

# The Impact of Zero Trust Architecture on Enterprise Cybersecurity

(Dr.) Abid Hussain

Professor

School of Computer Application & Technology & Dean

Research Career Point University,

Kota

[abid.hussain@cpur.edu.in](mailto:abid.hussain@cpur.edu.in)

Corresponding Author: \*Abid Hussain ([abid.hussain@cpur.edu.in](mailto:abid.hussain@cpur.edu.in)),

Received: 1 September, 2026 | Revised: 5 September 2026 | Accepted: 28 September 2026

**Abstract**—Enterprise cybersecurity is now crucial in safeguarding digital services, apps, data, networks, and devices against ever-changing cyber threats. This review examines major enterprise cybersecurity roles, applications, architectures, and emerging intelligent defense techniques. It discusses signature- and behavior-based threat detection, highlighting the speed of signature matching while noting its limitations against unknown and modified attacks. Enterprise security architecture is reviewed through key components such as the Internet, demilitarized zone, firewalls, and organizational security policies. Major applications include network security, endpoint detection and response, security risk assessment, compliance, encryption, and cloud security risk management. The review further examines Zero Trust Architecture (ZTA), emphasizing Zero Trust Network Access, policy-based access control, cloud-based ZTNA, IoT security, and healthcare applications. Identity and Access Management is considered through identity lifecycle management, access governance, and role-based access control. Finally, state-of-the-art AI/ML techniques are analyzed, including machine learning, deep learning, transformer models, graph neural networks, federated learning, explainable AI, adversarial machine learning, and generative AI. Their applications in intrusion detection, anomaly detection, malware classification, behavioral analysis, and Industrial IoT threat intelligence demonstrate their potential to strengthen adaptive, proactive, resilient, and intelligent modern enterprise cybersecurity systems.

**Keywords**—Enterprise Cybersecurity, Zero Trust Architecture, Threat Detection, Network Security, Cloud Security, IAM, Data Protection, Endpoint Security.

## I. INTRODUCTION

In today's quickly changing digital world, enterprises confront an expanding number of security risks and vulnerabilities [1]. Cyberattacks have skyrocketed with the rise of new innovation like mobile devices, the Internet of Things (IoT), and cloud computing. Business data and resource security faces additional challenges as a result [2]. DDoS attacks, phishing attacks, malware attacks, theft of sensitive data, or even threats from within enterprises are the most dangerous threats to enterprises [3]. These threats can cause financial losses, reputational damage, and loss of user

data. Companies need comprehensive security solutions to maintain stable company operations, ensure customer trust, and raise security awareness [4]. Cybercriminals are becoming more adept at evading classic security measures like firewalls, intrusion detection systems, and antivirus software.

The revolutionary security paradigm known as Zero Trust Architecture (ZTA) aims to strictly regulate access and do away with implicit trust. Unlike traditional models that establish security boundaries around network perimeters, Zero Trust mandates continuous verification of all users, devices, and applications attempting to access network resources [5][6]. The foundation of this strategy is the golden rule of "never trust, always verify," which guarantees that security regulations are constantly enforced via contextual analysis and real-time authentication. Using micro-segmentation and stringent access restrictions, ZTA reduces the likelihood of lateral movement and illegal access to networks [7]. The necessity for Zero Trust has been driven by the increasing sophistication of cyber threats, including ransomware attacks, insider threats, and supply chain compromises [8]. Cybercriminals continuously exploit weaknesses in identity management, privilege escalation, and endpoint security to infiltrate organizational networks. The perimeter defence approach has long been the foundation of cybersecurity models past. In this model, firewalls, intrusion detection systems, and other security measures were put in place to monitor and regulate incoming and outgoing traffic on an organization's network [9][10][11]. The assumption was simple: once inside the network, users and devices were trusted by default, and internal security was less of a concern. However, the dramatic shift toward cloud computing, mobile workforces, and highly interconnected systems has rendered this perimeter-based approach insufficient.

### A. Structure of the Paper

The structure of the paper is organized as follows: Section II discusses enterprise cybersecurity roles and applications. Section III presents Zero Trust Architecture, ZTNA, IAM, and AI/ML techniques. Section IV reviews existing literature and research gaps. Section V presents the conclusion and future work.

## II. ROLE OF ENTERPRISE CYBERSECURITY

Enterprise cybersecurity plays a critical role in protecting organizational data, applications, networks, devices, and digital services from evolving cyber threats. It helps prevent unauthorized access, malware, phishing, data breaches, and insider attacks while ensuring business continuity and regulatory compliance [12]. Effective cybersecurity strengthens customer trust, reduces financial and reputational risks, and supports secure digital transformation across modern enterprise environments. In the detection of the cybersecurity threat, researchers have categorized these strategies and methods into two, 1. Signature-based and 2. Behavioral-based.

