International Journal of Modern Computer Science and IT Innovations (IJMCSIT)
eISSN: 3087-4289
Volume03 Issue07 | Page No: - 47-56

Received: 30 May 2026, Revised: 15 June 2026, Accepted: 26 June 2026, Published: 22 July 2026

DOI: https://doi.org/10.55640/ijmcsit-v03i07-05

Zero Trust Architecture in Modern Cybersecurity: A Review of Core Principles, Applications, And Research Directions

Dr. Pradeep Laxkar [1]

[1] Associate Professor, Department of Computer Science and Engineering, ITM(SLS) University, Vadodara, Gujarat, India

ABSTRACT: Cloud computing, Internet of Things (IoT) devices, remote working environments and distributed digital infrastructures have driven the evolution of the perimeter-based security model to its limits. To counter this, Zero Trust Architecture (ZTA) has become a contemporary cybersecurity paradigm based on the principle of "never trust, always verify," which would involve ongoing checks, authentication, and authorization of users, devices, and applications. The paper provides a summary and covers all the key points of the ZTA, such as its principles, logical structure, security models and implementation. The study applies some of the main concepts, such as least-privilege access, micro-segmentation, continuous verification, policy-based access control and real-time security analytics. Additionally, the paper covers the use of ZTA in different industries, including IoT, cloud computing, Secure Access Service Edge (SASE), and identity-centric security solutions. A comparative analysis of the research contributions in the recent years is conducted to assess the recent advances, issues, and barriers of ZTA adoption. The survey points out other areas for further research including lightweight cryptography, dynamic trust evaluation, automated orchestration, scalability, interoperability, regulatory compliance. The survey provides a detailed reference guide for researchers, practitioners and policymakers to grasp and apply the principles of ZTA in the modern cyber security environment.

KEYWORDS: Zero Trust Architecture (ZTA), Cybersecurity, Identity and Access Management, Internet of Things (IoT), Threat Intelligence, Cyber Resilience.

1. Introduction

The landscape of cyber has changed so much in the past 20 years that the cloud, the Internet of Things, and the digitization of critical infrastructure are all cited as examples of the complexity of digital ecosystems [1][2]. This new environment renders ineffective the traditional perimeter security strategy, which was founded on the idea that dangers may originate from beyond the network's boundary. These antiquated architectures still rely mostly on VPNs and firewalls as perimeter defences, but they aren't foolproof against APTs, lateral movement, or insider threats.

Zero Trust Architecture is an innovative approach to security. ZTA is distinct from perimeter-based approaches since it does not blindly trust any node, device, or application on the network [3]. Under ZTA, the guiding idea is "never trust, always verify," which means that all requests to access resources, regardless of who is making them, must undergo constant authentication, authorization, and validation procedures. The ZTA model strengthens the security posture as per NIST SP 800-207, by supporting and implementing the following: "least-privilege access," "micro-segmentation," and "real-time policy enforcement.

The rising of IoT systems brings cybersecurity a bit more complicated because IoT devices are typically poorly secured, used in insecure settings, and running on limited resources. The issues found here make perimeter-based defense approach unsuitable and are the reason why ZTA is relevant in IoT environments[4][5]. Limited encryption, a lack of continuous monitoring, and insufficient policy enforcement across remote nodes are some of the issues that have prompted suggestions for IoT-specific alterations to ZTA [6][7]. Several studies are suggested to apply score based access control, context-aware trust engines and ML systems to detect anomalies in the context of the improvement of security of IoT in a ZTA [8][9].

ZTA is also being used to address other use cases such as cloud computing, industrial control systems, healthcare, 5G/6G mobile networks, which provide

granular access control, no implicit trust, and enhance the security posture of dynamic and distributed systems. Many studies [10][11] highlight its adaptability and resilience, especially in integrating with the latest technologies, such as AI, blockchain, and federated learning, in cyber-physical environments. The introduction of ZTA is conceptually sound, but it is not easy to apply, because there are no standard frameworks, orchestration challenges, interoperability issues, and very extensive policy configuration requirements. Further research has shown that no current solutions adequately handle the five pillars of cyber defence: authentication, authorisation, access control, encryption, auditing, and environment perception.

A. Structure of Paper

This paper is organized as follows: The principles, logical components, and issues of implementation associated with ZTA are presented in Section II, which describes the basic concepts and foundations of ZTA. In Section III the Zero Trust Security Model, its applications in IoT security, core security principles are discussed. There are important techniques for implementing ZTA described in Section IV. Section V is a literature review that is thorough of recent research. Finally, section VI concludes with key findings, future research directions.

