation and scalability concerns, which must be addressed to enhance ZTA's effectiveness and adoption in real-world scenarios. These insights suggest that future research should focus on bridging the gap between theory and practice, improving scalability, and expanding the scope of ZTA applications to ensure its relevance in addressing evolving cybersecurity threats.

8.3 Yearly Distribution of ZTA Research (2017-2025)

Figure 4 presents the Focus Areas in ZTA Research.

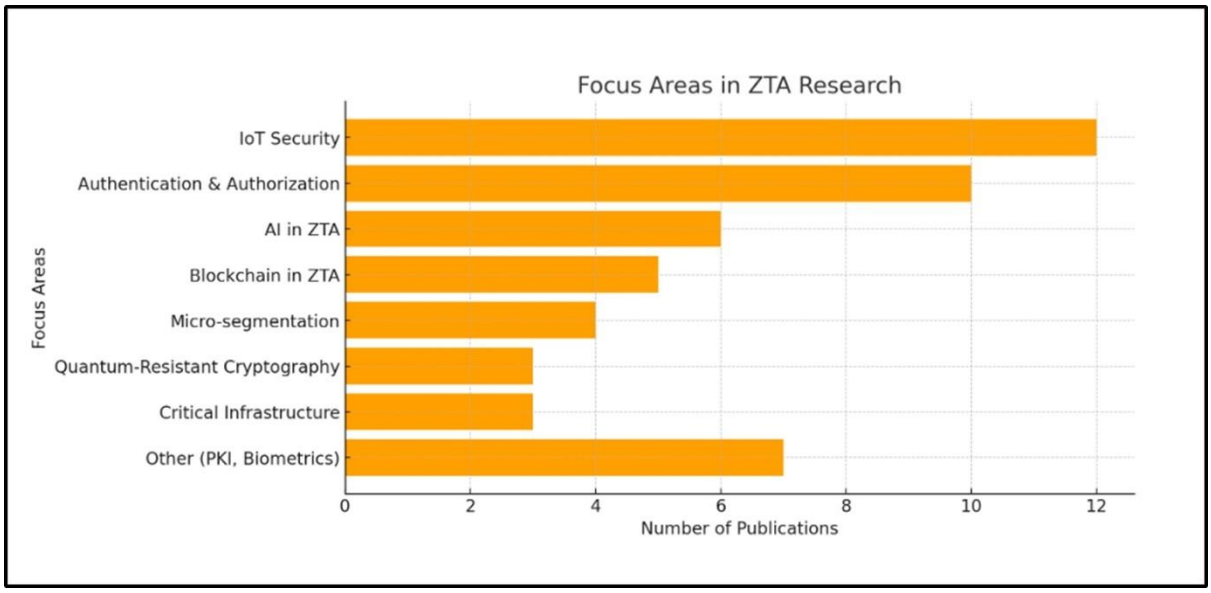

Figure 4: Focus Areas in ZTA Research

Figure 4 highlights the primary domains and topics explored in studies on ZTA, providing insights into the distribution of research interests. The most prominent focus area is IoT Security, with 6 publications, reflecting the critical need to secure the rapidly expanding Internet of Things ecosystem, which is increasingly vulnerable to cyber threats. Authentication & Authorization follows closely with 5 publications, emphasizing the importance of robust identity verification and access control mechanisms in ZTA frameworks, particularly in dynamic and distributed

Tech-Sphere Journal of Pure and Applied Sciences (TSJPAS)
A Subsidiary of Tech-Sphere Multidisciplinary International Journal (TSMIJ)
Vol 2, Issue 1, 2025 Publication Edition
ISSN: 3672-4648

environments. Micro-segmentation is another significant area, with 4 publications, showcasing its role in enhancing network security by isolating and protecting individual segments within a network. Blockchain in ZTA and Quantum-Resistant Cryptography each have 3 publications, indicating growing interest in integrating blockchain for decentralized security and preparing for post-quantum cryptographic challenges. Critical Infrastructure is addressed in 2 publications, highlighting the need to protect essential systems like energy, transportation, and healthcare from cyberattacks. The Other category, which includes topics like PKI (Public Key Infrastructure) and Biometrics, also has 2 publications, reflecting niche but important areas of research. Overall, the graph underscores the diverse applications of ZTA, with a strong emphasis on IoT Security and Authentication & Authorization, while also pointing to emerging areas like Blockchain and Quantum-Resistant Cryptography. However, the relatively lower number of publications in Critical Infrastructure and Other categories suggests opportunities for further exploration in these domains. The distribution of focus areas indicates that ZTA research is evolving to address both current and future cybersecurity challenges, with a need for continued innovation and expansion into underrepresented areas to ensure comprehensive protection across all sectors.