### A. Signature-Based Cybersecurity Threat Detection

This type of detection approach can able to detect malicious patterns or a specific identity of a suspicious file. The method is very fast compared to other techniques because any system has a limited number of signatures, and it is easier to match the signature. Consequently, this mechanism does not work on unknown threats, and the system fails to detect some threats with a slightly different signature [13]. The signature of any threat can be generated using hashing algorithms such as MD5 and SHA1. The IoC also help in the process of signature generation.

### B. Behavioural-Based Cybersecurity Threat Detection

Behavioral-based threat detection uses the learning approach to detect abnormal patterns in the system, whether it is generated by some network activities or by some suspicious file. The learning approach can be an ML or DL method [14]. The performance of these methods depends on various features, including API calls, browser-generated events, system and network events, file activities, and registry changes.

### C. Enterprise Security Architecture

Enterprise security architectures that work together in harmony with an organization's fundamental objectives and long-term plans include best practices, cutting-edge technology, and policy [15]. While information security technology gets all the attention, the policies that govern its deployment also dictate the procedures, guidelines, and materials that are required. Figure 1 shows how corporate security architecture is related to security practices like risk management, performance evaluation, and company optimization.

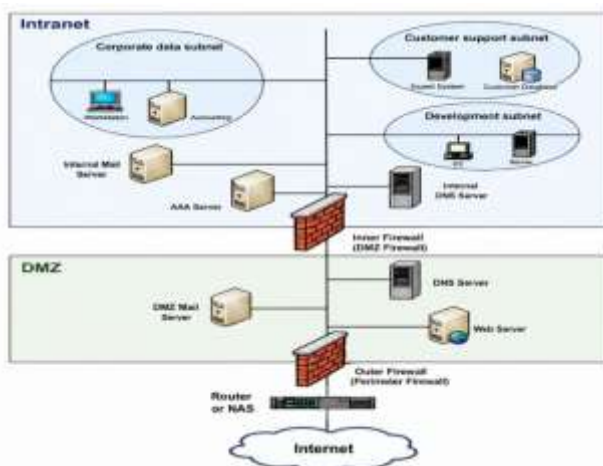


Fig. 1. Enterprise Network Physical Security Architecture

- **Internet:** The Internet Protocol Suite (TCP/IP) is a set of standards for data transfer between networks of computers all over the world. Connected via wireless connections, fiber-optic cables, copper lines, and other technologies, the Internet is a worldwide network that includes millions of public and private network devices.
- **Internet Demilitarized Zone (DMZ):** The term "demilitarized zone" (DMZ) refers to a specific kind of subnetwork that many organizations use to house and access their external services from the wider, distrusted Internet. The DMZ is the cyberspace that divides an internal network from an outside one. For internal networks, it acts as a "buffer" between the unregulated Internet and themselves.
- **Enterprise Firewalls:** A firewall is a security device or network of devices that acts as a middleman between a network and any unauthorized users or programs trying to access its resources. In a typical setup, a dedicated server is used to operate the firewall software, which in turn protects one of the networks from the other.

### D. Enterprise Cybersecurity of Application

Enterprise cybersecurity is applied across network security, cloud environments, endpoints, applications, data protection, identity management, and threat detection. Enterprise resource confidentiality, integrity, and availability may be guaranteed with the aid of these apps, which also help with preventing unauthorized access, securing sensitive information, monitoring suspicious activity, detecting cyberattacks, and maintaining regulatory compliance.

#### 1) Network Security

The specifics of the security breach in the network are laid forth here. First, the OSI model, its layers, and the protocols for each layer are described. After that, we take a close look at the assaults on each layer. Afterward, the methods and equipment used to secure networks will be detailed. Last but not least, we go over ways to secure wireless networks, potential threats to such networks, and wireless network security measures [16]. The following is a synopsis of the study's contributions, which were based on careful consideration of the aforementioned subjects:

- The state of affairs, shortcomings, and technical advancements in the area of cyber security are described.
- The most essential knowledge on cyber security basics is given.
- Threats, assaults, and current research in cyber security are detailed.
- OSI levels, network security, and threats on each layer are described.
- Current difficulties, issues, and recommended new assumptions.

#### 2) Endpoint Detection and Response (EDR)

With complex, distributed IT environments and sophisticated threats, EDR-SIEM serviceability is an evolving and critical function. It moves beyond simple deployment to include Managing diverse endpoints Many organizations now have a mix of on-premises, mobile, and cloud-based endpoints, all of which must be properly serviced and protected. Integrating advanced analytics These solutions leverage AI and ML, and serviceability ensures these tools are

properly tuned to balance accuracy with false positives. Leveraging managed services: Many organizations use MDR services from third-party experts to handle the complexities of this serviceability and monitoring [17].