2. Zero Trust Architecture: Concepts and Foundations

Zero Trust Architecture (ZTA) is different from the old security model that was built on perimeters. ZTA doesn't think that people or things inside the network can always be trusted. Instead, it thinks that nothing can be trusted, inside or outside the organization. The main components of ZTA are policy enforcement points, continuous monitoring service, trust evaluation engines and protected resources, which are depicted in the conceptual model of ZTA as shown in Fig. 1. This visualization is to complement the theoretical discussion with a structure (modified from NIST SP 800-207). The use of lightweight cryptographic techniques (such as Elliptic Curve Cryptography, homomorphic encryption, and post-quantum approaches) to guarantee secure communications without compromising efficiency is becoming more popular as a means to address technical difficulties in environments with limited resources, such as IoT devices.

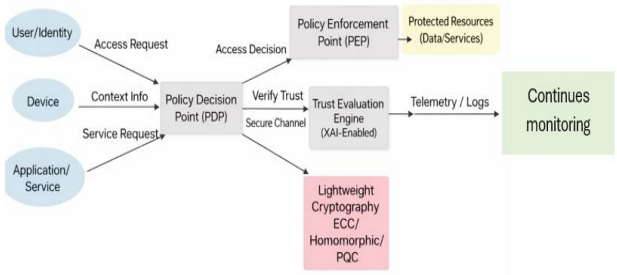

Fig. 1. Conceptual model of Zero Trust Architecture (ZTA) [12]

Traditionally, cybersecurity architectures worked by building trust with users or devices once they were behind perimeter security controls like VPNs or firewalls. The rise of cloud computing, byod (Bring Your Own Device) laws, remote workforces, and, most importantly, IoT devices has rendered the traditional barrier obsolete [13]. Attackers' lateral movement across infiltrated networks and APTs are examples of security incidents that affect the perimeter security method. No matter where you are, ZTA can access and enforce least-privilege access by segmenting on a per-session basis. This model naturally enhances the security against external attacks and insider attacks [14][15].

A. NIST ZTA Principles

The following seven principles of ZTA are outlined in NIST Special Publication 800-207, which serves as the foundational document for ZTA [16]:

- The term "resource" applies to any and all data and computer services.
- The location of the network has no bearing on the security of any transmission.
- Personalised materials can be accessed session by session.
- Decisions about access are made by dynamic policies using observable properties.
- The safety of all assets is being checked constantly.
- Complete identification prior to granting access.
- Environmental data collecting in real-time (adaptive decision-making).

The concepts lay the groundwork for developing and evaluating ZTA models across domains, particularly with the varied, widely dispersed, and vulnerable IoT devices. These are some of the core principles, with regulatory alignment becoming more vital. The legal acceptance and industrial significance of ZTA principles are enhanced when their scope is expanded to conform to compliance standards like as GDPR, HIPAA, and NHS DSP.

B. ZTA Logical Components

ZTA is made up of many services that have many logical parts and may be run either locally or in the cloud. The policy enforcement point (PEP), the policy administrator (PA), and the policy engine (PE) are three of these components that NIST considers core, as shown in Fig. 2.

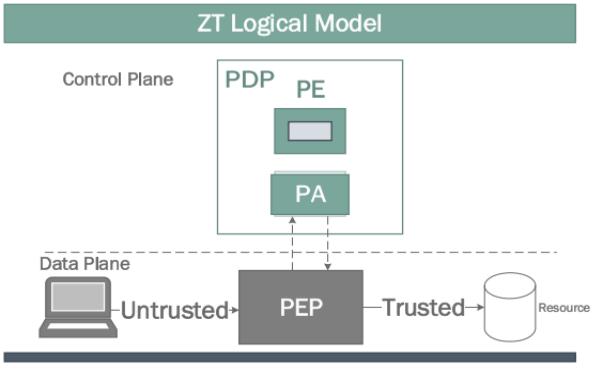

Fig. 2. Core logical components of ZT [17]

These three essential parts perform the following functions:

- The "brain" of the system is a trust algorithm, and the "legacy" is the PE, which takes data from outside sources and utilises it to guide access choices that adhere to company policy.

- Policy administrator (PA): The PA is subservient to the PE's decision on the matter of access. As part of its policy enforcement communications with the PEP, it is possible to include it into the PE.

- A user's connection to a resource can be established, maintained, and eventually severed by the PEP. The client (representing a device agent) and the resource (representing a gateway) are its two primary components. It is common practice for trust zones to go beyond the PEP.

SIEM, activity logs, data access restrictions, continuous diagnostics and mitigation, and identity management are among the other components. work in tandem with the aforementioned fundamental components to make zero trust security a reality.

C. Challenges of Zero-Trust

There is a wide range of difficulties that organisations face when they try to implement the Zero Trust paradigm, and these difficulties must be carefully considered and strategically addressed. There is no denying Zero Trust's worth, but overcoming these challenges is essential to the technology's widespread acceptance and maximum impact [18][19][20]. This section provides valuable insight into the numerous challenges associated with Zero Trust implementation and offers suggestions for completing the task. Shifting company culture is an integral part of implementing a Zero Trust approach. Zero Trust "always verify" and "least privilege" philosophies may create some tension between employees who are accustomed to a perimeter-based trust model.