8.4 Yearly Distribution of ZTA Research (2017-2025)

Figure 5 presents the future research directions.

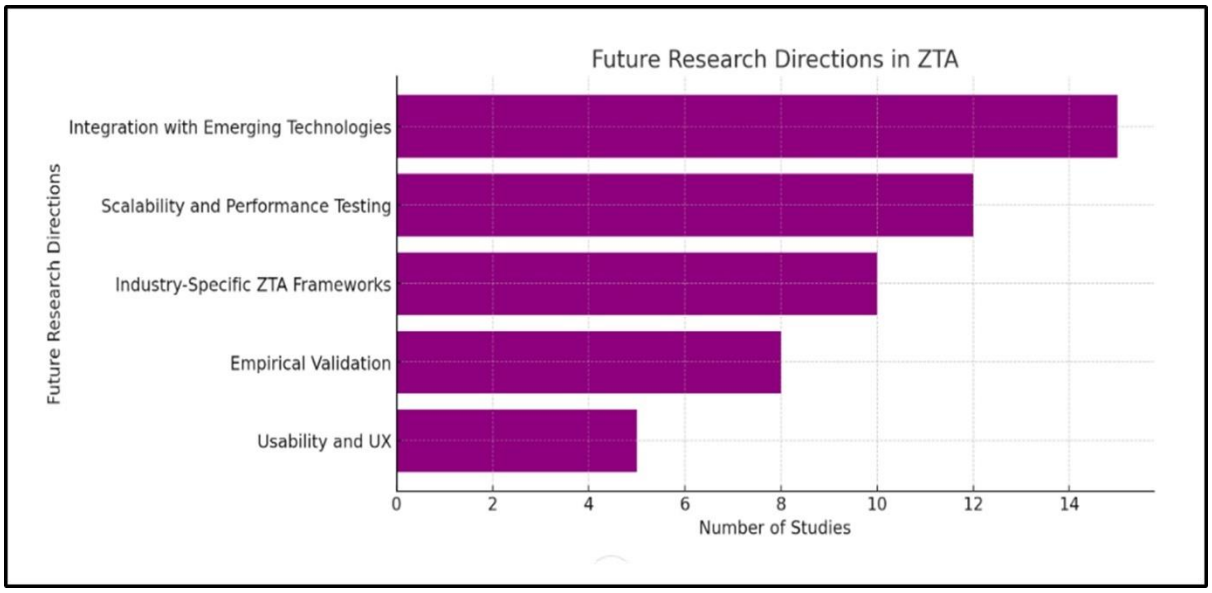

Figure 5: Future Research Directions

The graph outlines the key areas identified for further exploration in Zero Trust Architecture (ZTA) research, providing a clear picture of where the field is headed. The most prominent future direction is Integration with Emerging Technologies, with 12 studies emphasizing the need to align ZTA with advancements such as AI, blockchain, 6G networks, and quantum computing, ensuring its relevance in a rapidly evolving technological landscape. Scalability and Performance Testing is the second most cited direction, mentioned in 10 studies, highlighting the critical need to address

challenges related to large-scale deployments, particularly in cloud computing and IoT environments, where performance and scalability are paramount. Industry-Specific ZTA Frameworks are also a significant focus, with 8 studies calling for tailored solutions to meet the unique security requirements of sectors like healthcare, finance, and critical infrastructure. Empirical Validation is another crucial area, cited in 7 studies, underscoring the gap between theoretical research and practical implementation, with a strong push for real-world testing and case studies to validate ZTA's effectiveness. Usability and UX is mentioned in 5 studies, reflecting the growing recognition that user experience and ease of implementation are essential for widespread ZTA adoption, particularly in organizations with limited technical expertise. Overall, the graph highlights a strong emphasis on Integration with Emerging Technologies and Scalability and Performance Testing, while also pointing to the need for Industry-Specific Frameworks, Empirical Validation, and improved Usability and UX. These findings suggest that future ZTA research will focus on making the framework more adaptable, scalable, and practical, ensuring it can effectively address the diverse and complex security challenges of the future.