### 3) Security Risk Assessment

Security risk assessment is a systematic process of identifying, analyzing, and evaluating potential security risks within an organization's information systems, data, and processes. It plays a fundamental role in understanding the threat landscape and implementing effective risk mitigation strategies [18]. Here's a detailed overview of security risk assessment:

- **Identification of Assets:** The first step in a security risk assessment is to identify and classify the critical assets within an organization, including information systems, data repositories, hardware, software, and personnel. Understanding what needs to be protected is essential for assessing potential risks.
- **Threat Identification:** Once assets are identified, the next step is to identify potential threats and vulnerabilities that could pose risks to those assets. This involves analyzing external and internal threats that could exploit weaknesses in the system.
- **Vulnerability Assessment:** Vulnerability assessments are useful for finding security flaws, misconfigurations, or holes that malicious actors may exploit. The phase often involves the use of vulnerability scanning tools and penetration testing procedures.

### 4) Compliance and Security

There exists a prevalent misconception that compliance to standards and regulation equals strong cybersecurity. However, attackers don't care whether an organization is fully compliant or not, they try to find vulnerabilities anyway. In their empirical compliance to regulatory frameworks had no impact on data breach occurrence [19]. Furthermore, they find that: "immature hospitals are motivated by meeting compliance mandates rather than actually protecting information.

### 5) Encryption Techniques

Data integrity inside corporate applications is safeguarded by implementing cybersecurity measures, one of which is encryption [20]. Encryption is an important safeguard against data breaches and illegal access, especially with the sophistication of cyber threats. Encryption keeps sensitive information safe from prying eyes by transforming it into a form that cannot be read without the correct decryption key.

### 6) Cloud Security Risk Management

Cloud security risk management is a focus area in current cloud computing research. As a result, researchers proposed different security risk management methods and frameworks. assessment as a service, qualitative and quantitative, hierarchical, graph analysis and security matrix assessment [21]. They identified the main processes and components of the methods, but they didn't assess the effectiveness of those methods. surveyed existing knowledge on cloud computing risk assessment.

## III. FUNDAMENTALS OF ZERO TRUST ARCHITECTURE

Zero trust is a cybersecurity model that prioritizes protection by implementing ZT principles within a business

network infrastructure. Its primary goal is to improve network security via coordinating component interactions, controlling access, and organizing workflow [22]. The deployment of ZTA within an organization consists of various logical components that are interconnected and can be implemented as an in-house or cloud-based service.

### A. Zero Trust Network Access (ZTNA)

ZTNA emerges as a response to these challenges, offering a more flexible and robust approach to securing modern network environments. The core principle of ZTNA is simple yet powerful: "never trust, always verify" [23]. Unlike traditional models that automatically trust any device within the network perimeter, ZTNA assumes that every request for access, regardless of its origin, must be treated with caution and subjected to strict verification.

#### 1) Policy-Based Access Control

The core of ZTNA is PBAC, which controls who may access what resources based on predetermined security rules. Who may use what resources, when, and how is defined by these regulations [24]. Unlike traditional models with static permissions, PBAC in ZTNA is dynamic and adapts in real-time, leveraging data about users, devices, and network environments to make access decisions.

#### 2) Cloud-Based ZTNA

Cloud-Based ZTNA solutions are designed to address the unique security challenges of cloud environments, including multi-tenancy and dynamic resource allocation [25]. Unlike traditional on-premises security models, cloud-native ZTNA enforces layered access controls—from device and network entry points to the application layer—ensuring security coverage in cloud-first architectures. Cloud-based ZTNA continuously evaluates access based on user identity, device health, and behaviour patterns, adapting as conditions change.

### 3) Internet of Things (IoT) and ZTA

Modern research shows that resource-aware policy enforcement, decentralized trust engines, and dynamic context-awareness are becoming more important in ZTA frameworks for the IoT, even if they are the foundational features of most of these frameworks. With these updates, we want to shore up IoT networks that are susceptible to physical and cyber manipulation, have limited computing resources, and use weak default credentials.

### 4) Healthcare Systems and ZTA

Cyberattacks in the healthcare industry may compromise sensitive patient information, put people's lives in jeopardy, and cause noncompliance with regulations. Increased reliance on telemedicine, cloud storage, IoT patient monitoring, and EHRs has increased the attack surface and shown weaknesses in conventional security systems [26]. With its potential to provide granular access control, guarantee data secrecy, and partition clinical networks from both internal and external dangers, the ZTA paradigm has attracted interest in the healthcare industry.

