International Journal of Innovative Research in Engineering and Management (IJIREM)
ISSN (Online): 2350-0557, Volume 12, Issue 6, December 2025
DOI: https://doi.org/10.55524/ijirem.2025.12.6.10
Article ID IJIR3143, Pages 56-60
www.ijirem.org

Cyber Security Challenges and Emerging Trends in Digital Transformation: A Zero-Trust and AI-Driven Approach

Karan[1], and Dr. Shelly Garg[2]

[1] MCA Scholar, Amity Institute of Information Technology, Amity University Gurugram, Haryana, India
[2]Assistant Professor, Department of Computer Science and Engineering, Amity University, Gurugram, Haryana, India

Correspondence should be addressed to Karan ; karanydv786@gmail.com

Received: 1 November 2025 Revised: 15 November 2025 Accepted: 29 November 2025

ABSTRACT- The opportunities to scale and automate provide unprecedented opportunities due to digital transformation, which is facilitated by cloud-native and universal IoT devices, as well as AI-powered service provision. This article examines some of the key cyber security issues compounded by such technologies such as the increased and decentralized attack surface, the threats of data proliferation and privacy, and AI-enhanced attacks . We point out such emerging trends as Zero-Trust Security Architecture], AI-enhanced threat detection and response, and the combination of Security-by-Design and DevSecOps to overcome these challenges. The paper concludes that sustainable cyber resilience presupposes the alignment of technology and people and processes to make sure that security becomes an inherent component of design and operations.

KEYWORDS- Cyber Security, Emerging Technologies, Iot, Cloud Computing, Artificial Intelligence, Zero Trust, Ransomware, Cyber Resilience

I. INTRODUCTION

The digital transformation is transforming the way the governments, enterprises, and individuals generate and consume value, but this transformation comes with security trade-offs [10]. Cloud-native architectures, giant IoT ecosystems, AI-based applications, and 5G connections are scalable and automatable, but they create complex interconnected environments that are difficult to secure [11]. Recent news indicates that the rate and even more advanced forms of cyber-attacks, such as ransomware, supply-chain breaches, and AI-powered phishing, are on the rise [13]. Several critical infrastructure sectors like energy, healthcare, manufacturing, and finance have continued to be a major target since their disruption can cause significant economic and societal effects[14].

The two main questions of this paper are:

- What are the prevailing cyber security threats posed or escalated by emerging technologies?
- What are the most effective security trends and architectural patterns that can overcome these challenges?

The paper is divided in the following way: Section II is a literature review; Section III is the methodology; Section IV identifies the cyber security challenges; Section V addresses the emerging trends; Section VI is a summary of the discussion; and Section VII presents the recommendations to subsequent work.

II. LITERATURE REVIEW

Previous studies in cyber security focused on perimeter-based defense, cryptography and access control in a static environment. As virtualization and cloud computing became more popular, scholars studied multi-tenancy threats, virtualization escape, shared responsibility, and data exposure of a new kind.

In recent works, the complexity of hybrid multi-cloud systems, IoT systems, and connected networks of OT (Operational Technology) have been noted. The most common vulnerabilities reported in IoT security research include poor authentication, default passwords, ineffective patching systems and inadequate monitoring of the devices. Reports by industry also highlight that there are shortages of skills, governance and operational problems as organizations increase their attack surfaces.

Earlier research in the field of cyber security was on perimeter defense, cryptography and access control in a non-dynamical environment[1]. With the increase in popularity of virtualization and cloud computing, researchers researched on the multi-tenancy threats, virtualization escape, shared responsibility models and novel data exposure[5]. The original research on autonomic computing laid down a set of principles of self-managing systems still used in security architecture today[4].

The recent literature has covered the complexity of hybrid multi-cloud systems, the IoT systems, and connected networks of OT (Operational Technology) in detail[6][7]. Poor authentication, default passwords, lack of an effective patching system and lack of monitoring of the devices are the most widespread vulnerabilities that have been reported in the ionot security research[6]. The lack of cyber security expertise and gaps in governance are strongly mentioned in industry reports as organizations multiply their attack surfaces at a very high rate[8].