1) Cultural Barriers and Organizational Resistance:

The shift to the traditional security model to Zero Trust requires a paradigm change in the organizations themselves. The concepts behind Zero Trust — continuous verification and “least privilege” — can be difficult for employees who are familiar with a perimeter-based trust model.

2) Technical Complexity and Integration

Deploying Zero Trust within an organisation can be challenging and expensive. Changing to the new system may introduce compatibility challenges among legacy systems, technologies, and platforms, necessitating careful planning and gradual transition to the new system.

3) Balancing Security and Usability

One of the biggest challenges in implementing Zero Trust is the security vs user experience trade-off. Users may become frustrated and the process may become inefficient due to the constant checks and controls. The solution to this problem is to create user-friendly interfaces and to refine the authentication process and workflow to ensure that user productivity is maximized while still maintaining the added security benefits.

4) Financial Considerations

Zero Trust technology, staffing and ongoing maintenance are all factors in the costs. Resources should be committed to security infrastructure enhancements, training and monitoring equipment. This demands a careful cost-benefit analysis and strategic allocation of resources, weighing the financial investments against the benefits, and risk mitigation.

5) Data Privacy and Regulatory Compliance

Data privacy must be aligned with rules and regulations and Zero Trust provides continuous verification and access controls. Fitting into data protection legislation, such as GDPR or HIPAA, is a fragile relationship between awareness of legal needs and robust security measures, including data governance practices.

6) Organizational Scalability

Zero trust strategies should be flexible enough to meet the organization's evolving demands. However, as the organization grows, it is essential to plan the architecture carefully and remain adaptable to evolving requirements

to ensure ZTA is effective and efficient [21].

3. Zero Trust Security Model

There is no implicit trust in the ZT security concept. Everything up until this point has the potential to be hostile, including people, gadgets, data transfers, and programs' inputs and outputs. Despite the phrase's widespread use in the IT sector, the concept that underpinned it could have existed long before the name was even invented. Solutions dealing with zero trust intrusion tolerant systems have been around since at least 2002, specifically for a ZT security model that uses that word. These solutions are based on the idea that compromise is inevitable [22][23]. The ZT model has since been popularized for application to network architectures, as described.

A. Internet of Things (IoT) Security

The expansion of the IoT ecosystem has made zero trust a must-have security measure for all linked devices. Zero Trust is a security framework that employs rigorous access controls and continuous device verification to lessen the possibility of assaults on the IoT [24]. A complete inventory of all networked IoT devices is required in order to implement a Zero Trust security architecture for IoT devices. Devices should be categorised in this inventory according to their nature, function, data sensitivity level, and other relevant criteria [25].

B. Secure Access Service Edge (SASE)

Organisations should let more employees to access their private networks over the employer's local Internet in order to accommodate the increasing demand for remote work. Because of this, it becomes more expensive to ensure that remote workers use approved devices and services to access company resources in a private and secure manner. Additional worry arises from the possibility of connection latency to the organization's private network while handling a large group of people. At the edge of the cloud, Organisations may streamline and reduce the cost of implementing their network plan with the help of Secure Access Service Edge, which consolidates several network utility and security roles [26].

C. Multi-Factor Authentication (MFA)

A new strategy for security is required due to the increase of complex assaults like as phishing, insider threats, and credential theft. This has prompted the development of a new paradigm in cybersecurity, the ZTA. The use of many authentication methods, known as MFA, is a key feature of ZTA that greatly improves security. A number of problems, including usability problems, weariness, and susceptibility to new threats, arise from the fact that most MFA systems are rigid and often hardcoded in the rules [27].

D. Core Principles

ZTA's interconnected principles and tenets boost security by doing away with implicit trust and replacing it with explicit verification. These vary somewhat depending on the source, but they share one thing in common – that there is no reliable resource, user, device or application. These principles are not just philosophical, but guidelines for design and implementation that would benefit a robust security infrastructure. This section outlines a number of these ground-breaking ideas:

1) Data Centric Security

The idea of ZTA places a premium on data protection. The importance of safeguarding data cannot be overstated, regardless of its origin or location. The first step in developing a data-centric security architecture is to catalogue all of the sensitive information and mission-critical applications [28]. Even if all other security procedures are foolproof, data still has to be labelled with characteristics like personally identifiable information (PII), other sensitive information, and a host of others to ensure sufficient protection. Additional benefits of data tagging during import and production include improved data categorization.

2) Principle of Least Privilege Access

This concept is important to ZT since it ensures that users and entities only have access to the resources, they actually need to complete their tasks. It says that a person or device should be granted permissions only to run the program and do the job. The idea of least privilege makes accounts less visible and less accessible, reducing the damage that can be done by an attacker to a network if it is compromised. All it means is that only the information and resources each user or device really needs are available.