### B. IAM Components and Technical Architecture

Modern enterprise identity management requires a comprehensive architectural approach that integrates multiple technological components into a cohesive security framework [27]. Organizations need to grasp the interplay between these elements in order to build identity governance capabilities that can manage varied business environments. The following

analysis examines the core architectural elements that form the foundation of successful IAM implementations.

#### 1) Identity Lifecycle Management Infrastructure

The operational backbone of any effective IAM system, encompassing the complete journey of digital identities from creation to termination. This comprehensive process begins when new employees join the organization, triggering automated account creation workflows that are based on predefined role templates and specific business requirements. The provisioning workflow must seamlessly integrate with human resources systems to ensure that account creation aligns with employment status and organizational hierarchy.

#### 2) Access Governance and Role-Based Control Systems

The policy foundation that guides all access decision-making processes throughout the organization. RBAC implementation creates standardized access patterns that align directly with organizational structures and specific job functions, significantly reducing administrative complexity while improving security consistency across the enterprise. RBAC systems define roles based on actual job responsibilities rather than individual user requests, enabling scalable access management that can accommodate organizational growth and structural change.

#### C. State-of-the-Art AI/ML Techniques in Cybersecurity

Transforming cybersecurity by improving automated threat detection, intrusion detection, malware classification, behavioral analysis, and threat intelligence. Recent reviews highlight deep learning, transformer models, graph neural networks, federated learning, explainable AI, adversarial machine learning, and generative AI as important approaches for addressing sophisticated and evolving cyber threats.

#### 1) Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

IDS and IPS are critical components of any cybersecurity architecture, designed to monitor network traffic for suspicious activities and either alert the relevant authorities through an Intrusion Detection System (IDS) or take immediate action to block potential network attacks through an Intrusion Prevention System (IPS)[28][29]. Historically, these systems relied on signature-based methods for detecting known network attacks. While effective in identifying well-documented attack vectors, such approaches struggled to detect novel or unknown threats, leaving organizations vulnerable to zero-day attacks and sophisticated network intrusions[30].

#### 2) Enhancing Anomaly Detection with Machine Learning

One of the key benefits of integrating ML into IDS/IPS systems is its ability to improve anomaly detection. Traditional IDS/IPS systems are often rule-based, meaning they rely on predefined patterns and signatures to identify malicious activity [31]. However, this reliance on fixed rules limits their ability to detect previously unseen threats or attacks that deviate from established norms. In contrast, ML algorithms can analyze vast amounts of network traffic data, learning what constitutes normal behavior within a system and identifying deviations that may indicate malicious activity.

#### 3) Deep Learning and Neural Networks

Another advanced ML technique that has gained traction in enhancing IDS/IPS systems is DL, particularly through the use of neural networks. DL models are capable of analyzing complex data patterns, making them well-suited for the

multidimensional nature of network traffic data [32]. For instance, RNNs and LSTM networks can model temporal dependencies in network behavior, identifying anomalies over time that might indicate slow, stealthy intrusions, such as APTs.

#### 4) AI for Threat Intelligence in IIoT

IIoT systems face unique cybersecurity threats due to their highly distributed nature and lack of standardized architectures. AI-driven cybersecurity solutions, particularly deep learning-based models, have emerged as a critical defense against complex IIoT threats [33]. A recent study introduced a self-learning ConvLSTM2D-based multisector threat intelligence and detection mechanism, capable of proactively defending against sophisticated IIoT attacks.

### IV. LITERATURE REVIEW

This section reviews recent Zero Trust Architecture studies, emphasizing AI-driven access control, blockchain integration, cloud security, IoT protection, and adaptive cybersecurity mechanisms.

R. K. Kotapati (2026) explored how AI can be integrated into Zero Trust Network Access and Privileged Access Management models to create a more inclusive and equitable cybersecurity stance in enterprises around the world. In the past, strict security measures have unintentionally blocked neurodivergent people and users in areas with low-tech infrastructure. This study proposes an AI-based adaptive architecture that uses predictive analytics and behavioral biometrics to supplant exclusionary, traditional authentication techniques. The study assesses the effectiveness of inclusive security by relying on a filtered set of 364 simulated log entries of enterprise access, including a variety of patterns of user interaction and geographic latencies [34].

R. K. S. Sulthana, et al. (2026) Cloud computing's meteoric ascent, digital transformation, and hybrid business settings have all highlighted the shortcomings of perimeter-based defensive methods. In response, ZTA has arisen as a revolutionary cybersecurity architecture. ZTA is based on micro-segmentation, continuous verification, and least privilege access. It enforces dynamic, context-aware authentication for every user, device, and data transaction which removes implicit trust. To further improve ZTA's flexibility, we integrate AI, ML, and behavioral analytics. This allows us to identify threats in real-time, respond automatically to incidents, and analyses risks intelligently [35].

