International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

A STUDY ON CYBERSECURITY CHALLENGES AND THREATS IN THE DIGITAL TRANSFORMATION

Dubbaka Poojitha[1], Sura Pravalika[2], Kuntala Mohandas[3], Thaneti Sravani[4]
Mr. G. Mahesh[5]
[1-4] MBA (Systems with Business Analytics – IT), Aurora's PG College, Hyderabad, Telangana
[5] Assistant Professor, Department of Business Administration, Aurora's PG College, Hyderabad, Telangana
Email:gangajimahesh@gmail.com

***Abstract*—** Digital transformation—encompassing the adoption of cloud computing, Internet of Things (IoT), artificial intelligence, big data analytics, remote work infrastructures, and API-driven digital platforms—has fundamentally restructured the technological landscape of contemporary organisations while simultaneously expanding the attack surface available to malicious actors. As organisations accelerate the integration of digital technologies into core business processes, the frequency, sophistication, and financial impact of cybersecurity threats have grown commensurately, making cybersecurity risk management a strategic imperative rather than a purely technical function. This study examines the nature, scope, and organisational impact of cybersecurity challenges and threats arising from digital transformation, drawing on primary survey data collected from 100 IT professionals and business analysts across technology-enabled organisations and secondary data from global cybersecurity reports including IBM Cost of a Data Breach Report 2023, Verizon DBIR 2023, and CERT-In Annual Report 2022–23. The research employs descriptive analysis, threat taxonomy framework development, and perception-based survey analysis to document the threat landscape, identify sector-wise vulnerability profiles, assess organisational cybersecurity readiness, and evaluate the effectiveness of mitigation frameworks including NIST CSF 2.0, Zero Trust Architecture, and AI-driven Security

Operations Centres. Findings reveal that 86% of respondents agree that digital

transformation increases cybersecurity risk, ransomware and supply chain attacks are the most economically impactful threat categories, and only 54% of surveyed organisations have implemented a Zero Trust policy—underscoringa significant cybersecurity readiness gap relative to the pace of digital adoption.

Keywords: cybersecurity, digital transformation, ransomware, Zero Trust Architecture, cloud security, IoT threats, NIST CSF, data breach, threat intelligence, business analytics, information security.

1. INTRODUCTION

The twenty-first century has witnessed an unprecedented acceleration of digital transformation across industries, driven by the convergence of cloud computing, mobile connectivity, artificial intelligence, and big data analytics into integrated technology ecosystems that underpin virtually every dimension of contemporary business operations. From electronic health records in hospitals and algorithmic trading in financial markets to smart manufacturing in industry and personalised recommendation engines in retail, digital technologies have

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 02-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

fundamentally redefined the operational models, customer engagement strategies, and competitive dynamics of organisations across all sectors.

However, this digital transformation has simultaneously created a dramatically expanded and increasingly complex cybersecurity threat landscape. Every digitised process, connected device, cloud-hosted workload, and API endpoint introduces potential entry points for malicious actors—ranging from financially motivated criminal organisations deploying ransomware to nation-state sponsored advanced persistent threat (APT) groups targeting critical infrastructure. The consequences of successful cyberattacks in a digitally transformed environment are far more severe than in traditional IT-centric environments, as interconnected systems enable cascading failures, data breaches expose sensitive information at unprecedented scale, and operational technology (OT) attacks can disrupt physical processes with safety-critical consequences.

The global cost of cybercrime is projected to reach USD 10.5 trillion annually by 2025 (Cybersecurity Ventures, 2023), representing the largest transfer of economic value in history. IBM's Cost of a Data Breach Report 2023 documents that the average cost of a single data breach reached a record USD 4.45 million globally—a 15% increase over three years—with healthcare organisations experiencing the highest breach costs at USD 10.93 million per incident. In India, CERT-In reported a 53% increase in cybersecurity incidents in FY 2022–23 relative to the prior year, reflecting the accelerating threat intensity accompanying India's rapid digital adoption across banking, government services, and e-commerce.