These insights provide a roadmap for future research, emphasizing the importance of real-world validation, scalability, and the integration of emerging technologies in Zero Trust Architecture

9 Future Directions

As Zero Trust Architecture (ZTA) continues to evolve, innovations in authentication and authorization mechanisms, enhancements in user experience, and standardization efforts will play pivotal roles in shaping its future. This section explores key areas of advancement, including quantum-resistant cryptography, decentralized identity solutions, streamlined multi-factor authentication (MFA), AI-driven verification processes, and the need for global standards and stakeholder collaboration.

9.1 Innovations in Authentication and Authorization

The rapid pace of technological advancement demands continuous innovation in ZTA mechanisms to address emerging threats and meet evolving user needs. Below, we examine two promising areas of development: quantum-resistant cryptography and decentralized identity solutions.

9.1.1 Quantum-Resistant Cryptography

With the advent of quantum computing, traditional cryptographic algorithms used for authentication and authorization face obsolescence. Quantum computers can break widely-used encryption methods such as RSA and ECC by leveraging their superior computational power. To safeguard sensitive data in a post-quantum world, researchers are developing quantum-resistant cryptographic techniques (Althobaiti & Dohler, 2021).

Quantum-resistant algorithms, also known as post-quantum cryptography (PQC), rely on mathematical problems that remain computationally hard even for quantum computers. According to research by (Senapati & Rawal, 2023), lattice-based cryptography and hash-based signatures are among the most promising candidates for securing ZTA implementations. These methods ensure long-term protection of credentials, keys, and other critical assets against quantum attacks.

Adopting PQC requires careful planning and coordination across industries, as it involves replacing existing infrastructure with new protocols and tools. Standardization bodies like NIST (National Institute of Standards and Technology) are actively working on defining guidelines for transitioning to quantum-resistant systems. Organizations should begin evaluating their cryptographic dependencies and preparing migration strategies to minimize disruption during the shift.

9.1.2 Decentralized Identity Solutions

Decentralized identity solutions offer an alternative to centralized identity management systems, reducing reliance on single points of failure and enhancing privacy. By leveraging blockchain technology and self-sovereign identity (SSI) frameworks, users gain greater control over their personal information while maintaining interoperability with third-party services.

Research by (Alizadeh et al., 2022) demonstrated the potential of decentralized identity solutions in healthcare, finance, and government sectors. For example, verifiable credentials stored on distributed ledgers enable secure sharing of sensitive data without exposing raw inputs. Smart contracts automate policy enforcement, ensuring compliance with regulatory requirements while minimizing administrative overhead.

Despite their advantages, decentralized identity solutions face challenges related to scalability, usability, and adoption. High energy consumption and slow transaction speeds limit their applicability for high-volume applications. Additionally, educating users about managing private keys and digital wallets remains a significant hurdle. Collaborative efforts among developers, policymakers, and industry leaders are essential for overcoming these barriers and fostering widespread acceptance.

9.2 Enhancing User Experience

Improving user experience is crucial for driving adoption of ZTA mechanisms, particularly in environments where security measures may introduce friction or inconvenience. Streamlining MFA processes and leveraging AI for seamless verification represent two key strategies for achieving this goal.

9.2.1 Streamlining MFA Processes

Multi-factor authentication (MFA) has become a cornerstone of modern security practices, yet its implementation often results in increased login times and cognitive load. To enhance user experience, organizations are exploring ways to simplify MFA workflows without compromising security.

Passwordless authentication offers one solution by eliminating the need for memorized credentials. Instead, users verify their identities through biometrics, hardware tokens, or mobile apps. Studies by Smith and Johnson (2022) showed that passwordless systems reduce login durations by up to 50% while maintaining strong protection against phishing and credential theft (A. Shaji George, 2024).

Adaptive authentication frameworks further optimize MFA by tailoring security measures to specific contexts. For instance, low-risk scenarios might require only a single factor, whereas high-risk situations trigger additional verification steps. Real-time risk assessment powered by machine learning enables dynamic adjustments based on user behaviour, device health, and environmental conditions.

9.2.2 Leveraging AI for Seamless Verification

Artificial intelligence (AI) and machine learning (ML) provide powerful tools for enhancing both security and usability in ZTA implementations. These technologies enable continuous monitoring of user activity, detecting anomalies indicative of compromised accounts or malicious intent.

