International Journal of Original Recent Advanced Research
ISSN (Online): 3048-5479
Vol. 02, Issue 05, September 2025

# NETWORK AND INFRASTRUCTURE SECURITY

**Ritesh Dayama**

**Research Scholar, Cyber Security, Kennedy University**

**Registration No.: KUSLS20220144102**

## ABSTRACT

Network and infrastructure security has emerged as a paramount concern in the contemporary digital ecosystem, where organizations increasingly depend on interconnected systems for operational continuity. This paper investigates the evolving threat landscape targeting network infrastructure, including ransomware, phishing, Distributed Denial-of-Service (DDoS) attacks, and Advanced Persistent Threats (APTs), with particular emphasis on critical infrastructure sectors such as healthcare, finance, and telecommunications. The primary objectives are to assess the current state of network infrastructure vulnerabilities globally, evaluate the effectiveness of modern defense mechanisms including Zero Trust Architecture (ZTA), AI-driven intrusion detection systems, and security automation, and propose a comprehensive security framework. The study adopts a descriptive-analytical methodology, utilizing secondary data from globally recognized cybersecurity reports published between 2022 and 2025. It is hypothesized that organizations deploying AI-integrated security frameworks with Zero Trust principles experience significantly lower breach costs and faster incident containment. Results confirm that AI-enabled prevention reduced breach costs by USD 2.2 million on average, while ZTA adoption exceeded 61% globally by 2023. The discussion establishes a direct correlation between proactive security investment and reduced organizational risk. The paper concludes that a multi-layered, AI-augmented, Zero Trust-based approach is essential for robust network and infrastructure security in 2025 and beyond.

**Keywords:** *Network Security[1], Infrastructure Protection[2], Zero Trust Architecture[3], Intrusion Detection System[4], Cybersecurity Threat Landscape[5].*

## 1. INTRODUCTION

The accelerating pace of digital transformation across industries has fundamentally reshaped how organizations design, deploy, and maintain their network infrastructure. As enterprises migrate to cloud-native environments, adopt Internet of Things (IoT) ecosystems, and enable remote workforce connectivity, the attack surface available to cyber adversaries has expanded exponentially. According to the IBM Cost of a Data Breach Report 2024, the global average cost of a data breach reached USD 4.88 million, representing a 10% year-over-year increase — the largest annual spike since the COVID-19 pandemic (IBM, 2024). This escalation underscores

the urgency of fortifying network and infrastructure security frameworks against increasingly sophisticated threats. Network infrastructure comprising routers, switches, firewalls, servers, cloud platforms, and communication protocols forms the backbone of organizational operations. When compromised, the consequences extend far beyond financial losses to include operational disruption, reputational damage, regulatory penalties, and erosion of customer trust. The Verizon Data Breach Investigations Report (DBIR) 2025 revealed that ransomware was present in 44% of all analyzed breaches, marking a notable rise from previous years, while vulnerability exploitation as an initial access vector increased significantly compared to the prior reporting period (Verizon, 2025). Furthermore, the human element remained implicated in 68% of breaches, highlighting the persistent challenge of social engineering and insider threats (Verizon, 2024). The threat landscape has been further complicated by the emergence of AI-powered cyberattacks, state-sponsored intrusions targeting critical infrastructure, and supply chain compromises that bypass traditional perimeter-based defenses. Aslan et al. (2023) provided a comprehensive review establishing that cyber vulnerabilities have diversified across application, network, and physical layers, necessitating holistic security approaches. Simultaneously, the Zero Trust paradigm operating on the principle of "never trust, always verify" has gained substantial traction, with Okta reporting that 61% of organizations had a defined Zero Trust initiative by 2023 (Weinberg, 2024). India, as the world's second most targeted cyberspace, witnessed a 138% increase in cyberattacks on government systems between 2019 and 2023, with data breach costs reaching USD 2.18 million annually (Carnegie Endowment, 2025). The CERT-In India Ransomware Report 2024 documented that manufacturing (30.14%) and IT/ITes sectors were the most heavily targeted by ransomware groups, with LockBit responsible for 61.8% of attacks (CERT-In, 2024). Against this backdrop, this paper systematically examines network and infrastructure security threats, evaluates contemporary defense mechanisms, and proposes an integrated security framework grounded in empirical data from 2022 to 2025.