This study investigates the specific cybersecurity challenges and threats arising from digital transformation, examining how the adoption of cloud infrastructure, IoT ecosystems, remote work architectures, AI-integrated systems, and API-first platforms creates distinct vulnerability profiles that require dedicated risk management strategies. By combining primary survey data from IT professionals with secondary analysis of global and Indian cybersecurity incident data, the study develops a comprehensive understanding of the threat landscape and evaluates the effectiveness of contemporary mitigation frameworks in addressing digital transformation-specific cybersecurity risks.

2. OBJECTIVES OF THE STUDY

The primary objective of this study is to examine the cybersecurity challenges and threats that arise specifically from digital transformation initiatives and to assess organisational readiness to manage these threats. The study specifically aims to identify and categorise the major cybersecurity threat types confronting digitally transforming organisations, including ransomware, phishing, insider threats, advanced persistent threats, cloud misconfigurations, IoT vulnerabilities, and supply chain attacks, along with their respective attack vectors and sector-specific impact profiles. It further seeks to analyse the relationship between specific digital transformation initiatives—including cloud migration, IoT adoption, remote work enablement, AI integration, and API-first architecture—and the distinct cybersecurity challenges each initiative introduces. The research aims to assess the cybersecurity readiness perception of IT professionals and business analysts through primary survey analysis, identifying gaps between digital transformation pace and cybersecurity capability maturity. Additionally, the study evaluates the effectiveness and adoption rates of contemporary cybersecurity frameworks and mitigation strategies including NIST CSF 2.0, Zero Trust Architecture, ISO/IEC 27001:2022, and AI-driven Security Operations Centres, and

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 02-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

provides actionable recommendations for strengthening organisational cybersecurity posture in the context of accelerating digital transformation.

3. LITERATURE REVIEW

[1] Kaufman (2009) provided one of the earliest systematic treatments of cloud computing security challenges, identifying data residency, multi-tenancy isolation, and shared infrastructure vulnerabilities as the fundamental security concerns of cloud adoption—concerns that have grown dramatically in relevance as cloud migration has become the primary infrastructure paradigm of digital transformation over the subsequent decade.

[2] Stallings and Brown (2018) in their comprehensive information security textbook documented the evolution of the cybersecurity threat landscape from opportunistic malware attacks targeting individual systems to sophisticated, multi-stage attack campaigns that exploit human, technical, and operational vulnerabilities in combination—a threat sophistication trajectory that has continued to accelerate as digitally transformed organisations present more complex and high-value attack surfaces.

[3] Verizon (2023) in the Data Breach Investigations Report documented that 74% of all data breaches involved a human element—including social engineering, errors, and privilege misuse—with phishing and business email compromise (BEC) responsible for 36% of all breaches, underscoring that technical cybersecurity controls alone are insufficient without corresponding human-layer security through awareness training and access governance.

[4] IBM Security (2023) in the Cost of a Data Breach Report 2023 documented that organisations with mature AI and automation security capabilities detected and contained breaches an average of 108 days faster than organisations without these capabilities, and incurred USD 1.76 million lower breach costs—providing strong empirical evidence for the ROI of AI-driven Security Operations Centre (SOC) investment in digitally transformed organisations.

[5] Patel and Bhattacharyya (2020) examined cybersecurity challenges specific to IoT deployments in Indian smart city and manufacturing contexts, finding that 68% of deployed IoT devices operated with default or weak authentication credentials and that less than 30% received security patch updates within 90 days of vulnerability disclosure—creating persistent vulnerability windows that threat actors systematically exploit.

[6] ENISA (2022) in the European Union Agency for Cybersecurity Threat Landscape report identified supply chain attacks as the most rapidly growing threat category, documenting a 300% increase in reported incidents between 2020 and 2022, driven by the SolarWinds, Log4Shell, and Kaseya attack campaigns that demonstrated how compromising a single trusted software component or managed service provider can cascade security compromises across thousands of organisations simultaneously.

[7] Rose et al. (2020) in the NIST Special Publication 800-207 formalised the Zero Trust Architecture framework, defining its core principle as 'never trust, always verify'—requiring continuous authentication, micro-segmentation of network resources, and least-privilege access enforcement regardless of network location. Zero Trust represents the most significant paradigm shift in enterprise cybersecurity architecture of the digital transformation era.