S. Qiu and C. Li (2025) Proposed a novel access control scheme for supply chain finance by integrating ZTA with blockchain technology to enhance security and operational efficiency. The scheme utilizes ZTA to achieve dynamic management and access control for enterprises, ensuring data security during access. The scheme integrates identity management and access control modules into the blockchain via smart contracts. This ensures automated, tamper-resistant transaction execution. Credit scoring makes use of the RF method, which outperforms more conventional classifiers like decision trees and SVM on datasets that are high dimensional and diverse [36].

A. H. A. Alwyn, et al. (2025) advanced cybersecurity trends: the development and deployment of AI-based policies and Zero Trust principles for the management of access control rules in cloud-based environments. With AI-driven

policies, decision-making can be automated as to who is allowed to access which resources, at what time, and under which conditions. Through analyzing such a large pool of historical and real-time data, machine learning automation can anticipate potential threats, judge user behavior and adapt access control regulation dynamically to minimize risks. Ensuring that only authorized individuals are granted access to sensitive data or systems is one use case for these intelligent systems [37].

T. Sarkorn, et al. (2024) Used The comprehensive application of Zero Trust principles within Next Generation Firewall (NGFW) devices by integrating the improved ZTA and NGFW to provide durable security controls thorough and continuously updated. This is necessary to mitigate and prevent the complexity of cyber threats. The article examine key elements of the ZTA, including user authentication. Subdivision and implementation of least privileged access within existing NGFW devices are also discussed. Case studies and current progress are discussed to demonstrate the practical benefits and challenges of this integration. The results show that integrating the ZTA architecture with NGFW devices not only strengthens security measures but also enhances security. It also provides a scalable and adaptable solution for modern organizations facing complex and persistent cyber threats [38].

S. Al-Tamimi, et al. (2024) covers ZTA for IoT network security. A combination of identity verification, fine-grained segmentation, and constant monitoring might be the way ZTA handles problems. Organizations may successfully implement ZTA and ensure a solid security posture against growing threats with the practical guidance provided by this study, which contributes to building a complete framework for ZTA customized for the IoT. The research also emphasizes the integration of cutting-edge technology. The study covers ZT, ZTA concepts, algorithms workflows, security challenges, and solutions for IoT network security [39].

K. Che and S. Sheng (2023) analyzes the genetic defects in the inherent mechanism of cloud native, especially the service governance framework mechanism, from a new perspective. These genetic defects not disappear with the intergenerational development of mobile cloud native. Therefore, they are also known as the endogenous security common problems of cloud native. the endogenous security threats that may be introduced by security flaws such as "default information authenticity" and "ubiquitous data visibility". Guided by the theory of endogenous security in cyberspace, it proposes the idea and method of using "zero trust" to break the "default trust" and using "implicit mapping" to achieve "limited visibility" of user data to solve the common problems of cloud native endogenous security, And a new zero trust gateway architecture ecology and corresponding applicability function quantification load balancing strategy have been reconstructed [40].

Existing studies have advanced ZTA through AI-driven authentication, behavioral analytics, blockchain, IoT security, and next-generation firewalls. However, research gaps remain, particularly the lack of unified enterprise-wide ZTA frameworks. Limited research addresses integration with legacy systems, hybrid cloud environments, IoT devices, and distributed infrastructures. AI-based approaches also require extensive data for accurate risk assessment, while privacy, explainability, and adversarial attack protection need further attention. Many studies use simulated or domain-specific datasets, limiting generalizability and real-world validation. As summarized in Table I, current research lacks integrated, scalable, adaptive, and continuously monitored security mechanisms. Future research should focus on AI-enabled ZTA frameworks integrating identity management, behavioral analytics, micro-segmentation, continuous authentication, and automated threat response while ensuring privacy, usability, interoperability, and regulatory compliance.