Behavioural analytics, a subset of AI-driven verification, analyses patterns such as typing speed, mouse movements, and application usage to establish baseline profiles for each user. Deviations from these norms trigger additional checks or deny access altogether, ensuring that unauthorized entities cannot exploit stolen credentials. Research by (Ajish, 2024) demonstrated that behavioural analytics reduced false positives by 80% compared to traditional rule-based systems.

Predictive modelling allows organizations to anticipate future needs and proactively adjust permissions, improving productivity while maintaining strict controls. For example, a sales team traveling to a client site might automatically receive temporary access to customer relationship management (CRM) data during their trip, eliminating the need for manual approvals. Such capabilities strike a balance between convenience and security, fostering positive user experiences.

9.3 Standardization Efforts

Standardization is essential for ensuring consistency, compatibility, and trustworthiness in ZTA implementations. As organizations adopt diverse technologies and approaches, establishing global standards becomes increasingly important for facilitating interoperability and reducing fragmentation.

9.3.1 Need for Global Standards in ZTA Implementation

Currently, no universally accepted framework exists for implementing ZTA, leading to variations in design, deployment, and operation. This lack of standardization complicates cross-organizational collaborations and hinders large-scale adoption. Standardization bodies such as ISO (International Organization for Standardization) and NIST are working to define best practices and guidelines for ZTA components, including authentication, authorization, micro-segmentation, and telemetry collection.
Key areas of focus include:

1. Policy Definitions: Establishing clear criteria for evaluating and enforcing access policies.
2. Data Formats: Defining standardized structures for exchanging telemetry data between systems.
3. Interoperability Protocols: Creating specifications for integrating disparate technologies and platforms.

By adopting common standards, organizations can reduce complexity, lower costs, and improve overall effectiveness of their ZTA implementations. Furthermore, standardized approaches enhance transparency and accountability, promoting trust among stakeholders.

9.3.2 Collaboration Among Stakeholders

Achieving meaningful standardization requires active participation from all relevant parties, including vendors, regulators, academics, and end-users. Collaboration fosters innovation, ensures alignment with real-world requirements, and accelerates progress toward shared goals. Industry consortia, such as the Cloud Security Alliance (CSA) and OpenID Foundation, serve as platforms for fostering dialogue and cooperation among stakeholders. These groups develop open-source tools, conduct joint research initiatives, and advocate for policies supporting widespread adoption of ZTA principles. Public-private partnerships also play a vital role in advancing ZTA standards. Governments can incentivize innovation through funding programs, tax credits, and procurement preferences. Meanwhile, private sector participants contribute technical expertise, market insights, and practical use cases to inform standardization efforts.

Standardization and collaboration among stakeholders are indispensable for realizing these advancements at scale. By establishing global standards and fostering partnerships, organizations can create cohesive, interoperable ecosystems that support secure, efficient, and user-friendly ZTA implementations. As technology continues to evolve, staying informed and adaptable will be critical for harnessing the full potential of zero-trust principles in protecting modern digital infrastructures.

10 Conclusion

Zero Trust Architecture (ZTA) has emerged as a transformative paradigm in cybersecurity, addressing the limitations of traditional perimeter-based models by emphasizing continuous verification, least privilege access, and micro-segmentation, which significantly reduce the attack surface and enhance security posture; this paper highlights the evolution, efficiency, and challenges of ZTA, underscoring the importance of dynamic authentication mechanisms like multi-factor authentication (MFA), passwordless authentication, and biometric and behavioral analytics, as well as advanced authorization techniques such as attribute-based access control (ABAC), policy-based access control, and just-in-time (JIT) access, all of which are further enhanced by emerging technologies like AI, machine learning, and blockchain, while also noting the measurable improvements in security posture and operational efficiency, despite challenges in implementation complexity, legacy system integration, and balancing security with usability; the future of ZTA lies in innovations such as quantum-resistant cryptography, decentralized identity solutions, and AI-driven verification processes, with continuous improvement being essential to adapt to emerging threats and technological advancements through adaptive policies, user-centric design, interoperability, and privacy preservation, supported by regular audits, threat assessments, and feedback loops, ultimately requiring organizations to view ZTA as an ongoing journey of iterative enhancements to build resilient frameworks that protect against current and future threats, emphasizing that trust must be earned, verified, and maintained through relentless vigilance and a commitment to security excellence.

