INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

# Advanced Information Security and Assurance: A Literature Review of Zero Trust Architecture, Artificial Intelligence, and Cybersecurity Resilience

**Celinne Atienza Mendez, Dr. Reagan Ricafort**

**AMA University Quezon City, Philippines**

**DOI: https://doi.org/10.51583/IJLTEMAS.2026.150600161**

**Received: 02 July 2026; Accepted: 07 July 2026; Published: 18 July 2026**

## ABSTRACT

The quick uptake of cloud computing, artificial intelligence (AI), Internet of Things (IoT), and hybrid workplace solutions has changed the cybersecurity needs in a way that renders the traditional notion of perimeter defense inefficient in addressing sophisticated attack scenarios such as ransomware, insider threats, and advanced persistent threats (APTs). This literature review analyzes advancements in the field of Advanced Information Security and Assurance from 2016 to 2026.

Key advancements include NIST SP 800-207 published in 2020, widespread use of Zero Trust Architecture (ZTA), and incorporation of AI into security analytics. The reviewed sources show that Zero Trust drastically minimizes attack surfaces using continuous authentication, least-privilege access, and microsegmentation. Also, AI is beneficial in improving threat detection through predictive analytics, behavioral anomalies detection, and automation of the incident response process.

On the other hand, AI also poses emerging risks such as adversarial machine learning, automated API reconnaissance, AI phishing scams, and intelligent malware. Additionally, cyber resilience, explainable AI, and adaptive governance are the identified research areas important for protecting future digital infrastructures. While significant advances have been made, there are still many challenges related to complexity, interoperability, staffing shortage, privacy, and governance.

**Keywords—** information security, cybersecurity assurance, zero trust architecture, artificial intelligence, cloud security, cyber resilience

## INTRODUCTION

Indeed, today, information security is among the major concerns of companies that conduct business online. With the increased use of cloud computing, mobility, IoT technologies, and distributed information systems, the attack surface for hackers increases. At the same time, attacks have become much more sophisticated, which causes financial and operational disruptions, as well as significant reputational damage.

Traditionally, information security has concentrated on the protection of the networks of organizations through the use of firewall and other perimeters of defense like intrusion prevention systems. However, today's threat landscape requires new approaches that are not effective enough when dealing with remote work and cloud-native environment and cross-domain information sharing. According to recent studies, the Zero Trust Architecture (ZTA) becomes one of the key trends in the field of cybersecurity based on the principle of "never trust, always verify."

This literature review will discuss important advancements in the sphere of advanced information security and assurance within 2016-2026 years. Security assurance approaches, Zero Trust models, artificial intelligence technologies used in cybersecurity, cloud security problems, and cyber resilience approaches will be considered.

## BACKGROUND LITERATURE

Information security is the protection of information assets from any form of unauthorized access, disclosure, modification, disruption, or destruction. Information assurance takes the security measures further by guaranteeing the reliability, resilience, and compliance of information systems.

Today's security assurance focuses on the continuous assessment of security controls, risk management processes, and organizational governance structures. Security assurance frameworks help the organization demonstrate its compliance with legal and industry standards while finding out about the vulnerabilities that may be exploited by others. The recent literature defines System Security Assurance (SSA) as a methodology for the assessment of the trustworthiness of an information system in terms of security standards, legal obligations, and best practices.

Due to the growing complexity of information systems, security assurance has become a multidisciplinary domain.

Nowadays, information security and assurance have become integral parts of the digital infrastructure due to the increasing use of connected systems, cloud computing, and other data-driven technologies. The old models of security are not enough to cope with the current situation because they cannot provide proper protection from sophisticated threats. As a result, new, more flexible, intelligent and resilient approaches should be used in order to ensure continuous monitoring, detection, and response to different threats.

One of the trends in the area is the implementation of Zero Trust Architecture. It is a security model that is based on the concept of "never trust, always verify," which means that there is no trust and all requests for access are continuously verified and checked regardless of their origin. In other words, Zero Trust Architecture ensures that the attacks cannot use the lateral movement and increases the level of protection from both internal and external sources of threat. Literature indicates that this framework is very effective when it is used in the cloud-based or hybrid environment (Rose et al., 2020).