TABLE I. SUMMARY OF KEY STUDIES ON ZERO TRUST ARCHITECTURE ON ENTERPRISE CYBERSECURITY

| Author & Year                | Research Focus                     | Method/Technology                                               | Key Contribution                                                                       | Advantages                                       | Limitations                                                 |
|------------------------------|------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------|-------------------------------------------------------------|
| R. K. Kotapati (2026)        | Inclusive enterprise cybersecurity | AI, ZTNA, PAM, predictive analytics, behavioral biometrics      | Proposed adaptive authentication to improve inclusive and equitable access             | Adaptive and user-centric security               | Based on only 364 simulated log entries                     |
| R. K. Sulthana et al. (2026) | Enterprise Zero Trust security     | ZTA, AI, ML, behavioral analytics, micro-segmentation           | Enabled predictive threat detection, real-time risk assessment, and automated response | Dynamic and context-aware protection             | Complex implementation and integration                      |
| S. Qiu & C. Li (2025)        | Secure supply chain finance        | ZTA, blockchain, smart contracts, Random Forest                 | Developed dynamic access control with tamper-resistant transactions                    | Strong integrity and automated access management | Mainly focused on supply chain finance                      |
| A. H. A. Alwyn et al. (2025) | Cloud-based access control         | AI, ML, adaptive security policies                              | Automated risk-based access decisions using behavioral and real-time data              | Fine-grained and adaptive access control         | Requires large amounts of quality data                      |
| T. Sarkorn et al. (2024)     | ZTA-enabled network firewalls      | ZTA, NGFW, authentication, least privilege                      | Integrated Zero Trust principles with NGFW for continuous protection                   | Scalable and adaptable enterprise security       | Integration with existing infrastructure can be challenging |
| S. Al-Tamimi et al. (2024)   | IoT network security               | ZTA, identity verification, segmentation, continuous monitoring | Proposed a Zero Trust framework tailored for IoT environments                          | Improved IoT protection and visibility           | Resource and deployment constraints                         |
| K. Che & S. Sheng (2023)     | Cloud-native security              | Zero Trust, implicit mapping, Zero Trust gateway                | Addressed default trust and excessive data visibility in cloud-native systems          | Improved visibility control and security         | Limited applicability beyond cloud-native environments      |

## V. CONCLUSION AND FUTURE WORK

Enterprise cybersecurity requires a thorough and flexible strategy to safeguard assets against changing cyberthreats.

The review demonstrates that traditional signature-based detection remains effective for known threats, while behavioral-based detection improves identification of abnormal activities. Network security, endpoint protection,

risk assessment, encryption, cloud security, and compliance provide defensive capabilities. Zero Trust Architecture strengthens protection through continuous verification, controlled access, policy enforcement, and resource segmentation. Identity and Access Management supports identity lifecycle management and role-based access governance. AI and ML enhance cybersecurity by enabling intrusion detection, anomaly identification, behavioral analysis, and threat intelligence. Techniques, including deep learning, transformer models, graph neural networks, federated learning, explainable AI, adversarial machine learning, and generative AI, provide opportunities for adaptive security solutions. Overall, integrating security controls with Zero Trust principles, identity governance, and technologies can improve resilience. In today's digital surroundings, this kind of integration aids organizations in risk management, information security, continuity, and effective response to complex cyber-attacks.

Future work should focus on developing adaptive AI-driven cybersecurity frameworks capable of real-time threat prediction, automated response, and continuous learning. Future studies should also investigate Zero Trust integration, explainable AI, federated learning, privacy preservation, adversarial robustness, and scalable security solutions for cloud, IoT, and complex enterprise environments.

- **Funding:** This research received no external funding.
- **Institutional Review Board Statement:** Not applicable.
- **Informed Consent Statement:** Not applicable.
- **Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.
- **Conflicts of Interest:** The author declares no conflict of interest.

#### How to cite this article:

Abid Hussain, "The Impact of Zero Trust Architecture on Enterprise Cybersecurity," *Journal of Global Research in Multidisciplinary Studies*, vol. 2, no. 9, pp. 01–07, Sep. 2026. Doi, XXX