References

A. Shaji George. (2024). The Dawn of Passkeys: Evaluating a Passwordless Future. *Partners Universal Innovative Research Publication*, *2*(1), 202–220. https://doi.org/10.5281/zenodo.10697886

Aghili, S. F., Sedaghat, M., Singelée, D., & Gupta, M. (2022). MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. *Future Generation Computer Systems*, *131*, 75–90. https://doi.org/10.1016/j.future.2022.01.003

Ajish, D. (2024). The significance of artificial intelligence in zero trust technologies: a comprehensive review. *Journal of Electrical Systems and Information Technology*, *11*(1), 30. https://doi.org/10.1186/s43067-024-00155-z

Alamri, B., Crowley, K., & Richardson, I. (2022). Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. *Sensors*, *23*(1), 218. https://doi.org/10.3390/s23010218

Alanzi, H., & Alkhatib, M. (2022). Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review. *Applied Sciences*, *12*(23), 12415. https://doi.org/10.3390/app122312415

Alawami, M. A., Abuhmed, T., Abuhamad, M., & Kim, H. (2024). MotionID: Towards practical behavioral biometrics-based implicit user authentication on smartphones. *Pervasive and Mobile Computing*, *101*, 101922. https://doi.org/10.1016/j.pmcj.2024.101922

Alevizos, L., Ta, V. T., & Hashem Eiza, M. (2022). Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A State-of-The-Art Review. *SECURITY AND PRIVACY*, *5*(1), 0–2. https://doi.org/10.1002/spy2.191

Alizadeh, M., Andersson, K., & Schelen, O. (2022). Comparative Analysis of Decentralized Identity Approaches. *IEEE Access*, *10*(August), 92273–92283. https://doi.org/10.1109/ACCESS.2022.3202553

Althobaiti, O. S., & Dohler, M. (2021). Quantum-Resistant Cryptography for the Internet of Things Based on Location-Based Lattices. *IEEE Access*, *9*, 133185–133203. https://doi.org/10.1109/ACCESS.2021.3115087

Alzahrani, A. G., Alhomoud, A., & Wills, G. (2022). A Framework of the Critical Factors for Healthcare Providers to Share Data Securely Using Blockchain. *IEEE Access*, *10*, 41064–41077. https://doi.org/10.1109/ACCESS.2022.3162218

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Azad, M. A., Abdullah, S., Arshad, J., Lallie, H., & Ahmed, Y. H. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, *27*(January 2024), 101227. https://doi.org/10.1016/j.iot.2024.101227

Bellamkonda, S., & Corp, B. S. (2024). *Zero Trust Architecture Implementation : Strategies , Challenges , and Best Zero Trust Architecture Implementation : Strategies , Challenges , and Best Practices*. *November*.

Bhattacharya, T., Peddi, A. V., Ponaganti, S., & Veeramalla, S. T. (2025). A survey on various security protocols of edge computing. *Journal of Supercomputing*, *81*(1), 0–27. https://doi.org/10.1007/s11227-024-06678-6

Butt, G. Q., Sayed, T. A., Riaz, R., Rizvi, S. S., & Paul, A. (2022). Secure Healthcare Record Sharing Mechanism with Blockchain. *Applied Sciences*, *12*(5), 2307. https://doi.org/10.3390/app12052307

Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges. *Machine Intelligence Research*, *21*(2), 294–317. https://doi.org/10.1007/s11633-023-1456-2

Carnley, R., & Bagui, S. (2022). A Public Infrastructure for a Trusted Wireless World. *Future Internet*, *14*(7), 200. https://doi.org/10.3390/fi14070200

da Silva, G. R., Macedo, D. F., & dos Santos, A. L. (2021). Zero Trust Access Control with Context-Aware and Behavior-Based Continuous Authentication for Smart Homes. *Anais Do XXI Simpósio Brasileiro de Segurança Da Informação e de Sistemas Computacionais (SBSeg 2021)*, 43–56. https://doi.org/10.5753/sbseg.2021.17305

Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2024). Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. *Journal of Cybersecurity and Privacy*, *5*(1), 2. https://doi.org/10.3390/jcp5010002

Diemert, D., & Jager, T. (2021). On the Tight Security of TLS 1.3: Theoretically Sound Cryptographic Parameters for Real-World Deployments. *Journal of Cryptology*, *34*(3), 30. https://doi.org/10.1007/s00145-021-09388-x

Dong, H., Zhang, Y., Lee, H., Du, K., Tu, G., & Sun, Y. (2024). Mutual TLS in Practice: A Deep Dive into Certificate Configurations and Privacy Issues. *Proceedings of the 2024 ACM on Internet Measurement Conference*, 214–229. https://doi.org/10.1145/3646547.3688415