3) Micro-segmentation

The ZTA solution creates smaller and more secure zones of the network that increase the security of the network. The technique creates isolated segments and gives them selective access restrictions to make it challenging to move threats within a network. Micro-segmentation is the design principle that limits workloads and applications from accessing the network broadly to limit attack surface and control the flow of network traffic within segments. It has the advantage over traditional perimeter protection because it locks attackers out of the network's sides rather than moving around in small steps.

4) Continuous Authentication and Authorisation

Each access request to ZTA is validated to determine the identity of both the user and the device. From all practical purposes, the processes of authentication and authorization should be continuous and thereby provide access to the authorized people and devices. Access requests were not only checked for credentials, but also checked for several topic variables such as identity, location, time, and device security posture. Continuous authentication reduces the risk of unauthorized use by giving access as needed based on the actual situation [1].

5) Policy-Based Access Controls

User identification, device posture, time, location, and data sensitivity are all factors that should be considered when granting access under ZTA's set policy. This allows businesses to comply with regulatory requirements or implement business requirements in terms of fine-grained and granular access control [29]. The rules could be based on a number of criteria and levels of resource sensitivity, including data, user, device, threat and legal considerations. Policies need to be correct, consistent, as brief as possible, and as comprehensive as possible.

6) Real-time Visibility and Analytics

ZTA emphasizes the need to closely monitor network traffic and user activities for any suspicious actions. This visibility in real-time is a prerequisite for security personnel to be able to respond if an attack occurs as the security issue becomes critical. Using ZTA, companies can enhance their security posture by identifying vulnerabilities and threats in the analysis of asset security data, network traffic, and access requests.

7) Automation and Orchestration

ZTA applies security controls rapidly and reliably through orchestration and automation. These are key to the complexity management of ZTA at scale [30]. Automation dynamically reconfigures security policies, simplifies access control and supplies end-to-end zerotrust enforcement.

8) Assume Breach

The number one rule of ZTA is that the breach has already taken place. The paradigm is not only on breach prevention but also containment and mitigation [5]. Security precautions have been taken to attempt to reduce the impact by blocking lateral movement or unwanted access to sensitive data. Fig. 3 below depicts the NIST Incident Response Cycle, which gives a thorough rundown of how to deal with security issues, beginning with preparedness and ending with analysis of what happened after the fact. A corporation can reliably detect, respond to, and recover from any security breach thanks to this iterative procedure.

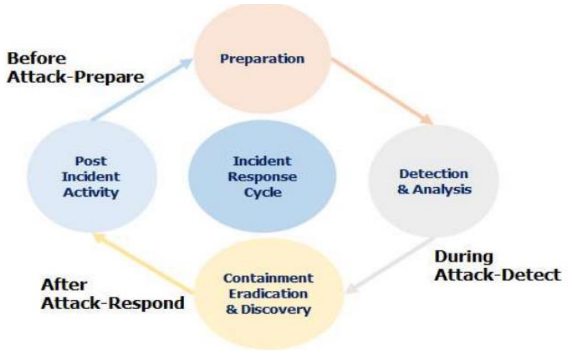

Fig. 3. NIST Incident Response Cycle[31]

The ZTA framework is more of a collection of rules for how a system or process should be designed than an actual architecture. Core values are consistent regardless of how an organization chooses to put them into practice. Further, understanding the present infrastructure and business processes is necessary for creating the necessary security rules and mapping the access flows.

4. ZTA Implementation Techniques

Several technologies and methods can be used by a company to apply ZTA. The policy rules that make up PE (Policy engine) are culled from many data sources, as mentioned above.

- Identity and Access management
- Application and Network Logs Gathered by SIEM
- Intelligence on Potential Dangers (a database of external and internal threats)
- Continuous Diagnostics and Mitigation (CDM)
- Compliance with a number of industry-set standards

The components and data sources that drive an organization's PE might also affect the final ZTA [32].

A. Identity management

The IoT has revolutionised digital communication, allowing users to instantly share data and engage in hands-free interactions regardless of their physical location. Devices, sensors, machine agents, and service accounts are examples of non-human identities that raise serious security problems, despite the fact that this transformation has many practical advantages. Protecting people's identities has always been the responsibility of perimeter security schemes. Internal actors' implicit confidence and strict trust limits are the foundation of these frameworks. There isn't much evidence to support non-human identities. Their shortcomings are driving a new security paradigm shift toward ZTA, which holds that "never trust, always verify" is the best policy's [33].

B. Network and Application logs collected through

SIEM

The ability for SIEM and ZT systems to communicate with one another is a game-changer in the world of cyber defence. Integrating SIEM's real-time monitoring and analytics with Zero Trust's stringent access constraints and ongoing verification principle.[34].