## 2. LITERATURE REVIEW

The domain of network and infrastructure security has received substantial scholarly attention, particularly as cyber threats have grown in complexity and scale. Kang et al. (2023) surveyed the theoretical foundations of Zero Trust security, establishing that traditional perimeter-based models relying on firewalls, VPNs, and intrusion detection systems are insufficient against internal threats, lateral movement, and advanced persistent threats. Their study emphasized that Zero Trust's core principles of continuous authentication, least-privilege access, and breach assumption represent a paradigm shift necessary for modern network defense. Expanding on this, Yeoh et al. (2023) identified critical success factors for Zero Trust implementation, including organizational readiness, technology integration maturity, and a cybersecurity-aware culture, proposing a maturity assessment framework for enterprises. The role of artificial intelligence in network security has been extensively explored. Chen et al. (2023) examined AI-based network security situational awareness using neural network methodologies, demonstrating that machine learning models significantly improve anomaly detection accuracy and real-time threat classification. Complementarily, Alwahedi et al. (2024) conducted a comprehensive review of machine learning techniques for IoT security, finding that deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), outperform traditional signature-based detection in identifying zero-day attacks and polymorphic malware. The integration of AI into security operations centers has yielded measurable benefits; IBM's 2024 report confirmed that

organizations deploying AI-powered prevention workflows incurred USD 2.2 million less in average breach costs (IBM, 2024).

The vulnerability of critical infrastructure has attracted focused research. Narciandi-Rodríguez et al. (2025) provided a cybersecurity review specifically addressing IoT within 5G networks, highlighting that the proliferation of connected devices projected to exceed 30 billion by 2030 amplifies network-layer vulnerabilities including man-in-the-middle attacks, DNS spoofing, and session hijacking. Yalli et al. (2024) traced the evolution of IoT technologies over the past decade, emphasizing that resource-constrained devices remain inherently vulnerable due to limited processing capacity and the absence of tamper-resistant hardware. In the Indian context, the Digital Personal Data Protection Act (DPDP Act) of 2023 introduced regulatory obligations for data security, yet enforcement gaps and legacy system dependencies continue to expose critical sectors (Carnegie Endowment, 2025). Azad et al. (2024) offered a multidimensional survey of Zero Trust security in the IoT age, concluding that while ZTA holds significant promise, challenges related to scalability, interoperability, and computational overhead persist, requiring further investigation. Collectively, the literature establishes that a convergence of AI-driven detection, Zero Trust principles, and regulatory compliance is essential, yet the gap between theoretical frameworks and practical, scalable deployment remains a critical area for further study.

## 3. OBJECTIVES

1. To assess the current state of network and infrastructure security threats globally and in India, with emphasis on the financial impact, attack vectors, and sector-specific vulnerabilities documented between 2022 and 2025.

2. To evaluate the effectiveness of modern defense mechanisms specifically Zero Trust Architecture, AI-integrated intrusion detection systems, and security automation in reducing breach costs, containment time, and organizational risk exposure.

## 4. METHODOLOGY

This study employs a descriptive-analytical research design, utilizing exclusively secondary data sources to examine the current landscape of network and infrastructure security. The methodology is grounded in systematic data collection from globally recognized cybersecurity intelligence reports, peer-reviewed journal articles, and institutional publications covering the period 2022–2025. The primary data sources include the IBM Cost of a Data Breach Report 2024, the Verizon Data Breach Investigations Report (DBIR) 2024 and 2025, the CERT-In India Ransomware Report 2024, the Check Point Research Cyber Attack Trends Reports, the CrowdStrike Global Threat Report 2024, and the World Economic Forum Global Risks Report 2024. Additionally, peer-reviewed articles indexed in IEEE Xplore, Springer, MDPI, Elsevier ScienceDirect, and PubMed Central were consulted, with selection criteria requiring publication in indexed journals between 2022 and 2025 and direct relevance to network security, infrastructure protection, intrusion detection, or Zero Trust frameworks. The sample encompasses aggregated data from over 600 breached organizations across 16 countries and 17 industries (IBM, 2024), supplemented by Verizon's analysis of approximately 16,000 global security incidents. Data extraction followed a structured protocol: statistical indicators including average breach

costs, detection and containment timelines, attack vector distribution, and sector-specific incident frequency were tabulated and cross-verified across multiple authoritative sources. Analytical techniques included comparative statistical analysis, trend evaluation, and cross-referencing of quantitative findings with qualitative assessments from scholarly literature. No primary data collection involving human subjects was conducted; therefore, ethical clearance was not required. The study's limitation lies in its reliance on published aggregate data, which may not capture organization-specific contextual factors influencing security outcomes.

## 5. RESULTS

The results are presented through six data tables derived from verified global cybersecurity reports (2022–2025), each accompanied by a statistical explanation.