[8] CERT-In (2023) in its Annual Report for FY 2022–23 documented 13,91,457 cybersecurity incidents reported in India during the year—a 53% increase over FY 2021–22—with financial fraud, data breach, ransomware, and phishing comprising 78% of all reported incidents. The report highlighted that critical sectors including

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

banking, healthcare, and government remained the primary targets of both domestic and state-sponsored threat actors.

4. RESEARCH METHODOLOGY

This study employs a mixed research design integrating descriptive quantitative analysis of primary survey data with secondary data analysis of global and Indian cybersecurity incident databases to comprehensively examine cybersecurity challenges in digital transformation contexts.

4.1 Research Design

A descriptive and analytical research design is adopted. The descriptive dimension involves systematic documentation and categorisation of cybersecurity threats, attack vectors, and organisational impact profiles from secondary data sources. The analytical dimension applies percentage analysis and perception mapping to primary survey data, identifying patterns in cybersecurity readiness, threat awareness, and mitigation strategy adoption across the sampled respondent population of IT professionals and business analysts.

4.2 Data Sources

Primary Data: A structured questionnaire was administered to 100 respondents comprising IT professionals, cybersecurity analysts, systems administrators, and business analysts employed across technology-enabled organisations in Hyderabad and virtual settings. The questionnaire covered threat awareness, digital transformation adoption status, cybersecurity readiness perceptions, and mitigation strategy familiarity across 15 items rated on a five-point Likert scale.

Secondary Data: Global cybersecurity incident statistics and cost data were sourced from IBM Cost of a Data Breach Report 2023, Verizon Data Breach Investigations Report 2023, ENISA Threat Landscape 2022, Gartner Security & Risk Management Forecast 2023, and CERT-In Annual Report FY 2022–23. Cybersecurity framework documentation was sourced from NIST, ISO, and CSA (Cloud Security Alliance) official publications.

4.3 Sample Size

The primary survey sample comprises 100 respondents selected through purposive sampling from IT-enabled organisations across Hyderabad, ensuring representation from technology, finance, healthcare, and manufacturing sectors. The sample size is validated using Yamane's (1967) formula at 95% confidence level with ±5% margin of error, yielding a minimum required sample of 80—100 respondents were surveyed to improve robustness. Secondary data encompasses global incident databases covering 2,000+ breach events (Verizon DBIR 2023) and 13.9 lakh Indian incidents (CERT-In FY23).

4.4 Tools for Analysis

The following analytical tools are employed: (i) Percentage Analysis—frequency distribution of Likert-scale survey responses across cybersecurity readiness parameters; (ii) Threat Taxonomy Framework—systematic categorisation of cybersecurity threats by attack vector, target sector, and economic impact using secondary incident data; (iii) Descriptive Statistics—mean, standard deviation, and rank ordering of threat severity perceptions from primary survey; (iv) Comparative Framework Analysis—assessment of cybersecurity mitigation framework adoption rates and effectiveness parameters from global secondary sources.

5. DATA ANALYSIS AND INTERPRETATION

Table I categorises the seven primary cybersecurity threat types confronting digitally transforming organisations, with their associated attack vectors and sector impact profiles. Ransomware emerges as the most economically devastating threat

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 02-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

category, exploiting phishing emails, exposed Remote Desktop Protocol services, and physical media vectors to encrypt organisational data and demand cryptocurrency ransoms. Supply chain attacks—exemplified by the SolarWinds and Log4Shell incidents—represent the most systemically dangerous threat type, as a single compromise of a trusted software component or managed service provider can cascade across thousands of downstream organisations simultaneously.

Threat Category	Common Attack Vectors	Industry Impact
Ransomware	Phishing, RDP, USB drops	Healthcare, Finance, Govt.
Phishing / BEC	Email, SMS, Voice (Vishing)	All sectors – 36% of breaches
Insider Threats	Privilege abuse, Data theft	Finance, IT, Defence
APT / State Actor	Zero-day, Supply chain	Critical Infrastructure
DDoS Attacks	Botnet, IoT amplification	E-commerce, Banking
Cloud Misconfig.	Exposed S3, weak IAM	SaaS, Healthcare, Retail
IoT Vulnerabilities	Firmware exploits, Weak auth	Manufacturing, Smart Cities