C. Threat Intelligence

The Internet has proliferated in such a way that it has opened up tremendous potential for benefits, but also resulted in several cyber security threats that have posed a significant risk to personal information, national security, and economic security.

D. Continuous Diagnostics and Mitigation

The Zero Trust (ZT) model of cybersecurity removes the concept of implicit trust, and continually re-authenticates every interaction in an organization. Zero Trust is meant to keep modern settings safe and allow for digital change by using strong authentication methods, dividing networks, stopping threats at Layer 7, and making "least access" rules easier to understand and apply. "Never trust, always verify" is what Zero Trust is all about. The ZTA's CDM program can be made better by adding a learning model to handle the ongoing evaluation and guess potential threats based on the past data [35].

E. Compliance to various industry defined standards

A Zero Trust Architecture is critical for ensuring that companies adhere to regulations. ZTA Audit Findings of Noncompliance and Time Spent on Compliance Reporting, for example, show how the tool helps businesses meet the standards of several security laws, such as PCI DSS, HIPAA, and the General Data Protection Regulation (GDPR). The real-time data that ZTA provides, along with its comprehensive recording and constant monitoring, makes compliance much easier to audit. It is possible to monitor the frequency with which businesses do not adhere to specific security requirements with the Audit Findings of Noncompliance metric [36].

5. Literature Review

This section provides a survey of previous work that has been done on a comparable subject and keywords that are relevant to it.

Soni et al. (2026) offers a comprehensive and multi-dimensional synthesis of ZTAs. It also examines the principles and implementation strategies of various ZTAs, comparing them using multiple parameters to highlight their strengths and weaknesses. In addition to the synthesis of ZTAs, the work demonstrates its practical value with sector-specific examples to make it more relevant for real-world applications. The study used detailed analysis to define research gaps and areas of existing research which need further investigation. Such findings can be used to inform future advances in digital security. The results are intended to assist organizations in identifying and implementing the most effective ZT strategies to improve the cybersecurity posture [37].

Pigola, Meirelles and Costa (2026) embraces the zero trust (ZT) paradigm, with trust being a structural asset that is continuously verified. It explores the importance of cultural alignment, financial readiness, compliance and operational upheaval, and the role that businesses play in building trust through security practices. There is growing interest in the ZT dimensions but they have not been explored at the enterprise level. The study is based on the principal–agent theory and the results of qualitative interviews, entropy-based MCDM, and PLS-SEM survey analysis, it is found that cultural and financial factors are the most important, then compliance, and operations. It offers a structure and a sequence of activities to enhance TM, resilience and regulatory alignment [38].

Mushtaq, Mohsin and Mushtaq (2025) The primary challenges are scalability issues, lack of lightweight cryptographic solutions for resource-limited environments, poor orchestration capabilities and lack of regulatory compliance with GDPR and HIPAA standards. In terms of cross-domain comparisons, enterprise and cloud installations are somewhat well-established, whereas the Internet of Things (IoT), blockchain, and big data deployments are still encountering performance and regulatory challenges. Lightweight cryptography, context-aware trust engines, automated orchestration, and regulatory integration are the four pillars upon which ZTA adoption rests, and the outcomes show both their success and their failure. Potentially useful for academics, practitioners, and legislators interested in strengthening cybersecurity resilience, this evaluation can serve as a roadmap for future ZTA studies and applications [12].

Gambo and Almulhem (2025) describes the evolution of ZTA over the years and some major trends in development and publications, in addition to speculating some of the reasons to be attributed for the increase in the last few years. It also provides examples of the effective application of ZTA principles for granular access control, system behavior monitoring and to simplify security administration in complex and distributed networks. It is a detailed research to provide a handbook for researchers and practitioners interested in using ZTA to build more resilient and adaptive security systems in this ever-changing threat environment [39].

Dhiman et al. (2024) offer valuable insights for

researchers, practitioners, and policymakers relevant to the Zero Trust paradigm, strategies, challenges and future research directions. The survey aims to contribute to the design and implementation of secure network architectures for critical infrastructures by enhancing the understanding of Zero Trust [40].

Mensah (2024) integration of ZTA with 5G networks, the IoT, edge computing, AI, ML, postquantum cryptography, blockchain technology, and other new developments are on the horizon. The purpose of this article is to provide a thorough explanation of Zero Trust Architecture by combining the results of recent studies and industry frameworks. This architecture may help organisations better prepare for cybersecurity in the ever-changing digital landscape [41].

Kang et al. (2023) Trust in hacking is talked about, and then the history, ideas, and rules behind zero trust are gone over in more detail. Existing study is looked at in terms of its features, strengths, and weaknesses, along with zero trust successes and how they can be used technically in Cloud and IoT settings. Lastly, the idea and its current problems are looked at to help zero trust grow and be used in the future [42].