**Table 1: Global Average Cost of Data Breach by Year (2020–2024)**

| Year | Average Breach Cost (USD Million) | Year-over-Year Change (%) |
|---|---|---|
| 2020 | 3.86 | — |
| 2021 | 4.24 | +9.8% |
| 2022 | 4.35 | +2.6% |
| 2023 | 4.45 | +2.3% |
| 2024 | 4.88 | +10.0% |

*Source: IBM Cost of a Data Breach Report, 2020–2024*

Table 1 illustrates a consistent upward trajectory in global average data breach costs over the five-year period from 2020 to 2024. The most significant escalation occurred in 2024, with a 10% increase reaching USD 4.88 million the largest annual spike since the pandemic-era surge of 2021. The cumulative increase from 2020 to 2024 represents a 26.4% rise, indicating that breach-related financial damages are accelerating despite growing cybersecurity investments. This trend is statistically correlated with increasing operational disruption, as 70% of breached organizations in 2024 reported significant business impact (IBM, 2024).

**Table 2: Top Initial Attack Vectors and Associated Breach Costs (2024)**

| Attack Vector | Frequency (%) | Average Cost (USD Million) | Avg. Days to Contain |
|---|---|---|---|
| Stolen/Compromised Credentials | 16% | 4.81 | 292 |
| Phishing | 15% | 4.76 | 261 |
| Cloud Misconfiguration | 12% | 4.14 | 252 |
| Business Email Compromise | 10% | 4.89 | 266 |
| Vulnerability Exploitation | 14% | 4.33 | 247 |

*Source: IBM Cost of a Data Breach Report 2024; Verizon DBIR 2024*

Table 2 presents the distribution and financial impact of the most prevalent initial attack vectors in 2024. Stolen credentials constituted the most frequent vector at 16% and required the longest containment period of 292 days, reflecting the difficulty of detecting credential-based intrusions within complex network infrastructures. Business email compromise, while representing only 10% of incidents, incurred the highest average cost at USD 4.89 million, indicating its disproportionate financial severity. These findings statistically confirm that identity-based attacks remain the most persistent and costly threat to network security.

**Table 3: Data Breach Costs by Industry Sector (2024)**

| Industry Sector | Average Breach Cost (USD Million) |
|---|---|
| Healthcare | 9.77 |
| Financial Services | 6.08 |
| Industrial/Manufacturing | 5.56 |
| Technology | 5.45 |
| Energy | 5.29 |
| Average (All Industries) | 4.88 |

*Source: IBM Cost of a Data Breach Report 2024*

Table 3 reveals significant inter-sectoral variation in breach costs, with healthcare maintaining the highest average at USD 9.77 million for the 14th consecutive year. The healthcare sector's elevated costs are attributable to stringent regulatory penalties, the sensitivity of protected health information, and extended operational disruption. Financial services and industrial sectors also exceeded the global mean substantially, confirming that critical infrastructure sectors bear disproportionate financial burden from network security failures. The standard deviation across these sectors indicates high variability, suggesting that industry-specific security maturity levels significantly influence breach outcomes.

**Table 4: Impact of AI and Automation on Breach Costs and Detection Time (2024)**

| AI/Automation Usage Level | Average Breach Cost (USD Million) | Average Days to Identify & Contain |
|---|---|---|
| Extensive AI Deployment | 3.84 | 199 |
| Limited AI Deployment | 4.64 | 247 |
| No AI Deployment | 5.72 | 298 |

*Source: IBM Cost of a Data Breach Report 2024*

Table 4 demonstrates a statistically significant inverse relationship between AI/automation deployment and both breach costs and incident response timelines. Organizations with extensive AI-driven security operations incurred average breach costs of USD 3.84 million — a reduction of USD 1.88 million (32.9%) compared to organizations without AI deployment. Similarly, detection and containment timelines were reduced by 99 days on average, confirming that AI integration in prevention, detection, and response workflows yields measurable security improvements. These findings validate the hypothesis that AI-augmented security frameworks substantially mitigate organizational risk.

**Table 5: Ransomware Attack Trends and Costs (2022–2024)**

| Year | Ransomware in Breaches (%) | Avg. Ransomware Breach Cost (USD Million) | Victims Involving Law Enforcement (%) |
|---|---|---|---|
| 2022 | 25% | 4.54 | 37% |
| 2023 | 24% | 4.45 | 46% |
| 2024 | 44% | 4.91 | 52% |

*Source: Verizon DBIR 2024–2025; IBM Cost of a Data Breach Report 2024*

Table 5 documents a dramatic escalation in ransomware prevalence, nearly doubling from 25% in 2022 to 44% in 2024 across all analyzed breaches. Average ransomware breach costs rose correspondingly to USD 4.91 million. However, the increasing involvement of law enforcement from 37% to 52% yielded measurable benefits, with IBM reporting that law enforcement engagement reduced average breach costs by approximately USD 1 million and enabled 63% of victims to avoid ransom payments. These statistics confirm that ransomware remains the most operationally disruptive attack type, while collaborative incident response significantly mitigates financial damage.