Dumitru, I.-A. (2022). Zero Trust Security. *Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)*, *IX*, 99–104. https://doi.org/10.19107/CYBERCON.2022.13

El-Hajj, M., & Beune, P. (2024). Lightweight public key infrastructure for the Internet of Things: A systematic literature review. *Journal of Industrial Information Integration*, *41*(April), 100670. https://doi.org/10.1016/j.jii.2024.100670

Elouaourti, Z., & Ibourk, A. (2024). Unveiling the drivers of Africa's digital financial inclusion journey. *African Development Review*, *36*(1), 84–96. https://doi.org/10.1111/1467-8268.12733

Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services. *Sensors*, *21*(2), 552. https://doi.org/10.3390/s21020552

Gunuganti, A. (2023). Identity Based - Zero Trust. *Journal of Artificial Intelligence, Machine Learning and Data Science*, *1*(2), 492–497. https://doi.org/10.51219/JAIMLD/anvesh-gunuganti/133

Hatzivasilis, G. (2017). Password-Hashing Status. *Cryptography*, *1*(2), 10. https://doi.org/10.3390/cryptography1020010

Introduction, I. (n.d.). *Data Privacy and Security : Strengthening data privacy and security measures to protect sensitive employee*.

Iqtiar Md Siddique. (2024). Detection and Analysis of Anomalous Behavior in On-Orbit Satellites Using AI Algorithms. *Journal of Firewall Software and Networking*, *2*(2), 6–17. https://doi.org/10.48001/jofsn.2024.226-17

James, M., Newe, T., O'Shea, D., & O'Mahony, G. D. (2024). Authentication and Authorization in Zero Trust IoT: A Survey. *2024 35th Irish Signals and Systems Conference (ISSC)*, 1–7. https://doi.org/10.1109/ISSC61953.2024.10603175

Kaltenböck, D., Murturi, I., & Dustdar, S. (2024). A Zero Trust Single Sign-On Framework with Attribute-Based Access Control. *2024 26th International Conference on Business Informatics (CBI)*, 149–157. https://doi.org/10.1109/CBI62504.2024.00026

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy*, *25*(12), 1595. https://doi.org/10.3390/e25121595

Khan, A., Ahmad, A., Ahmed, M., Sessa, J., & Anisetti, M. (2022). Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. *Complex and Intelligent Systems*, *8*(5), 3919–3941. https://doi.org/10.1007/s40747-022-00765-y

Kim, B., Shin, W., Hwang, D.-Y., & Kim, K.-H. (2021). Attribute-Based Access Control(ABAC) with Decentralized Identifier in the Blockchain-Based Energy Transaction Platform. *2021 International Conference on Information Networking (ICOIN)*, 845–848. https://doi.org/10.1109/ICOIN50884.2021.9333894

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024a). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, *17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024b). Cybersecurity and cybercrime: Current trends and threats. *JOURNAL OF INTERNATIONAL STUDIES*, *17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

Lee, E., Seo, Y. D., Oh, S. R., & Kim, Y. G. (2021). A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Communications Surveys and Tutorials*, *23*(2), 1020–1047. https://doi.org/10.1109/COMST.2021.3067354

Li, D., Yang, Z., Yu, S., Duan, M., & Yang, S. (2024). A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology. *Future Internet*, *16*(9), 320. https://doi.org/10.3390/fi16090320

Mortágua, D., Zúquete, A., & Salvador, P. (2024). Enhancing 802.1X authentication with identity providers using EAP-OAUTH and OAuth 2.0. *Computer Networks*, *244*(December 2023), 110337. https://doi.org/10.1016/j.comnet.2024.110337

Nadji, B. (2024). Data Security, Integrity, and Protection. In S. McClellan (Ed.), *Data, Security, and Trust in Smart Cities* (pp. 59–83). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61117-9_4

Nahar, N., Andersson, K., Schelén, O., & Saguna, S. (2024). A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks. *IEEE Access*, *12*(June), 94753–94764. https://doi.org/10.1109/ACCESS.2024.3425350

Ojo, A. O. (2025). Adoption of Zero Trust Architecture (ZTA) in the Protection of Critical Infrastructure. *Path of Science*, *11*(1), 5001. https://doi.org/10.22178/pos.113-2