He et al. (2022) This article talks about the current zero trust architecture and looks at the basic technologies that it is based on, such as proving identities, limiting access, and evaluating reliability. compare and analyse the main solutions for each technology to find out their pros and cons, as well as the present problems and study trends for the future. What wants to do is help with the study and use of future zero trust architectures [43].

TABLE I. COMPARATIVE ANALYSIS OF RECENT STUDY ON ZERO TRUST ARCHITECTURE

Author(s) & Year	Focus Area	Techniques / Approach	Limitations / Challenges	Recommendations / Future Directions
Soni et al. (2026)	Comparative synthesis of ZTAs across sectors	Multi-parameter analysis, comparative evaluation, sector-specific case studies	Limited empirical validation; lacks dynamic trust metrics	Develop adaptive ZT models with real-time trust scoring and cross-domain validation.
Pigola, Meirelles and Costa (2026)	Enterprise-level trust embedding and cultural alignment	Principal–agent theory, qualitative interviews, entropy-based MCDM, PLS-SEM	Underexplored enterprise-level dimensions; small sample size	Expand quantitative validation; integrate cultural and financial readiness into ZT adoption frameworks.
Mushtaq, Mohsin and Mushtaq (2025)	Scalability and compliance in ZTA implementations	Cross-domain comparative review (Cloud, IoT, Blockchain, Big Data)	Weak orchestration; limited lightweight cryptography; regulatory misalignment	Advance lightweight cryptographic schemes; automate orchestration; align with GDPR/HIPAA.
Gambo and Almulhem (2025)	Historical evolution and practical enforcement of ZTA	Analytical review of publications and adoption trends	Lack of quantitative performance metrics; limited predictive modeling	Incorporate telemetry-based analytics; develop adaptive monitoring for distributed networks.
Dhiman et al. (2024)	Foundational understanding of Zero Trust paradigm	Systematic survey of approaches and research objectives	Conceptual focus; minimal technical validation	Extend to critical infrastructure case studies; propose measurable ZT maturity models.
Mensah, (2024)	Emerging trends and integration with advanced technologies	Synthesis of studies and industry frameworks	Limited empirical testing of integrated ZTA models	Explore ZTA integration with 5G, IoT, AI, ML, PQC, and block chain for holistic resilience.
Kang et al. (2023)	Technical applications and conceptual analysis	Review of trust principles and ZT achievements in Cloud/IoT	Fragmented evaluation; lacks unified performance benchmarks	Develop standardized evaluation metrics; enhance interoperability across domains.
He et al. (2022)	Core technologies in Zero Trust Architecture	Comparative analysis of identity authentication, access control, trust assessment	Limited scalability; insufficient integration of emerging technologies	Strengthen identity-centric trust engines; adopt post-quantum cryptography for future ZTAs.

A. Research Gap

The reviewed studies collectively point to some research gaps in the field of ZTA. While there is considerable progress in comparative synthesis, enterprise adoption architectures and technical reviews, there are some challenges that still need to be addressed such as lightweight cryptography in resource constrained systems, automatic orchestration, dynamic trust metrics, and regulatory alignment. Moreover, it is not supported by sufficient empirical evidence in different areas (Internet of Things, blockchain, big data, etc.) and there are no unified performance indicators. These gaps highlight the importance of adaptive trust engines, integration capabilities with emerging technologies (AI, ML, PQC, 5G), and cross domain validation in bolstering ZTA resilience. A clear description of these gaps is given in Table I.

6. Conclusion and Future Work

A new paradigm in contemporary digital security, ZTA tries to address the issues with perimeter-based security paradigms. It is also known as Zero Trust Security. The "never trust, always verify" principle is at the heart of ZTA, which employs micro-segmentation, real-time monitoring, least-privilege access, continuous authentication, and authorisation to bolster security. This survey covered the fundamentals, principles, security models, and implementation methods of ZTA, as well as its use in IoT, cloud computing, SASE, and identity-centric security solutions. The literature survey shows that while great strides have been made in the adoption of ZTA, issues like scalability, interoperability, policy complexity, lightweight security mechanisms, and compliance remain unaddressed. Also, the variability of the evaluation metrics, and the absence of a comprehensive cross-domain validation, reduces the usefulness of existing implementations.

Further studies are needed on adaptive trust evaluation, automatic orchestration, lightweight cryptographic solution and intelligent policy enforcement. The adoption of emerging technologies like AI, ML, Blockchain, PQC and 5G/6G networks can enhance ZTA capabilities and boost cyber resilience in ever-more complex and distributed environments.