Modern studies have identified AI as a two-fold purpose technology[11]. Although AI indeed raises the detection level and the response rates by offering advanced analytics

and pattern recognition, it also allows attackers to produce deepfakes, launch phishing campaigns in large scale, and find vulnerabilities much faster. This two-sidedness is a key issue to cybersecurity workers and institutions[11].

Privacy Enhancing Technologies (PETs) and data protection systems are getting more scholarly attention. The tradeoff between innovation under data and regulatory compliance (e.g., GDPR) has motivated the study of the differentiating privacy, homomorphic encryption, and federated learning techniques[13].

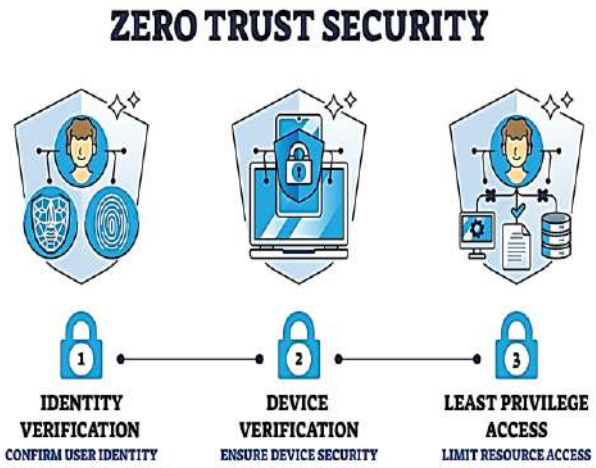

Figure 1: Zero Trust Security

In the above Figure 1 shows the Zero Trust Security model, which works on the idea of *never trust, always verify*. It has three main steps:

- Identity Verification: Confirms that the user is genuine using methods like biometrics or authentication.
- Device Verification: Ensures the device being used is secure and trusted.
- Least Privilege Access: Gives the user only the minimum access needed, reducing security risks.

Zero-Trust Architecture (ZTA) has become a paradigm to remove the implicit trust through constant verification of users, devices, and workloads[4]. The second line of study is that AI is a dual-purpose technology, improving detection and response to attacks and also helping attackers to make deepfakes, automate phishing, and find vulnerabilities.

III. RESEARCH METHODOLOGY

The method of the research is an academic study narrative, problem-driven review based on a compilation of scholarly research, industry threat-reporting, and standards-based documents. The aim is not to give a full systematic review but to give a synthesis of representative evidence which drives a systematic exploration of issues and solutions.

The choice of sources was based on the past five to six years and it focused on:

- Cyber security and new technology surveys.
- Cyber security reporting by sector.
- Zero trust, AI-driven security, and IoT risk technical papers.

The information was subdivided into four themes, namely: attack-surface expansion, data and privacy risks, AI-associated threats, and governance or skill issues. New trends were discussed concerning these issues, with an accent on the architectural principles, automation and human factors.

IV. CYBER SECURITY CHALLENGES IN LATEST TECHNOLOGIES

A. Bigger and Broader Attack Surface

Digital ecosystems have now extended to the on-premises data center, both social and private clouds, mobile devices, IoT endpoints, and services provided by third parties. The more integration points, such as API, sensor, microservice, or SaaS application, the more attackers have a potential entry point, and it is challenging to have holistic visibility and control[3]. The cloud-native applications are usually based on containers, orchestration platforms, and microservices designs, in which a misconfiguration may result in data stores or management interfaces being exposed. On the same note, resource-constrained IoT deployments might lack secure boot, hardware trust anchors, or effective patching, and in such cases would experience long-term vulnerabilities[7].