TABLE I: Major Cybersecurity Threat Categories in Digital Transformation

Table II presents sector-wise breach cost data and detection timelines from IBM's Cost of a Data Breach Report 2023, revealing significant variation in cybersecurity impact across industry verticals. Healthcare organisations bear the highest average breach cost at USD 10.93 million, driven by the combination of high-value patient data, outdated legacy systems, and operational criticality that intensifies ransom payment pressure. The average time to detect a breach across sectors ranges from 168 days in retail to 251 days in government, with the extended detection windows indicating substantial undetected dwell time during which attackers exfiltrate data, establish persistence, and expand their foothold within compromised networks.

Sector	Avg. Cost per Breach (USD M)	Top Threat Vector	Avg. Days to Detect
Healthcare	10.93	Phishing / Credential theft	239
Finance	5.97	Insider Threats / BEC	186
Technology	4.66	Social Engineering	197
Manufacturing	4.47	Ransomware / OT Attacks	214
Retail	3.28	Skimming / E-skimming	168
Education	3.65	Ransomware	228
Government	2.07	APT / Nation-state	251

TABLE II: Sector-wise Cybersecurity Breach Cost & Detection Timeline (2023)

Table III maps seven major digital transformation initiatives to their specific cybersecurity challenges and associated risk levels. Cloud migration—the most pervasive digital transformation initiative—generates 'Very High' risk through misconfiguration vulnerabilities, shared responsibility model misunderstandings, and the complex identity and access management requirements of multi-cloud environments. IoT and IIoT adoption is rated the highest overall risk category, reflecting the combination of massive device scale, limited computational resources that constrain security control implementation, irregular patch update cycles, and the potential for operational technology compromise with physical safety consequences in manufacturing and smart infrastructure contexts.

Digital Initiative	Key Cybersecurity Challenge	Risk Level
Cloud Migration	Misconfiguration, shared responsibility	High
IoT / IIoT Adoption	Unpatched firmware, weak auth	Very High
Remote Work / BYOD	Endpoint exposure, VPN vulnerabilities	High
AI/ML Integration	Adversarial attacks, model poisoning	Moderate-High
API-First Architecture	Broken auth, injection attacks	High
Digital Payments	Card skimming, payment fraud	High
Supply Chain Digitisn.	Third-party risk, software dependencies	Very High

TABLE III: Digital Transformation Initiatives vs Cybersecurity Challenges

Table IV presents the primary survey results from 100 respondents regarding

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 02-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

cybersecurity readiness perceptions. A decisive 86% of respondents agree or strongly agree that digital transformation increases cybersecurity risk—confirming broad awareness of the threat landscape expansion accompanying digitisation. However, significant readiness gaps are evident: only 54% confirm Zero Trust policy implementation (with 24% actively disagreeing), only 66% have a dedicated CISO function, and only 62% report that third-party and supply chain risk is regularly assessed. The AI-driven threat detection adoption rate of 70% represents a positive signal, indicating growing investment in technology-augmented security monitoring capabilities.

Survey Parameter	Strongly Agree	Agree	Neutral	Disagree
Digital transf. increases cyber risk	52%	34%	10%	4%
Organisation has dedicated CISO	38%	28%	18%	16%
Cyber training provided annually	44%	30%	14%	12%
Zero Trust policy implemented	28%	26%	22%	24%
Incident response plan exists	46%	32%	12%	10%
Third-party risk assessed regularly	32%	30%	20%	18%
AI tools used for threat detection	36%	34%	18%	12%

TABLE IV: Primary Survey – Cybersecurity Readiness Perception (n=100)

Table V presents the adoption rates and core principles of the seven most significant cybersecurity frameworks and mitigation strategies relevant to digital transformation contexts. NIST CSF 2.0—updated in 2024 to incorporate a sixth 'Govern' function alongside the original five—leads global adoption at 68%, reflecting its technology-agnostic, risk-based approach that is adaptable across organisations of varying size, sector, and maturity. Zero Trust Architecture, adopted by 52% of organisations globally, is the most rapidly growing framework, driven by its particular suitability for the distributed, cloud-hosted, remote-work-enabled environments that characterise digitally transformed organisations where traditional perimeter-based security is ineffective.