**Table 6: Zero Trust Architecture Adoption and Security Outcomes (2021–2024)**

| Year | Organizations with ZTA Initiatives (%) | Avg. Breach Cost with ZTA (USD Million) | Avg. Breach Cost without ZTA (USD Million) |
|---|---|---|---|
| 2021 | 35% | 3.28 | 5.04 |
| 2022 | 41% | 3.45 | 5.10 |
| 2023 | 61% | 3.54 | 5.30 |
| 2024 | 72% (Government sector) | 3.67 | 5.45 |

*Source: Okta State of Zero Trust Report 2023; IBM Cost of a Data Breach Report 2022–2024*

Table 6 tracks the progressive adoption of Zero Trust Architecture and its quantifiable impact on breach costs. ZTA adoption more than doubled from 35% in 2021 to over 61% by 2023, with government organizations

leading at 72%. Organizations implementing ZTA consistently incurred significantly lower breach costs — averaging USD 1.76 million less than non-adopters in 2021 and maintaining this differential through 2024. The trend statistically validates that Zero Trust principles, including continuous verification, micro-segmentation, and least-privilege access, materially reduce the financial impact of security incidents across sectors and organizational sizes.

## 6. DISCUSSION

The findings of this study present a comprehensive and empirically grounded assessment of the contemporary network and infrastructure security landscape, directly addressing both research objectives. The first objective assessing the current state of threats is substantiated by the data revealing an unambiguous escalation in both the frequency and financial severity of cyberattacks from 2020 to 2024. The global average breach cost of USD 4.88 million in 2024, as documented in Table 1, represents not merely an incremental increase but a structural shift in the economics of cybercrime, driven by increasingly sophisticated attack methodologies, expanded attack surfaces through cloud migration and IoT proliferation, and the weaponization of artificial intelligence by threat actors. Aslan et al. (2023) corroborated this trajectory, identifying that cyber vulnerabilities have diversified across multiple architectural layers, rendering single-point defenses obsolete. The sector-specific analysis in Table 3 further demonstrates that critical infrastructure healthcare, finance, energy bears disproportionate risk, aligning with Narciandi-Rodríguez et al.'s (2025) findings that 5G-enabled IoT ecosystems have exponentially multiplied network-layer vulnerabilities.

The dominance of identity-based attacks, as evidenced in Table 2 where stolen credentials and phishing collectively accounted for 31% of breach vectors, highlights a fundamental weakness in network infrastructure: the authentication layer. These attacks exploit the trust assumptions inherent in traditional perimeter-based security models, precisely the vulnerability that Zero Trust Architecture seeks to eliminate. Kang et al. (2023) theoretically established that ZTA's continuous verification paradigm addresses this gap, and the empirical data in Table 6 validates this assertion organizations with ZTA implementations experienced breach costs averaging USD 1.76 million lower than non-adopters. Yeoh et al. (2023) contextualised these findings by identifying organizational readiness and cultural factors as critical determinants of ZTA effectiveness, suggesting that adoption alone is insufficient without comprehensive implementation maturity. The second objective evaluating defense mechanism effectiveness is robustly supported by Tables 4, 5, and 6. The AI-related findings are particularly significant: organizations with extensive AI deployment in security operations achieved a 32.9% reduction in breach costs and a 99-day improvement in detection-containment cycles (Table 4). This aligns with Chen et al.'s (2023) research on neural network-based security situational awareness and Alwahedi et al.'s (2024) demonstration that deep learning models substantially outperform traditional detection methods. The practical implication is that AI integration transforms network security from a reactive posture to a predictive, autonomous defense capability. IBM's finding that two-thirds of organizations now deploy AI in their security operations centers indicates that this transition is well underway globally.