B. Information Proliferation and Information Privacy

The new technologies are data hungry in nature[13]. AI and analytics pipelines have the ability to combine mass amounts of personal, behavioural and operational information across various platforms and jurisdictions, presenting difficult data governance issues. Attacks within these sites are not only capable of exposing unchanging records, but can also divulge deduced profiles, company models, and confidential working knowledge. The regulatory regimes such as the GDPR and other privacy laws in various places require a firm commitment to issues of consent, data minimization, breach reporting and cross-border data transfers and at times organizations cannot do this uniformly.

C. Attacks and Adversarial Machine Learning Enhanced by AI

Attackers are continuously moving toward AI and automation to attack on a large scale and tailor their campaign[11]. These include fake phishing emails as well as deepfakes of voice or video materials that imitate executives thus complicating social engineering and particularly when time is of the essence. Data poisoning, model theft and adversarial inputs may pose risks to machine learning models themselves, leading to misclassification. Adversarial examples can have physical or financial effects in security-sensitive areas of autonomous vehicles, healthcare diagnostics, and fraud detection[16].

D. Ransomware, Supply-Chain, and OT/ICS Threats

Ransomware is one of the most noticeable threats, and recent attacks have been inflicted on hospitals, local administrations, and factories. Credential theft, privilege escalation and lateral movement are frequently also used together by attackers to encrypt data and backups in hybrid environments and then present extortion demands [17]. Attacks of supply-chains use trust relationship with a software vendor, managed service provider or hardware supplier to attack multiple downstream customers simultaneously. Industrial control systems and OT (Operational Technology) networks that previously operated independently are becoming more and more

interconnected with enterprise IT and cloud analytics and are now vulnerable to modern malware and remote access threats.

E. Skills deficit and Governing failures.

The human factor is an imperative bottleneck. A large number of organizations are complaining about the lack of recruitment and retention of cyber security specialists who have knowledge of cloud security, DevSecOps, incident response, and industrial control systems. Meanwhile, non-technical leadership teams can either be underestimating cyber risk or have no clear governance arrangements, which leads to lack of consistency in investment and responsibility fragmentation[18]. Consequently, security teams tend to work in a reactive fashion, focusing on firefighting, rather than strategic architecture and maintaining an improvement approach.

Table 1: Major Cyber Security Challenges in Emerging Technologies

Challenge	Primary Contexts	Typical Issues
Attack surface expansion	Cloud, IoT, 5G, SaaS	Misconfigurations, exposed APIs, weak device security
Data proliferation and privacy	AI/ML, analytics, multi-cloud	Unclear data flows, cross-border transfers, inference risks
AI-enhanced attacks	Phishing, social engineering	Deepfakes, automated phishing, adaptive malware
Ransomware and supply-chain	Hybrid IT/OT, critical sectors	Lateral movement, third-party compromise
Skills and governance gaps	All sectors	Shortage of experts, siloed decision-making

The key cybersecurity threats in the new technologies are described in Table 1.
It groups issues in five major areas, which are expansion of attack surfaces, data privacy concerns, threats augmented by AI, ransomware and supply-chain dilemmas, and governance/skill disparity. Under each domain, the table will indicate the technologies (e.g., cloud, IoT, AI/ML, hybrid IT/OT) and provide a list of common vulnerabilities of these technologies. The given table is the structured overview of the most important risks underlying contemporary cybersecurity concerns.

V. EMERGING TRENDS IN CYBER SECURITY

A. Zero-Trust Security Architecture

Zero trust changes the attitude of implicit trust inside a perimeter to constant validation of users, devices, and services irrespective of their position inside a network[10][19]. The main principles are Least-privilege access, micro-segmentation, strong identity and access management, and behaviour and context monitoring. Practically, zero trust is normally done in stages, beginning with identity-based controls, including multi- factor authentication, single sign-on, and conditional access policies. In the long term, organizations can expand micro segmentation to workloads, use policy-based access to APIs and services, as well as combine AI-driven analytics to identify anomalous behaviour in real time.