REFERENCES

1. R. Keshava, S. K. Pandurangan, M. Sakthivanitha, S. Parmsivan, G. Sunkara, and R. Maruthi, "AI-Powered Algorithms for the Prevention and Detection of Computer Malware Infections," in 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), IEEE, Sep. 2025, pp. 1673–1680. doi: 10.1109/ICESC65114.2025.11212519.
2. V. Sharma, "Zero Trust Architecture for 5G Networks," Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci., vol. 12, no. 6, pp. 1–11, Nov. 2024, doi: 10.37082/IJIRMPS.v12.i6.232707.
3. J. B. Mehta, "Securing Test Automation in Zero Trust Architectures: A Framework for Continuous Verification," in 2025 International Conference on Computer and Applications (ICCA), IEEE, Dec. 2025, pp. 1–5. doi: 10.1109/ICCA66035.2025.11430950.
4. S. Tyagi and A. Tyagi, "Evaluating the Performance with Deep Learning Techniques in Cybersecurity for Effective Threat Detection," 2026, pp. 437–452. doi: 10.1007/978-981-96-8687-2_31.
5. N. Adik, "The Rise of Open and Free Networks: A Community-Driven Paradigm for Decentralized Connectivity," in 2025 IEEE First International Conference on Innovations in Engineering and Next-Generation Technologies for Sustainability (ICINVENTS), Coimbatore, India: IEEE, 2025, pp. 1–9, November. doi: 10.1109/ICINVENTS64613.2025.11402224.
6. S. Ameer, L. Praharaj, R. Sandhu, S. Bhatt, and M. Gupta, "ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model," ACM Trans. Priv. Secur., vol. 27, no. 3, Aug. 2024, doi: 10.1145/3671147.
7. S. Al-Tamimi, Q. A. Al-Haija, and K. Alrawashdeh, "Zero-Trust Architecture for Securing Internet of Things (IoT) Networks: A Review," in CIEES 2024 - IEEE International Conference on Communications, Information, Electronic and Energy Systems, 2024. doi: 10.1109/CIEES62939.2024.10811176.
8. Z. ElSayed, N. Elsayed, and S. Bay, "A Novel Zero-Trust Machine Learning Green Architecture for Healthcare IoT Cybersecurity: Review, Analysis, and Implementation," in SoutheastCon 2024, IEEE, Mar. 2024, pp. 686–692. doi: 10.1109/SoutheastCon52093.2024.10500139.
9. I. A. Khan et al., "A context-aware zero trust-based hybrid approach to IoT-based self-driving vehicles security," Ad Hoc Networks, 2025, doi: 10.1016/j.adhoc.2024.103694.
10. K. Li et al., "Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things," IEEE Internet Things J., May 2025, doi: 10.1109/JIOT.2025.3603957.
11. A. M. Abdelmagid and R. Diaz, "Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems," Risk Anal., 2025, doi: 10.1111/risa.70026.
12. S. Mushtaq, M. Mohsin, and M. M. Mushtaq, "A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains," 2025. doi: 10.3390/s25196118.
13. J. B. Mehta, "An Autonomous Dependency And Failure-Propagation Modeling System For Security-Critical Distributed Enterprise Cloud Computing Environments,"," 202641001713, 2026
14. N. D. Bhandarwar, "A Mathematical Framework For Explainable And Adversarially Robust Ids Using Ml For Large-Scale Enterprise And Cloud Systems," Int. J. Appl. Math., vol. 39, no. 1s, pp. 1200–1212, Jan. 2026, doi: 10.12732/ijam.v39i1s.1910.
15. V. K. Bollu, "Threat Landscape in Artificial Intelligence Systems: Taxonomy, Attack Vectors and

Security Implications," World J. Adv. Res. Rev., vol. 29, no. 1, pp. 285–294, 2026, doi: 10.30574/wjarr.2026.29.1.0007.

16. B. Embrey, "The top three factors driving zero trust adoption," Comput. Fraud Secur., 2020, doi: 10.1016/S1361-3723(20)30097-X.

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

18. D. Jain and S. Jain, "Artificial Intelligence (AI)-Driven Network Traffic Anomaly Detection for IT Infrastructure Security," in 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395685.

19. H. K. Yadav, "Design and Implement Machine Learning Based Predictive Analytics for Road Safety and Accident Prevention," in 2026 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India: IEEE, 2026, pp. 1–6, March. doi: 10.1109/IATMSI68868.2026.11465965.

20. Y. Muni, "A Review of Efficient Routing Architectures Using OSPF, BGP, and MPLS in Multi-Protocol Networks," Eng. Technol. J., vol. 11, no. 01, Jan. 2026, doi: 10.47191/etj/v11i01.21.

21. Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120–134, Jun. 2014, doi: 10.1016/j.jnca.2014.01.014.

22. S. Singh, "Advancing Network Security in 5G: Leveraging the 5G-NIDD Dataset for Intrusion Detection and Mitigation," in 2025 IEEE 12th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, Nov. 2025, pp. 1–6. doi: 10.1109/CSCloud66326.2025.00055.