Alongside, Artificial Intelligence (AI) has become an important part of cybersecurity and information assurance. AI technologies, such as machine learning, deep learning, and behavioral analysis, are applied for detection of anomalies, forecasting cyber attacks, and automated incident responses. AI-based security solutions allow analyzing huge amounts of data in real-time mode, thus, enabling a quicker detection of cyber threats compared to rule-based ones. However, the academic papers also highlight certain issues such as adversarial attacks on AI models, data biases, and the need for the explainability of AI in security decision-making.

One of the key ideas of modern cyber security is cybersecurity resilience. It refers to the ability of an organisation to prepare for, respond to, recover from and adapt to cyber incidents. Contrary to conventional cybersecurity solutions that are concerned mostly about prevention of cyber incidents, resilience assumes a continuity of operations even when cyber incidents occur. Cybersecurity resilience has several components, such as incident response, disaster recovery planning, the availability of redundancy, and ongoing risk assessments. According to the researchers, cybersecurity resilience can help reduce operational disruption and financial damages due to cyber incidents.

The use of zero trust, AI and resilience principles are a sign of the times, highlighting a paradigm shift in cybersecurity from a static defence posture to intelligent security ecosystems. In the modern interpretation of Advanced Information Security and Assurance, governance, risk management, compliance, culture, as well as technology, are all part of the picture. There are several frameworks like ISO/IEC 27001, NIST Cybersecurity Framework, and Zero Trust recommendations that offer practical methods for developing a framework like this one.

Additionally, human elements are still the main vulnerability in any cybersecurity system according to the literature overview. Even though there are many advanced security tools, social engineering, phishing, and insider threats keep using people's ignorance or mistakes. Consequently, it is important for an organization to combine its technological tools with ongoing user training and policy enforcement.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

In summary, it can be stated that the future of information security and assurance will be in integrated, adaptive, and intelligent security frameworks. It requires the combination of zero trust approach, AI-powered security systems, and resilience.

The move from perimeter-based cybersecurity to the identity-centric security framework is one of the most noteworthy advancements made in information assurance in recent years. Up until 2020, Zero Trust principles were largely referred to as design paradigms. Nonetheless, with the emergence of NIST Special Publication 800-207 (Rose et al., 2020), an official Zero Trust Architecture (ZTA) framework was developed, highlighting four key Zero Trust tenets, such as continuous verification, least-privilege access, policy enforcement, and continuous monitoring. From that point onward, ZTA became the reference architecture used for cloud-native systems, hybrid environments, critical infrastructure, and enterprise cybersecurity.
According to recent systematic literature reviews, the use of the Zero Trust approach has been expanding rapidly within the domains of healthcare, finance, manufacturing, and governmental organizations, due to the inability of perimeter-based security to provide adequate protection in distributed digital environments (Arruda et al., 2023; Kang et al., 2023; Mushtaq et al., 2025). Instead of trusting the internal user by default, ZTA continuously assesses the identity of the user, the status of their device, context-based risks, and behavior patterns before providing any access.