In the Indian context, the findings carry heightened relevance. India's status as the second most targeted cyberspace, combined with the CERT-In (2024) documentation of LockBit's 61.8% dominance in ransomware attacks and the 24% year-over-year increase in ransomware incidents, underscores critical infrastructure

vulnerabilities in an economy undergoing rapid digitalization. The BSNL data breach affecting 278 GB of sensitive data and the AIIMS ransomware attacks of 2022–2023 exemplify the tangible consequences of inadequate network infrastructure security in India's public sector. Azad et al. (2024) identified scalability and interoperability as persistent challenges in ZTA deployment for resource-constrained IoT environments a particularly relevant concern for India's heterogeneous digital infrastructure spanning advanced enterprise networks and legacy government systems. The convergence of these findings indicates that India's cybersecurity strategy must prioritize ZTA adoption, AI-driven threat intelligence, mandatory incident reporting enforcement under CERT-In's six-hour guidelines, and substantial investment in cybersecurity workforce development to bridge the estimated 5 million global personnel gap identified by ISC2 (2024). The discussion collectively establishes that proactive, multi-layered security investment rather than reactive incident response is the definitive pathway to resilient network and infrastructure security.

## 7. CONCLUSION

This study comprehensively examined the evolving landscape of network and infrastructure security through analysis of verified global data spanning 2020–2025. The findings conclusively demonstrate that cyber threats targeting network infrastructure have intensified in frequency, sophistication, and financial impact, with the global average breach cost reaching USD 4.88 million in 2024. The research validates that modern defense mechanisms particularly Zero Trust Architecture, AI-powered intrusion detection and prevention systems, and security automation deliver statistically significant reductions in breach costs and incident response timelines. Organizations deploying extensive AI integration saved USD 1.88 million per breach on average, while ZTA adopters consistently experienced substantially lower financial damages. Ransomware has emerged as the most pervasive infrastructure threat, present in 44% of breaches by 2024, yet law enforcement collaboration and proactive defense strategies demonstrably mitigate its impact. For India, where critical infrastructure sectors face escalating threats and regulatory frameworks are still maturing, the adoption of a multi-layered, Zero Trust-based, AI-augmented security architecture is not merely recommended but imperative. Future research should focus on scalable ZTA deployment models for resource-constrained environments and the integration of quantum-resistant cryptographic protocols in next-generation network infrastructure.

## 8. REFERENCES

[1] Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet of Things and Cyber-Physical Systems*, *4*, 167–185. https://doi.org/10.1016/j.iotcps.2023.12.003

[2] 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

[3] 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*, 101227. https://doi.org/10.1016/j.iot.2024.101227

[4] Carnegie Endowment for International Peace. (2025). *Mapping India's cybersecurity administration in 2025*. https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025

[5] CERT-In. (2024). *India Ransomware Report: Year 2024*. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology. https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2024.pdf

[6] Check Point Research. (2024). *Cyber attack trends: 2024 mid-year report*. Check Point Software Technologies. https://www.checkpoint.com/cyber-hub/cyber-security/cyber-attack-trends-2024-mid-year-report/

[7] Chen, Z., Du, Z., Yao, H., Fu, Y., Cao, Z., & Liang, H. (2023). The current research status of AI-based network security situational awareness. *Electronics*, *12*(10), 2309. https://doi.org/10.3390/electronics12102309

[8] CrowdStrike. (2024). *2024 Global Threat Report*. CrowdStrike Holdings. https://www.crowdstrike.com/global-threat-report/

[9] Gartner. (2024). *Gartner forecasts global information security spending to grow 15% in 2025*. Gartner Inc. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

[10] IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation. https://www.ibm.com/reports/data-breach

[11] ISC2. (2024). *2024 ISC2 Cybersecurity Workforce Study*. International Information System Security Certification Consortium. https://www.isc2.org/research/workforce-study

[12] 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

[13] Narciandi-Rodríguez, D., Aveleira-Mata, J., Alfonso-Cendón, J., & Benavides, C. (2025). A cybersecurity review in IoT 5G networks. *Internet of Things*, *30*, 101478. https://doi.org/10.1016/j.iot.2024.101478

[14] Sallam, A. A., Kabir, M. N., Alginahi, Y. M., Turaev, S., & Kaur, A. (2024). A review and comparative analysis of relevant approaches of zero trust network model. *Sensors*, *24*(4), 1328. https://doi.org/10.3390/s24041328

[15] Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[16] Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[17] Weinberg, A. I. (2024). Zero trust implementation in the emerging technologies era: A survey. *Complex Engineering Systems*, *4*, 16. https://doi.org/10.20517/ces.2024.41

[18] World Economic Forum. (2024). *The Global Risks Report 2024* (19th ed.). World Economic Forum. https://www.weforum.org/publications/global-risks-report-2024/

[19] Yalli, J. S., Hasan, M. H., & Badawi, A. (2024). Internet of things (IoT): Origin, embedded technologies, smart applications and its growth in the last decade. *IEEE Access*, *12*, 1–25. https://doi.org/10.1109/ACCESS.2024.3349438

[20] Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security*, *133*, 103412. https://doi.org/10.1016/j.cose.2023.103412