#### REFERENCES

- [1] J. Kaur and K. R. Ramkumar, "The recent trends in cyber security: A review," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5766–5781, Sep. 2022, doi: 10.1016/j.jksuci.2021.01.018.
- [2] P. L. Jaiswal, R. Vishvakarma, and S. Jacob, "From Automation Panic to Workforce Resilience: A Governance Framework for Enterprise AI Transformation," *IARJSET*, vol. 13, no. 5, pp. 463–485, May, May 2026, doi: 10.17148/IARJSET.2026.13562.
- [3] S. C. Pallaprolu, R. Sankineni, M. Thevar, G. Karabatis, and J. Wang, "Zero-day attack identification in streaming data using semantics and Spark," in *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA: IEEE, 2017, pp. 121–128, June, doi: 10.1109/BigDataCongress.2017.25.
- [4] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Comput. Secur.*, vol. 72, pp. 212–233, Jan. 2018, doi: 10.1016/j.cose.2017.09.001.
- [5] H. Chaudhary, A. Detroja, P. Prajapati, and P. Shah, "A review of various challenges in cybersecurity using Artificial Intelligence," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, IEEE, Dec. 2020, pp. 829–836, doi: 10.1109/ICISS49785.2020.9316003.
- [6] S. Kumara and M. Shah, "Securing national connectivity infrastructure through identity resilience: implications for zero trust," *Futur. Technol. Open Access J.*, vol. 5, no. 3, pp. 276–286, August, 2026, doi: 10.55670/fpl.futech.5.3.24.
- [7] S. M. J. A. S. N., and R. M., "Zero trust architecture in modern computer networks," *World J. Adv. Res. Rev.*, vol. 7, no. 3, pp. 347–356, Sep. 2020, doi: 10.30574/wjarr.2020.7.3.0280.
- [8] S. Remella *et al.*, "Intelligent Cost Governance in Cloud Supply Chains," in *2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT)*, Belagavi, India: IEEE, 2025, pp. 1–7, December, doi: 10.1109/ICAFT66710.2025.11452715.
- [9] E. William, "From Perimeter Defense To Zero Trust: Evolving Cybersecurity for a Changing World," 2022.
- [10] 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)*, New York City, NY, USA: IEEE, 2025, pp. 1–6, November, December, doi: 10.1109/CSCloud66326.2025.00055.
- [11] V. Rohilla, K. Rohilla, P. Kumar, and N. Jain, "Intrusion Detection in Network Traffic Using Feature Selection and Optuna-Based Machine Learning Optimization," in *2026 3rd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*, Chennai, India: IEEE, 2026, pp. 1–6, April, doi: 10.1109/RMKMATE69073.2026.11518834.
- [12] R. K. Kanneganti, "Security and Compliance Issues in Cloud-Based Deployments of Content and Workflow Management Systems," *Eastasouth J. Inf. Syst. Comput. Sci.*, vol. 2, no. 01, pp. 131–138, Aug. 2024, doi: 10.58812/esiscs.v2i01.1122.
- [13] U. Narra, F. Di Troia, V. A. Corrado, T. H. Austin, and M. Stamp, "Clustering versus SVM for malware detection," *J. Comput. Virol. Hacking Tech.*, vol. 12, no. 4, pp. 213–224, Nov. 2016, doi: 10.1007/s11416-015-0253-z.
- [14] S. M. Bidoki, S. Jalili, and A. Tajoddin, "PbMMD: A novel policy based multi-process malware detection," *Eng. Appl. Artif. Intell.*, vol. 60, pp. 57–70, Apr. 2017, doi: 10.1016/j.engappai.2016.12.008.
- [15] W. H. Murray, "Enterprise Security Architecture," *Inf. Syst. Secur.*, vol. 6, no. 4, pp. 1–12, Dec. 1998, doi: 10.1201/1086/43299.6.4.19980101/30998.8.
- [16] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, 2013, doi: 10.1016/j.cose.2013.04.004.
- [17] P. L. Pradhan, "An Overview of EDR Serviceability for Security Information and Event Management (SIEM)," *J. Inf. Assur. Secur.*, vol. 21, no. 2, pp. 52–88, Jul. 2026, doi: 10.2478/ias-2026-0004.
- [18] B. G. Raggad, "Security Risk Management," in *Information Security Management*, CRC Press, 2010, pp. 317–390, doi: 10.1201/9781439882634-13.
- [19] J. Boeken, "From compliance to security, responsibility beyond law," *Comput. Law Secur. Rev.*, vol. 52, p. 105926, Apr. 2024, doi: 10.1016/j.clsr.2023.105926.
- [20] D. Ajiga, P. A. Okeleke, S. O. Folorunsho, and C. Ezeigweneme, "Designing Cybersecurity Measures for Enterprise Software Applications to Protect Data Integrity," *Comput. Sci. IT Res. J.*, vol. 5, no. 8, pp. 1920–1941, Aug. 2024, doi: 10.51594/csitrj.v5i8.1451.
- [21] T. K. Damenu and C. Balakrishna, "Cloud Security Risk Management: A Critical Review," in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, IEEE, Sep. 2015, pp. 370–375, doi: 10.1109/NGMAST.2015.25.
- [22] M. Vai *et al.*, "Zero Trust Architecture Approach for Developing Mission Critical Embedded Systems," in *2023 IEEE High Performance Extreme Computing Conference (HPEC)*, IEEE, Sep. 2023, pp. 1–5, doi: 10.1109/HPEC58863.2023.10363531.
- [23] F. A. Qazi, "Study of Zero Trust Architecture for Applications and Network Security," in *2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, 2022, pp. 111–116, doi: 10.1109/HONET56683.2022.10019186.
- [24] N. F. Syed, S. W. Shah, A. Shaghagh, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," 2022, doi: 10.1109/ACCESS.2022.3174679.
- [25] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," 2022, doi: 10.3390/su141811213.
- [26] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, "A Systematic

- Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains,” *Sensors*, vol. 25, no. 19, pp. 1–25, 2025, doi: 10.3390/s25196118.
- [27] N. Asthana, “Identity and Access Management (IAM) Expertise and Organizational Success Stories,” *J. Inf. Syst. Eng. Manag.*, vol. 11, no. 2s, pp. 153–166, Feb. 2026, doi: 10.52783/jisem.v11i2s.14359.
- [28] S. Samtani, H. Chen, M. Kantarcioglu, and B. Thuraisingham, “Explainable Artificial Intelligence for Cyber Threat Intelligence (XAI-CTI),” *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 4, pp. 2149–2150, Jul. 2022, doi: 10.1109/TDSC.2022.3168187.
- [29] Sharjil Iqbal, “NETWORK ATTACK DETECTION BY GROUP SEARCH OPTIMIZATION USING CONVOLUTIONAL DEEP LEARNING MODEL,” *Int. J. Eng. Res. Sci. Technol.*, vol. 22, no. 1, pp. 579–585, February, Feb. 2026, doi: 10.62643/ijerst.2026.v22.n1.pp579-585.
- [30] S. C. Pallaprolu, “Zero-day Attack Identification in Streaming Data: Nearest Neighbor Heuristics and Dynamic Semantic Network Generation in the Spark Eco-system,” University of Maryland, Baltimore County, 2017.
- [31] C.-Y. Chen *et al.*, “IEEE Access Special Section Editorial: Artificial Intelligence in Cybersecurity,” *IEEE Access*, vol. 8, pp. 163329–163333, 2020, doi: 10.1109/ACCESS.2020.3021604.
- [32] M. M. Nair, A. Deshmukh, and A. K. Tyagi, “Artificial Intelligence for Cyber Security,” in *Automated Secure Computing for Next-Generation Systems*, Wiley, 2024, pp. 83–114. doi: 10.1002/9781394213948.ch5.
- [33] I. Bibi, A. Akhunzada, and N. Kumar, “Deep AI-Powered Cyber Threat Analysis in IIoT,” *IEEE Internet Things J.*, vol. 10, no. 9, pp. 7749–7760, May 2023, doi: 10.1109/JIOT.2022.3229722.
- [34] R. K. Kotapati, “AI-Driven Zero Trust and PAM Architectures for Accessible, Inclusive, and Equitable Cybersecurity in Global Enterprise Environments,” in *2026 5th International Conference on Computer Networks, Big Data and IoT (ICCBID)*, IEEE, Jun. 2026, pp. 1136–1141. doi: 10.1109/ICCBID68589.2026.11619744.
- [35] R. K. S. Sulthana, R. P. Krishna, S. G. Naik, and Kavya, “Redefining Trust Boundaries: A Holistic Synthesis of Zero-Trust Architecture Across Emerging Ecosystems,” in *2026 IEEE International Conference on Emerging Synergy Science and Technology (ICESST)*, IEEE, Apr. 2026, pp. 1–5. doi: 10.1109/ICESST69086.2026.11582862.
- [36] S. Qiu and C. Li, “A Supply Chain Finance Access Scheme Under Zero Trust Architecture and Blockchain Technology,” in *2025 21st International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, IEEE, Jul. 2025, pp. 1–9. doi: 10.1109/ICNC-FSKD67701.2025.11198090.
- [37] A. H. A. Alwyn, A. A. M. Adrian, and P. Deepalakshmi, “Create Cloud-Based Access Control Rules Cybersecurity: Applications of AI-Driven Policies and Zero Trust Architecture,” in *2025 International Conference on Electronics and Computing, Communication Networking Automation Technologies (ICEC2NT)*, IEEE, Sep. 2025, pp. 1–6. doi: 10.1109/ICEC2NT65402.2025.11380090.
- [38] T. Sarkorn and K. Chimmancee, “Review on Zero Trust Architecture Apply In Enterprise Next Generation Firewall,” in *2024 8th International Conference on Information Technology (InCIT)*, IEEE, Nov. 2024, pp. 255–260. doi: 10.1109/InCIT63192.2024.10810611.
- [39] S. Al-Tamimi, Q. A. Al-Haija, and K. Alrawashdeh, “Zero-Trust Architecture for Securing Internet of Things (IoT) Networks: A Review,” in *2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/CIEES62939.2024.10811176.
- [40] K. Che and S. Sheng, “Cloud Native Network Security Architecture Strategy under Zero Trust Scenario,” in *2023 IEEE 7th Information Technology and Mechatronics Engineering Conference (ITOEC)*, IEEE, Sep. 2023, pp. 867–871. doi: 10.1109/ITOEC57671.2023.10291357.