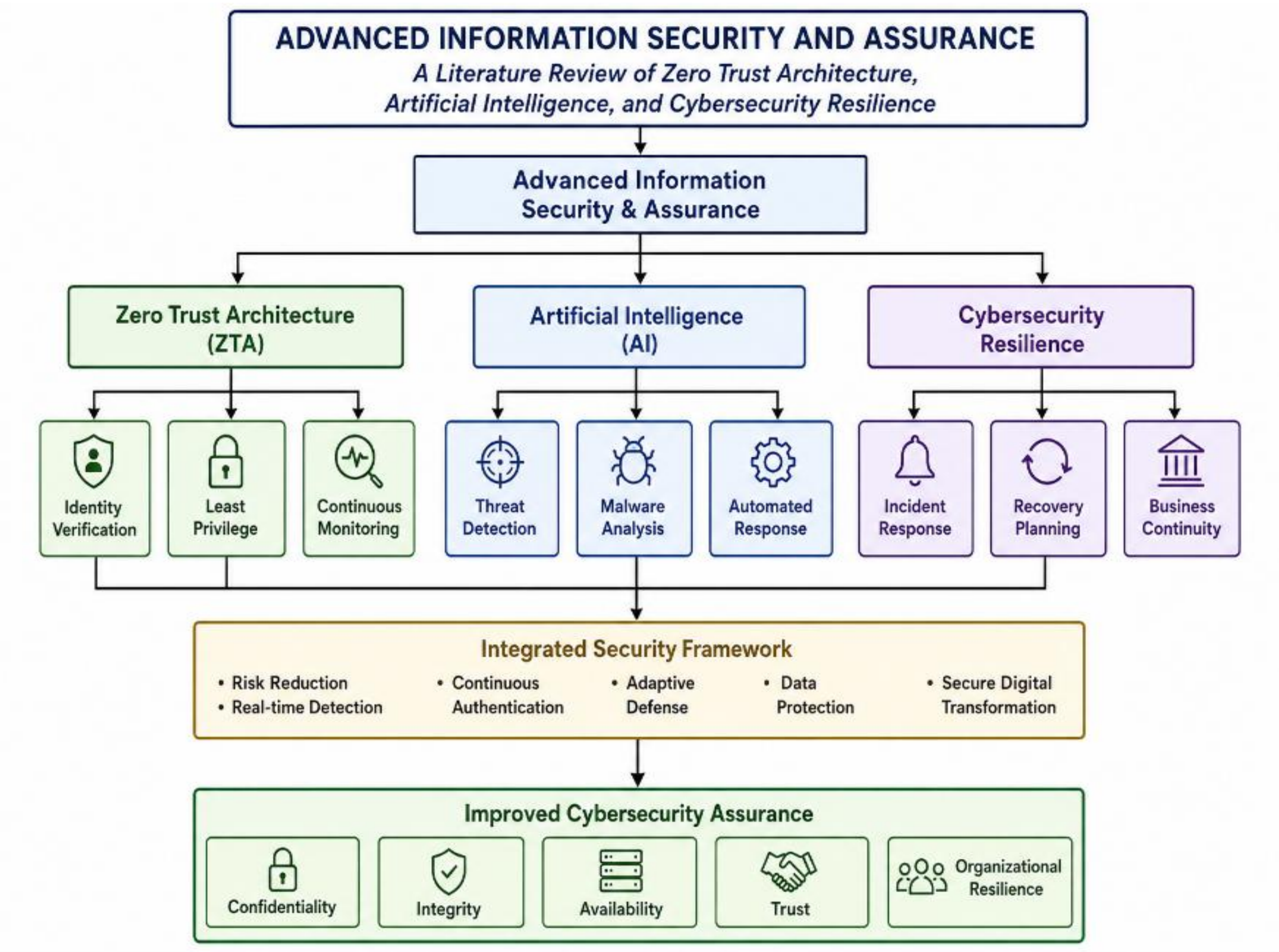


Figure 1. Conceptual Framework of Advanced Information Security and Assurance

| Year | Milestone | Significance |
|---|---|---|
| 2016 | AI begins widespread application in intrusion detection (Buczak & Guven) | Machine learning improves anomaly detection beyond signature-based systems. |

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

| | | |
|---|---|---|
| 2019 | Rapid enterprise cloud migration | Identity-based security becomes increasingly necessary. |
| 2020 | **NIST SP 800-207** published | Standardized Zero Trust Architecture principles. |
| 2021–2023 | Expansion of XDR, SOAR, and AI-powered security operations | Increased automation in detection and response. |
| 2023–2025 | Growth of Explainable AI (XAI) and Zero Trust implementation studies | Greater emphasis on trustworthy AI and governance. |
| 2025–2026 | Increased concern regarding AI-enabled cyber attacks | Focus shifts toward AI governance, adversarial AI, and cyber resilience. |

Table 1. Major Developments in Advanced Information Security and Assurance (2016–2026)

## METHODOLOGY

A narrative literature review is adopted for the current study as an approach to analyze the body of research that has been developed from 2016 to 2026.

Literature selection for this paper entailed:

1. Peer-reviewed journal articles and conference papers.

2.Literature reviews on cybersecurity and information assurance.