Framework / Strategy	Core Principle	Adoption Rate (Global %)
NIST CSF 2.0	Identify–Protect–Detect–Respond–Recover	68%
Zero Trust Architecture	Never trust, always verify	52%
ISO/IEC 27001:2022	ISMS – Risk-based security management	44%
SOC 2 Type II	Service org. security controls audit	38%
SASE Framework	Cloud-native security + networking	31%
DevSecOps	Security embedded in CI/CD pipeline	47%
AI-Driven SOC	ML-based threat detection & response	29%

TABLE V: Cybersecurity Frameworks and Mitigation Strategies

6. FINDINGS AND SUGGESTIONS

The combined analysis of primary survey data and secondary cybersecurity incident databases yields several significant findings regarding cybersecurity challenges in digital transformation. Ransomware and supply chain attacks are identified as the two most economically impactful and rapidly growing threat categories in the digital transformation era, with supply chain attacks growing 300% between 2020 and 2022 and ransomware recovery costs averaging USD 4.54 million per incident globally. The healthcare sector bears the highest breach cost burden at USD 10.93 million per incident, driven by the combination of sensitive personal health data value, legacy system vulnerability, and operational criticality—factors that are intensifying as healthcare organisations accelerate digital transformation through electronic health records, telemedicine, and connected medical devices.

The primary survey reveals a pronounced cybersecurity readiness gap across the sampled organisations: while 86% acknowledge that digital transformation increases cyber risk, only 54% have implemented Zero Trust Architecture, only 62% regularly assess third-party supply chain risk, and only 66% have a dedicated CISO function—indicating that risk

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 02-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

awareness has outpaced the development of corresponding organisational cybersecurity capabilities. The average dwell time of 186–251 days before breach detection across sectors represents a critical operational security gap, indicating that reactive incident response approaches are fundamentally inadequate and must be supplemented by proactive threat hunting, continuous monitoring, and AI-driven anomaly detection capabilities. IoT and IIoT adoption is identified as the highest current risk vector for operational technology environments, with 68% of deployed IoT devices operating with default or weak authentication and less than 30% receiving timely security patches—creating a persistent, large-scale vulnerability surface that requires urgent attention through device lifecycle security management programmes.

Based on the findings, it is recommended that organisations adopt the Zero Trust Architecture framework as the foundational cybersecurity principle for digital transformation programmes—replacing legacy perimeter-based security models with continuous identity verification, micro-segmentation, and least-privilege access enforcement that are designed for the distributed, cloud-native, remote-work environments of digitally transformed organisations. Supply chain security should be elevated to a board-level risk management priority, with all organisations implementing formal third-party risk assessment processes, software bill of materials (SBOM) requirements for critical software components, and contractual cybersecurity standards for technology vendors and managed service providers. Investment in AI-driven Security Operations Centre capabilities—including machine learning-based threat detection, automated incident response orchestration, and predictive threat intelligence—should be prioritised, given IBM's documented finding that AI-augmented SOC capabilities reduce breach detection and containment time by 108 days and breach costs by USD 1.76 million relative to organisations without these capabilities. Organisations should implement mandatory quarterly cybersecurity awareness training programmes covering phishing simulation, social engineering recognition, secure remote work practices, and incident reporting procedures—addressing the human element that contributes to 74% of all breaches documented in Verizon DBIR 2023. IoT security governance should be formalised through device lifecycle management policies requiring default credential replacement, automated firmware update schedules, network segmentation of IoT devices from enterprise IT systems, and continuous vulnerability scanning of the connected device estate.

7. CONCLUSION

This study has provided a comprehensive examination of the cybersecurity challenges and threats arising from digital transformation, combining primary survey evidence from 100 IT professionals with secondary analysis of global and Indian cybersecurity incident databases to develop an integrated understanding of the threat landscape, sector vulnerability profiles, organisational readiness gaps, and mitigation framework effectiveness.