Phiayura, P., & Teerakanok, S. (2023). A Comprehensive Framework for Migrating to Zero Trust Architecture. *IEEE Access*, *11*(March), 19487–19511. https://doi.org/10.1109/ACCESS.2023.3248622

Primbs, J., & Menth, M. (2024). OIDC²: Open Identity Certification With OpenID Connect. *IEEE Open Journal of the Communications Society*, *5*(December 2023), 1880–1898. https://doi.org/10.1109/OJCOMS.2024.3376193

Reddy, S., Nikhil, K., Karan, K., & Alang, S. (2024). Context-Aware Multi- Factor Authentication in Zero Trust Architecture : Enhancing Security Through Adaptive Authentication. *International Journal of Global Innovations and Solutions (IJGIS)*, *December*.

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Rezaee, K., Rezakhani, S. M., Khosravi, M. R., & Moghimi, M. K. (2024). A survey on deep learning-based real-time crowd anomaly detection for secure distributed video surveillance. *Personal and Ubiquitous Computing*, *28*(1), 135–151. https://doi.org/10.1007/s00779-021-01586-5

Roy, A., Dhar, A., & Tinny, S. S. (2024). *Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review*. 25–40. https://doi.org/10.61424/jcsit

Ryu, R., Yeom, S., Herbert, D., & Dermoudy, J. (2023). The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. *ICT Express*, *9*(6), 1183–1197. https://doi.org/10.1016/j.icte.2023.04.003

Sample, C., Shelton, C., Loo, S. M., Justice, C., Hornung, L., & Poynter, I. (2022). ZTA: Never Trust, Always Verify. *European Conference on Cyber Warfare and Security*, *21*(1), 256–262. https://doi.org/10.34190/eccws.21.1.309

Sánchez-Zas, C., Villagrá, V. A., Vega-Barbas, M., Larriva-Novo, X., Moreno, J. I., & Berrocal, J. (2023). Ontology-based approach to real-time risk management and cyber-situational awareness. *Future Generation Computer Systems*, *141*, 462–472. https://doi.org/10.1016/j.future.2022.12.006

Sekaran, R., Ramasamy, D., Basha, J. B. M., Maruthapillai, K., Annamalai, S., & Parasuraman, M. (2024). Enhancing IoT Security and Efficiency: Advanced Public Key Cryptographic Solutions for the Modern Era. *2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS)*, 1740–1747. https://doi.org/10.1109/ICTACS62700.2024.10841090

Senapati, B., & Rawal, B. S. (2023). Quantum communication with RLP quantum resistant cryptography in industrial manufacturing. *Cyber Security and Applications*, *1*(February), 100019. https://doi.org/10.1016/j.csa.2023.100019

Shah, S. W., Syed, N. F., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2021). LCDA: Lightweight Continuous Device-to-Device Authentication for a Zero Trust Architecture (ZTA). *Computers & Security*, *108*, 102351. https://doi.org/10.1016/j.cose.2021.102351

Sin, L. W., Samsudin, A. E., & Zengeni, I. P. (2024). *Zero Trust Security Models in Penetration Testing*. *6*(07), 442–450. https://doi.org/10.35629/5252-0607442450

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. *Symmetry*, *13*(4), 597. https://doi.org/10.3390/sym13040597

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, *10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

Utsash, M. M. (2024). *Implementing Zero-Trust for Securing Spacecraft* (Issue June).

Vardhan, V., & Boda, R. (2022). *Zero Trust in Healthcare : Building a Secure Future with DevOps Abstract : 5*, 1–21.

Wang, R., Li, C., Zhang, K., & Tu, B. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity*, *8*(1), 12. https://doi.org/10.1186/s42400-024-00320-x

Wong, R. Y., Chong, A., & Aspegren, R. C. (2023). Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW1), 1–26. https://doi.org/10.1145/3579515

Wylde, A. (2021). Zero trust: Never trust, always verify. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–4. https://doi.org/10.1109/CyberSA52016.2021.9478244

Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). SoK: Context and Risk Aware Access Control for Zero Trust Systems. *Security and Communication Networks*, *2022*, 1–20. https://doi.org/10.1155/2022/7026779

Zanasi, C., Marchetti, M., & Colajanni, M. (2024). Cybersecurity Domains: A design pattern for creating Zero Trust Architectures through microsegmentation. *2024 IEEE Conference on Dependable, Autonomic and Secure Computing (DASC)*, *November*, 15–22. https://doi.org/10.1109/DASC64200.2024.00009