3.Literature on Zero Trust Architecture, artificial intelligence-based cybersecurity, cloud security, and cyber-resilience.

4. Literature published from 2016 to 2026.

This selected literature has been synthesized through thematic analysis.

## LITERATURE REVIEW

### Evolution of Information Security and Assurance

The cybersecurity environment in the current context is very different from conventional security environments. Businesses nowadays tend to work in an ecosystem of the digital kind in which employees, apps, devices, and data are situated in various locations.

According to recent findings, the conventional model of perimeter security cannot anymore help solve the challenges of the modern era of cybersecurity. The emergence of remote access, cloud computing, and integration with third parties has required new models of security that emphasize identity authentication, continuous monitoring, and risk management.

In this case, information assurance has moved from security controls implementation to security validation activities.

### Zero Trust Architecture

Among the recent advances in cybersecurity, Zero Trust Architecture occupies a prominent position. While conventional approaches to cybersecurity rely on an assumption of trust within organizational networks, ZTA operates under the premise that there is no user, device, or application that should be considered trusted.

One of the main aspects of Zero Trust architecture lies in continuous validation through authentication, authorization, access control by least privilege, and monitoring. There is evidence that ZTA provides an effective

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

solution for potential threats connected to cloud computing, insider threats, working remotely, and distributed systems.

Systematic literature review reveals that ZTA gains popularity in healthcare, cloud computing, Internet of Things (IoT), industrial systems, enterprise networks, and artificial intelligence environments. Authentication, authorization, and access control have become the most widespread elements of ZTA.

Additionally, current research shows that more work needs to be done on orchestration, auditing, and environmental awareness.

It is evident from the reviewed literature that Zero Trust Architecture is fundamentally different from the existing approaches to network security. Unlike the existing approaches that by default treat all users accessing the corporate network with already authenticated credentials as trustworthy, Zero Trust treats each user's requests as potentially dangerous regardless of their origin. It was codified into a standard in NIST SP 800-207 (Rose et al., 2020) that specifies four principles of Zero Trust, which include continuous authentication, policy enforcement, least privilege access, and micro-segmentation.

Comparative analyses in the literature prove that Zero Trust is more effective in preventing insider threats, password breach, and lateral movements compared to the existing perimeter defenses since the decision about authorizing the user does not depend only on the initial login. At the same time, the literature reports implementation challenges that include difficulties associated with the integration of legacy systems, identity management, policy orchestration, and organizational readiness (Mushtaq et al., 2025; Gambo & Almulhem, 2025). Thus, the literature proves that Zero Trust requires a paradigm shift in the organization.

**Artificial Intelligence in Cybersecurity Assurance**

Artificial Intelligence has proved itself to be an essential element of cutting-edge cybersecurity tools. AI provides assistance in such processes as threat detection, vulnerability analysis, anomaly detection, incident response, and risk prediction.

According to a systematic literature review carried out recently, AI substantially increases security assurance due to automatic analysis of big data sets and recognition of patterns that would remain unnoticed for humans. AI-based technology helps increase the accuracy of threat detection and enables a faster response to threats.

Machine learning techniques have been found effective in detecting zero-day attacks, malware strains, phishing incidents, and network anomalies. In addition, AI-enabled platforms provide security analysis in digital environment through continuous monitoring and risk assessment.

Nonetheless, experts point out that there are certain problems associated with AI applications, such as issues of algorithmic bias, explainability, adversarial attacks, and privacy concerns. Explainable Artificial Intelligence (XAI) has turned into one of the key directions of scientific studies aiming at increasing the reliability of AI-driven cybersecurity solutions.

Literature review indicates that Artificial Intelligence is used as a two-edged sword in cybersecurity. On one hand, AI facilitates predictive threat detection using behavioral analytics, anomaly detection, malware classification, SOAR (Security Orchestration, Automation and Response), and risk scoring continuously. Network traffic, endpoint telemetry, authentication logs, and user behavior are analyzed using machine learning to detect unknown attacks that cannot be detected with signature-based systems (Buczak & Guven, 2016; Wen et al., 2025).

On the other hand, it is clear that today's attackers use AI to automatically perform reconnaissance and API probing, generate phishing emails, conduct social engineering campaigns, obfuscate malware, and discover vulnerabilities. With generative AI, highly personalized attacks on the organization are possible as they will bypass all existing detection technologies. Adversarial machine learning uses manipulation of training data or

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

evasion of classifiers for attacks on AI models. It is obvious that AI works as an offense and defense at once; therefore, organizations should apply explainable AI and governance.

**Cloud Security and Information Assurance**

Cloud computing has revolutionized the IT infrastructure of organizations due to its scalability and flexibility. However, cloud computing creates numerous security issues concerning identity management, data protection, multi-tenancy, and compliance issues.

Studies suggest that cloud security is becoming more identity-centric as it utilizes encryption technologies, continuous monitoring techniques, and zero trust approach. Organizations using cloud native systems need to have appropriate governance systems for ensuring secure access and data protection.

Assurance in cloud computing involves regular risk assessment and security audit processes.

**Cyber Resilience and Organizational Security**

Resilience includes more than just prevention as the key consideration here is how resilient the organization is in terms of anticipating, enduring, recovering from, and adapting to cyber-attacks.

Some recent research indicates that resilience-based security approaches include not only cybersecurity measures but also business continuity planning, disaster recovery, and corporate governance considerations. Cyber resilience cannot be achieved without coordination between technical staff, management, and regulators.

The growing number of ransomware attacks and supply chain attacks shows the significance of resilience-based security approaches.

**Emerging Challenges**

However, while there have been technological developments in advanced information security and assurance, numerous challenges still exist.

**Skill Gaps**

There is an ongoing skill gap problem in the cybersecurity industry where organizations lack competent individuals to handle their complex security environment.

**AI Threats**

While artificial intelligence can enhance cybersecurity, attackers make use of AI technologies to automatically execute their activities including recon, phishing attacks, malware creation, and social engineering attacks.

**Challenges in Implementing Zero Trust**

Implementing Zero Trust may necessitate extensive change within the organization. Several studies and practitioner dialogues show that implementing Zero Trust comprehensively is challenging for organizations.

**Compliance Requirements**

Firms need to continuously evolve in terms of compliance with regulatory requirements.

## DISCUSSION

According to the literature, there have been great advancements in the field of information security and assurance within the last decade. Classical models of security mainly relied on perimeter security while modern ones are centered on identity-centric security, continuous authentication and resiliency.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue VI, June 2026

Zero Trust Architecture can be seen as a revolutionary step in cybersecurity practices. Enforcing Continuous Authentication and Least-Privilege Access is aligned with the security requirements of cloud-based, distributed systems. There is clearly a trend from perimeter-based security towards identity-based security ecosystems, as seen in the literature. This progress has been further amplified by the introduction of NIST SP 800-207 in 2020, which laid down standard principles of Zero Trust for continuous authentication and least-privilege access. At the same time, the role of AI in cybersecurity has moved from detection to prediction of threat intelligence via behavior analysis and automation techniques. However, at the same time, AI has also grown increasingly harmful to the cyber ecosystem with the use of API reconnaissance, adversarial machine learning, intelligent malware, and phishing attacks using AI. So, the future of AI's effectiveness in cybersecurity will require more than just technology; it will demand governance and cyber resilience strategies as well.

Combining AI and Zero Trust is a promising way for increasing the level of security assurance. But adequate governance and human-in-the-loop method must be implemented to counter the new challenges posed by automation.

Cybersecurity strategies of the future will probably integrate adaptive architectures, AI-driven analytics, resilient frameworks and risk-oriented governance methods.

The literature shows that there have been tremendous developments in the area of information security and assurance in the past decade. The conventional model of information security was largely dependent upon perimeter security systems based on the premise that all users and devices were reliable when present in the corporate network. But with the widespread adoption of cloud technology, mobile computing, remote workforces, and IoT, such an approach has become outdated and inefficient. The modern cybersecurity framework has shifted its focus towards identity-based security.