B. Threat Detection and Response powered by A.I.

Security analytics, intrusion detection, and automated response are one of the most promising defensive ones of AI use [12]. Machine learning can examine such amounts of network flows, endpoint monitoring, and user behavior or activity to identify subtle patterns that may not be identified by conventional signature-based tools. SOAR systems based on AI have already become able to triage alerts, correlate events, and propose or take containment measures which could include host isolation or blocking malicious domains. Nevertheless, the systems have a high requirement of quality training data and solid governance to prevent bias, overfitting, and blind spots in which the attackers can take advantage.

C. DevSecOps and Security-by-Design

With the increased speed of software delivery, it is necessary to incorporate security at an earlier stage of the development process. Security-by-Design principles promote threat-based modelling and secure coding, as well as automated security testing at the design stage as opposed to viewing security as a compliance check at the end of the development stage. DevSecOps is a build on DevOps by incorporating security measures into continuous integration and continuous delivery pipelines (i.e. static and dynamic analysis, dependency scanning, and policy-as-code). The goal of this approach is to minimize vulnerabilities prior to production, reduce the number of feedback loops between the developers, and enhance cross-functional collaboration between the development, operations, and security teams[20].

D. Privacy-Protecting and Secrecy-Controlling Computing.

PETs are technologies that scholars and professionals are considering to use to balance data-driven innovation with privacy and regulation issues. They include differential privacy, homomorphic encryption, secure multiparty computation, and federated learning all of which are predicated on the notion that the analysis of the data can be performed without revealing raw sensitive data when it is not necessary. Confidential computing Confidential computing makes use of trusted execution environments, which are hardware-based to safeguard data, and code in use and handles the risk of malicious insiders or untrusted hypervisor(s) or untrusted cloud infrastructure. Even though these technologies are still in their infancy and may cause overheads to performance, they offer potential means of safeguarding sensitive workloads.

E. Sector-Specific Security Rules and Regulations

The areas of finance, healthcare, energy, and industrial control systems are being issued industry regulators and industry specific cyber security guidance. These structures tend to incorporate technical controls along with risk management, incident reporting together with resilience planning requirements. To provide an example, OT-specific instructions will involve the network delineation, highly controlled access, the inventory of assets, and the procedures of incident response, which will be tested and optimized [9]. These sectoral approaches realize the fact that the main principles of security are universal, but the

specifics of realisation are to be limited by the domain[14][15].

Table 2: Emerging Security Trends and Their Focus

Trend	Main Objective	Key Enablers
Zero-trust architecture	Reduce implicit trust and lateral movement	Strong identity, micro segmentation, continuous monitoring
AI-driven security analytics	Detect complex threats at scale	ML-based IDS/IPS, UEBA, SOAR
DevSecOps and security-by-design	Integrate security into development lifecycle	CI/CD security scanning, threat modelling, policy-as-code
Privacy-enhancing technologies	Enable analytics with better privacy	Differential privacy, homomorphic encryption, federated learning
Sector-specific frameworks	Align security with domain constraints	Regulations, best-practice guidelines, audits

In the above Table 2 shows the significant emerging cybersecurity trends and their security goals.

Every trend, such as Zero-Trust, AI-based analytics, DevSecOps, PETs, and industry-specific frameworks, is accompanied by the most significant enablers that enable organizations to make it a reality. The table gives a brief mapping of translating the current defensive strategies and the technologies that facilitate them.

VI. DISCUSSION

It has been discussed that there is a trade-off between innovation and security in the sense that technologies that allow agility and insight offer new opportunities to attackers[2]. There are also cloud services, IoT devices, AI models and 5G networks that are to be listed among the assets that should be monitored, governed, and protected. Zero trust new directions, AI security analytics, and DevSecOps provide formal answers to this complexity with the trend towards identity-based controls, automated detection, and/or integrated security operations[10][12].

These tactics would however require long-term investment both on architecture, equipments and people, as well as the culture of IT and business. Practically organizations can start with what they can initially get done, such as hardening identity and access control, adopting secure base-lined configurations and increasing visibility of asset and information flows, but then move on to more complex functions[14].