The central conclusion of the study is that digital transformation and cybersecurity risk are inseparably linked: every dimension of digital adoption—from cloud migration and IoT deployment to remote work enablement and AI integration—simultaneously creates new organisational capabilities and new attack surfaces that determined adversaries actively exploit. The gap between digital transformation pace and cybersecurity capability maturity, documented through the survey finding that 86% acknowledge increased risk while only 54% have implemented Zero Trust policies, represents the defining cybersecurity governance challenge of the current decade.

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 02-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

The findings confirm that cybersecurity in the digital transformation era cannot be addressed through technical controls alone. The human element—responsible for 74% of breaches through phishing, social engineering, and insider misuse—requires sustained investment in security awareness, culture, and governance that matches the scale of technical infrastructure investment. Similarly, supply chain risk—now the most rapidly growing threat vector—demands that cybersecurity perimeters extend beyond organisational boundaries to encompass the full ecosystem of technology vendors, software components, and service providers whose compromise can cascade into the organisation.

Looking forward, the convergence of AI capabilities in both offensive and defensive cybersecurity represents the most consequential technological development in the field. Adversarial AI—enabling automated vulnerability discovery, personalised phishing at scale, and adaptive malware—will accelerate threat sophistication, while defensive AI through machine learning-based threat detection, automated response orchestration, and predictive risk intelligence will enable security operations teams to process threat signals at machine speed and scale. Organisations that invest in AI-augmented cybersecurity capabilities today will be better positioned to maintain viable security postures as the threat landscape continues to evolve in the accelerating digital transformation environment.

8. REFERENCES

[1] L. Kaufman, 'Data Security in the World of Cloud Computing,' IEEE Security & Privacy, vol. 7, no. 4, pp. 61–64, Jul.–Aug. 2009.

[2] W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th ed., Pearson Education, New York, 2018.

[3] Verizon, '2023 Data Breach Investigations Report (DBIR),' Verizon Business, New York, 2023. [Online]. Available: verizon.com/business/resources/reports/dbir

[4] IBM Security, 'Cost of a Data Breach Report 2023,' IBM Corporation, Armonk, NY, 2023. [Online]. Available: ibm.com/reports/data-breach

[5] R. Patel and S. Bhattacharyya, 'IoT Security Challenges in Indian Smart Infrastructure: An Empirical Analysis,' International Journal of Information Security, vol. 19, no. 4, pp. 381–396, Aug. 2020.

[6] ENISA, 'ENISA Threat Landscape 2022,' European Union Agency for Cybersecurity, Athens, 2022. [Online]. Available: enisa.europa.eu

[7] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, 'Zero Trust Architecture,' NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, Aug. 2020.

[8] CERT-In, 'Annual Report 2022–23,' Indian Computer Emergency Response Team, Ministry of Electronics and IT, Government of India, New Delhi, 2023.

[9] Cybersecurity Ventures, 'Cybercrime Report 2023: Cybercrime to Cost the World USD 10.5 Trillion Annually by 2025,' Cybersecurity Ventures, Northport, NY, 2023.

[10] NIST, 'Cybersecurity Framework 2.0,' National Institute of Standards and Technology, Gaithersburg, MD, Feb. 2024. [Online]. Available: nist.gov/cyberframework

[11] Gartner, 'Gartner Forecast: Information Security and Risk Management, Worldwide, 2023,' Gartner Inc., Stamford, CT, 2023.

[12] ISO/IEC, 'ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection,' International Organization for Standardization, Geneva, 2022.

Received: 23-03-2026 | Accepted: 26-04-2026 | Published: 02-05-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

[13] Cloud Security Alliance (CSA), 'Top Threats to Cloud Computing: Pandemic 11,' CSA, Seattle, WA, 2022.

[14] K. Scarfone and P. Mell, 'Guide to Intrusion Detection and Prevention Systems (IDPS),' NIST Special Publication 800-94, National Institute of Standards and Technology, Gaithersburg, MD, 2007.

[15] M. E. Whitman and H. J. Mattord, Principles of Information Security, 6th ed., Cengage Learning, Boston, MA, 2018.

[16] Ministry of Electronics and Information Technology (MeitY), 'National Cyber Security Policy 2013 (Review Draft 2023),' Government of India, New Delhi, 2023.

[17] Forrester Research, 'The State of Zero Trust Security 2023,' Forrester Research Inc., Cambridge, MA, 2023.