One of the major advancements in this area is Zero Trust Architecture (ZTA), which is founded on the concept of “never trust, always verify.” In contrast to the assumption of trust dependent on the network’s physical location, Zero Trust demands continuous verification of users, devices, applications, and workloads before allowing access to organizational assets. Least-privilege access, micro-segmentation, multi-factor authentication (MFA), continuous monitoring, and risk-based access control are some of the key principles of Zero Trust architecture, which greatly minimize the attack surface area and make it impossible for attackers to move laterally once they breach the system. NIST has introduced these ideas in the NIST Special Publication 800-207 (Rose et al., 2020).

Just like cloud computing and machine learning, Artificial Intelligence (AI) has greatly revolutionized the field of cybersecurity through improved threat detection and reaction speed. AI systems have the ability to analyze vast amounts of data from network traffic, user activities, and systems logs in order to detect suspicious activities. In contrast with signature-based detection techniques, AI systems are able to detect previously unseen threats, such as zero day attacks and advanced persistent threats (APTs) due to their capability to detect abnormal behaviors. This includes predictive analysis, automated malware classification, phishing detection, vulnerability management, and Security Orchestration, Automation, and Response (SOAR).

Another interesting approach to improving cybersecurity is the combination of AI with Zero Trust Architecture. Zero Trust architecture is characterized by continuous trust evaluation and dynamic access control. The combination of Zero Trust Architecture and AI allows for adaptive authentication, dynamic risk scoring, intelligent access decisions, and policy enforcement, which allows an organization to continuously assess trust and react to emerging threats. However, according to researchers, the use of AI technology should complement and not replace human knowledge. Indeed, human supervision is crucial for validation, error correction, transparency, and avoidance of bias and manipulation in algorithms.

Other topics of great interest recently have been related to the cybersecurity resilience concept. Cybersecurity resilience is more than just about prevention—it's about making sure that the organization can prepare for, respond to, cope with and withstand the impact of a cyber incident. It incorporates the concepts like incident response planning, disaster recovery, business continuity management, cyber risk assessment and organizational learning.

The future cybersecurity strategy will include the synthesis of adaptive security architecture, AI driven analytics, Zero Trust, cyber resilience, and risk-based governance, to build integrated security ecosystems. Technologies like explainable AI (XAI), behavioral biometrics, extended detection and response (XDR), and autonomous security operations are anticipated to add another layer of security to organizations, along with aiding in trying to solve some of these transparency, privacy, and regulatory issues.

## CONCLUSION

Information security and assurance have become an integral part of organizational strategy in the age of digitization. According to the review of the literature, Zero Trust Architecture, artificial intelligence-based cybersecurity, cloud security, and cyber resilience strategies have transformed approaches to securing organizational information assets.

Despite the increased efficiency offered by such technologies, there are still considerable problems associated with their deployment, personnel deficiencies, regulatory issues, and threats associated with artificial intelligence. In terms of further research, one might consider addressing the problem of using explainable AI, automated assurance, and adaptive governance.

## REFERENCES

1. Arruda, L. G. S., Giozza, W., Nze, G. D. A., & Nunes, R. R. (2023). Implementação da arquitetura Zero Trust: Uma revisão sistemática de literatura. RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação, E56, 261–275.
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
3. Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A systematic literature review. arXiv.
4. 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.
5. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J. H., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476.
6. Mendes, C., & Rios, T. N. (2023). Explainable Artificial Intelligence and cybersecurity: A systematic literature review. arXiv.
7. Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of Zero Trust Architecture across domains. Sensors, 25(19).
8. Nadkarni, S., & Prügl, R. (2021). Digital transformation: A review, synthesis and opportunities for future research. Management Review Quarterly, 71(2), 233–341.
9. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology.
10. Shaikh, A., Chandre, P., Shafi, P. M., & Borde, S. (2023). Zero Trust security paradigm: A comprehensive survey and research analysis. Journal of Electrical Systems, 19(2), 28–37.
11. Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144.
12. Wen, S. F., Shukla, A., & Katt, B. (2025). Artificial intelligence for system security assurance: A systematic literature review. International Journal of Information Security, 24(1), 43.
13. National Institute of Standards and Technology. (2020). Zero Trust architecture (NIST Special Publication 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207