23. D. Horne and S. Nair, "Introducing Zero Trust by Design: Principles and Practice Beyond the Zero Trust Hype," dvances Secur. Networks, Internet Things (SAM, ICWN, ICOMP, ESCS 2021), pp. 512–525, 2021.

24. R. Lingam, S. Nagi, M. Chigurupati, and B. T. Myneni, "Resilient DevSecOps: Self-Healing Cloud-Native Systems via SRE-Driven AI Threat Detection and Response," in 2026 International Conference on Smart Futuristic Technology, IEEE, Jan. 2026, pp. 1–6. doi: 10.1109/ICSFT66733.2026.11508049.

25. S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, "Zero Trust: Applications, Challenges, and Opportunities," 2023.

26. S. Yiliyaer and Y. Kim, "Secure Access Service Edge: A Zero Trust Based Framework For Accessing Data Securely," in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), IEEE, Jan. 2022, pp. 0586–0591. doi: 10.1109/CCWC54503.2022.9720872.

27. S. R. Kandula, N. Kassetty, K. S. ALANG, and P. Pandey, "Context-Aware Multi-Factor Authentication in Zero Trust Architecture: Enhancing Security Through Adaptive Authentication," Int. J. Glob. Innov. Solut., Dec. 2024, doi: 10.21428/e90189c8.f525ef41.

28. T. Chuan, Y. Lv, Z. Qi, L. Xie, and W. Guo, "An Implementation Method of Zero-trust Architecture," J. Phys. Conf. Ser., vol. 1651, no. 1, p. 012010, Nov. 2020, doi: 10.1088/1742-6596/1651/1/012010.

29. S. Ahmadi, "Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities," J. Eng. Res. Reports, vol. 26, pp. 215–228, 2024, doi: 10.9734/JERR/2024/v26i21083.

30. Y. Cao, S. R. Pokhrel, Y. Zhu, R. Doss, and G. Li, "Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges," 2024. doi: 10.1007/s11633-023-1456-2.

31. M. Nasiruzzaman, M. Ali, I. Salam, and M. H. Miraz, "The Evolution of Zero Trust Architecture (ZTA) from Concept to Implementation," in 2025 29th International Conference on Information Technology, IT 2025, 2025. doi: 10.1109/IT64745.2025.10930254.

32. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

33. S. Mthethwa, E. Jembere, and M. Dlamini, "IAM-based Zero Trust Architecture for IoT: Securing Non-Human Identities in a Connected World," in 2025 IEEE International Conference on Smart Internet of Things (SmartIoT), IEEE, Nov. 2025, pp. 428–435. doi: 10.1109/SmartIoT66867.2025.00069.

34. L. Ahuja, S. Vashisth, and A. Thakur, "Integrating SIEM with Zero Trust Architecture," in 2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), IEEE, Jan. 2025, pp. 1–6. doi: 10.1109/IITCEE64140.2025.10915422.

35. P. SumanPrakash et al., "Learning-driven Continuous Diagnostics and Mitigation program for secure edge management through Zero-Trust

Architecture," Comput. Commun., vol. 220, pp. 94–107, Apr. 2024, doi: 10.1016/j.comcom.2024.04.007.

36. R. P. Reddy, "Zero Trust Architectures in Modern Enterprises: Principles, Implementation Challenges, and Best Practices," Int. J. Comput. Trends Technol., vol. 73, no. 6, pp. 48–57, Jun. 2025, doi: 10.14445/22312803/IJCTT-V73I6P107.

37. A. Soni, S. Kumar Nanda, R. Priyadarshini, and G. Panda, "A comprehensive review and comparative analysis of zero trust architecture: Evolution, implementation strategies, and key challenges," J. Comput. Secur., vol. 34, no. 2, pp. 85–110, Mar. 2026, doi: 10.1177/0926227X251409922.

38. A. Pigola, F. de Souza Meirelles, and P. R. da Costa, "Trust Management in the Age of Zero trust: a comprehensive multi-method analysis from enterprise challenges," Enterp. Inf. Syst., vol. 20, no. 1, Jan. 2026, doi: 10.1080/17517575.2025.2588753.

39. M. L. Gambo and A. Almulhem, "Zero Trust Architecture: A Systematic Literature Review," 2025.

40. P. Dhiman et al., "A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model," Sensors, vol. 24, no. 4, p. 1328, Feb. 2024, doi: 10.3390/s24041328.

41. F. Mensah, "Zero Trust Architecture: A Comprehensive Review of Principles, Implementation Strategies, and Future Directions in Enterprise Cybersecurity," Int. J. Adv. Res., vol. 10, no. 6, pp. 2454–132, 2024.

42. H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," Entropy, vol. 25, no. 12, 2023, doi: 10.3390/e25121595.

43. Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," Wirel. Commun. Mob. Comput., vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/6476274.