The collaboration with other parties, taking part in threat intelligence sharing programs, and adherence to relevant standards can help to strengthen the collective defense[15].

VII. CONCLUSION AND FUTURE WORK

The emerging technologies have raised the levels of cyberspace security, as well as, introduced new vulnerabilities and offered more advanced security measures. Among the key threats, there are the increase of attack surfaces, privacy and data problems, AI-assisted threats, ransomware and supply-chain attacks and endemic skills and governance gaps. The subsequent areas of future studies and practice entail the necessity to scale the principles of zero-trust, increase AI-driven security systems and become more resistant to adversarial manipulation, and implement privacy-enhancing technologies on general platforms. More empirical studies that can determine the effectiveness of security interventions in practice are also desirable, particularly in those spheres and resources where the digital infrastructure and the control system are still evolving[7][8].

At the end of the day, achieving a system of equilibrium between technology, people, processes will be the answer to the sustainable cyber resilience so that security considerations become part of the design, procurement, and operation of the systems and not an add on.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023. Available from: https://doi.org/10.3390/electronics12061333

[2] "Global Cybersecurity Outlook 2025," World Economic Forum (WEF), 2025. Available from: https://tinyurl.com/29wzdyaw

[3] Data Security Council of India, *India Cybersecurity Domestic Market 2023 Report*, 2023. Available from: https://tinyurl.com/22hhjh3u

[4] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," *Computer*, vol. 36, no. 1, pp. 41–50, Jan. 2003. Available from: https://ieeexplore.ieee.org/abstract/document/1160055

[5] W. S. Admass et al., "Cyber security: State of the art, challenges and future trends," *Int. J. Inf. Technol.*, 2024.

[6] IEEE Access, "A Survey of Threats, Technologies, and Solutions," vol. 12, pp. 5000–5015, 2024. Available from: https://ieeexplore.ieee.org/abstract/document/11052962

[7] S. Karmakar, "Cybersecurity issues in IoT cloud system," *RAMD J.*, 2024.

[8] ISACA, "State of Cybersecurity 2023: Navigating Current and Emerging Threats," 2023. Available from: https://tinyurl.com/ndxb8y8z

[9] J. Kindervag, *Build Security into Your Network DNA: The Zero Trust Network Architecture*, Forrester Research Inc., 2010. Available from: https://tinyurl.com/3a4fb2bx

[10] P. M. F. C. Ogenyi, "Zero-trust security architecture in the AI age: A new architecture," *IJSRA*, 2025.

[11] F. C. Ogenyi, "Securing the future: AI-oriented cybersecurity in the era of A-IoT," *Front. Comput. Sci.*, 2025.

[12] Sattrix, "Future trends in AI and machine learning in cybersecurity," 2025. Available from: https://tinyurl.com/2unb54jc

[13] ISACA, *The New Oil, The New Risk: Data Security in the Age of AI*, 2025. Available from: https://tinyurl.com/5n8sh6m4

[14] UK Government, "Emerging technologies and how they impact cyber security," 2025.

[15] Univ. of San Diego, "Top Cybersecurity Threats to Watch in 2025," 2025.

[16] P. M. F. C. Ogenyi et al., "A Survey of Adversarial Machine Learning in Critical Systems," *ACM Comput. Surv.*, 2024.

[17] Pure Storage, "How a Zero Trust Architecture Can Help Mitigate Ransomware Risks," 2025.

[18] SANS Institute, "ICS/OT Cybersecurity Survey: 2023's Challenges," 2025. Available from: https://tinyurl.com/bdfa2jdr
[19] Fortinet, "What Is Zero Trust Architecture (ZTA)? Benefits and Best Practices," 2024. Available from: https://www.fortinet.com/resources/cyberglossary/zero-trust-architecture
[20] Microsoft, "What Is Zero Trust Architecture?" Microsoft Security, 2023. Available from: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview