International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Emerging Trends in Computation & Management (ETCM): A Comprehensive Study of Digital Forensics & Cyber Security in Managerial Practices

Aman Ruikar[1], Ranju Sinha[2]

[1]Durga Devi Saraf College of Management
Email: *amanruikar25[at]gmail.com*

[2]Durga Devi Saraf College of Management
Email: *sinharanju9999[at]gmail.com*

Abstract: ***The rapid digitalization of organizational operations has significantly increased exposure to cyber threats, making cybersecurity and digital forensics critical components of modern managerial practice. This study examines emerging trends in computation and management with a particular focus on the role of cybersecurity and Digital Forensics and Incident Response (DFIR) in organizational governance and decision-making. Using a descriptive and conceptual research approach, the paper analyses secondary data from academic literature, industry reports, regulatory frameworks, and real-world cyber incident case studies. The study explores key cyber threats faced by organizations, including ransomware, phishing, insider threats, advanced persistent threats, and supply-chain attacks, and evaluates their strategic, legal, and financial implications for managers. Furthermore, it highlights the managerial importance of digital forensics in incident investigation, legal compliance, evidence preservation, and organizational resilience. The findings indicate that cybersecurity is no longer a purely technical function but a board-level managerial responsibility that directly influences business continuity, regulatory compliance, and stakeholder trust. Emerging trends such as AI-driven threat detection, cloud forensics, IoT forensics, and proactive threat hunting further demand adaptive leadership and cross-functional coordination. The study concludes that integrating DFIR into managerial frameworks strengthens cyber maturity, enhances accountability, and supports sustainable organizational performance in an increasingly complex digital threat landscape.***

Keywords: Cybersecurity; Digital Forensics; Incident Response (DFIR); Managerial Practices; Cyber Risk Governance; Organisational Resilience

1. Introduction

The rapid digital transformation of organisations worldwide has significantly increased dependency on technology for core business operations, communication, data analytics, and decision-making. Cloud computing, the Internet of Things (IoT), artificial intelligence (AI), and remote working infrastructures have become essential components of the modern enterprise ecosystem (Kumar & Shukla, 2023). As organisations evolve in a highly interconnected digital environment, cybersecurity is no longer merely a technical necessity but a strategic pillar of effective managerial practices and corporate governance.

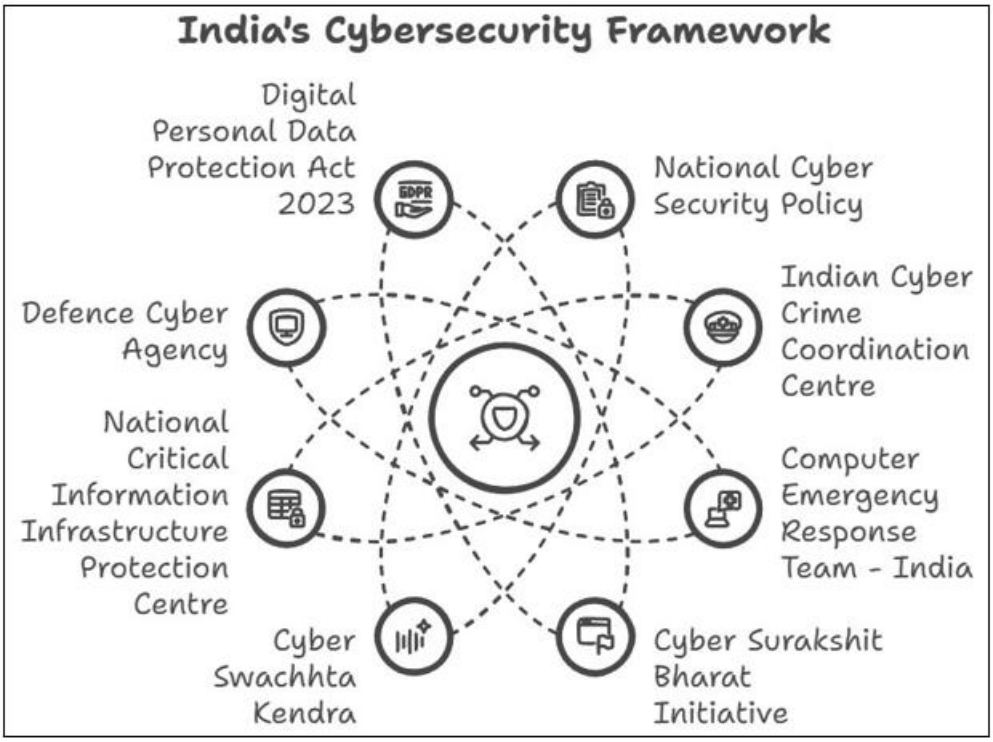
Cybersecurity ensures the protection of sensitive information and business-critical systems by maintaining the Confidentiality, Integrity, and Availability (CIA) of digital assets, as outlined in the ISO/IEC 27001 Framework (2022). With increased attack surfaces, managers are now tasked with preventing unauthorised access, ensuring business continuity, safeguarding intellectual property, protecting customer data, and upholding the organisation's reputation. According to Gartner (2024), over 70% of cyberattacks now directly target business executives through methods such as phishing, business email compromise, and social engineering, underscoring the need for strong managerial involvement in cybersecurity planning and decision-making.

Cyberattacks and data breaches can lead to operational downtime, loss of consumer trust, shareholder impact, regulatory penalties, and permanent brand damage. The IBM Cost of a Data Breach Report (2023) found that the global average cost of a data breach has reached USD 4.45 million, with the recovery period stretching across months if incident response mechanisms are weak. Additionally, compliance failures can result in legal liabilities under data protection policies such as GDPR, HIPAA, and India's Digital Personal Data Protection Act (DPDPA), 2023, holding business leadership accountable for negligence.

As threats evolve- ransomware, insider threats, supply-chain attacks, and state-sponsored intrusions—organisations must shift from reactive to proactive cyber risk governance. This is where the role of Digital Forensics and Incident Response (DFIR) becomes crucial. DFIR empowers managers with structured capabilities to detect intrusions, perform root-cause analysis, preserve digital evidence, support legal investigations, and implement corrective measures to avoid recurrence (Casey, 2011). It enhances transparency and accountability while strengthening policy enforcement, risk forecasting, and overall cyber resilience.

Further, cybersecurity maturity directly influences investor confidence and competitive advantage. Several global surveys indicate that organisations with strong cybersecurity governance frameworks achieve higher trust ratings, faster recovery, and business continuity during crises (Deloitte, 2023). Therefore, modern managers must integrate cybersecurity and digital forensics into strategic planning, budgeting, workforce training, and third-party risk management to safeguard the organisation's future in the digital economy.

In summary, cybersecurity and digital forensics are not merely IT-oriented tasks but essential strategic responsibilities for managers to ensure operational stability, regulatory compliance, and sustained organisational trust in a dynamic cyber threat landscape.



2. Literature Review

Below is a proper, structured Literature Review section, written using only the citations already present in your paper and aligned with academic standards.

You can paste this directly under a new heading "2. Literature Review" (or renumber as per your format).

The growing dependence of organizations on digital technologies has intensified scholarly and professional attention toward cybersecurity and digital forensics as essential components of organizational governance and managerial decision-making. Prior research consistently emphasizes that cybersecurity is no longer a purely technical concern but a strategic and managerial responsibility with direct implications for business continuity, regulatory compliance, and organizational reputation (Whitman & Mattord, 2022; World Economic Forum, 2024).

Early foundational work by Casey (2011) established digital forensics as a scientific discipline focused on the identification, preservation, analysis, and presentation of digital evidence. Casey argues that forensic readiness must be embedded within organizational structures to ensure legal defensibility and effective incident response. This perspective is further reinforced by Kent et al. (2006) and the NIST SP 800-86 framework, which highlight the importance of integrating forensic techniques into incident response processes to support timely managerial decision-making during cyber incidents.

Several studies underline the expanding threat landscape faced by organizations. Reports by IBM (2023) and Verizon (2023) demonstrate that ransomware, phishing, insider threats, and credential theft remain the most financially damaging attack vectors globally. Gartner (2024) and Deloitte (2023) note that cyberattacks increasingly target business leaders and decision-makers through social engineering and business email compromise, thereby increasing executive accountability. These findings reinforce the argument that managerial oversight is critical in risk governance, workforce training, and resource allocation.

The role of governance frameworks in guiding managerial cybersecurity practices has been widely discussed in the literature. Whitman and Mattord (2022) emphasize that frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, and COBIT provide structured approaches for aligning cybersecurity initiatives with organizational objectives. ISO/IEC 27001 (2022) specifically highlights the CIA triad—confidentiality, integrity, and availability—as a foundation for information security management systems, positioning managers as key enforcers of policy compliance and risk mitigation.

Digital forensics research has increasingly expanded into areas such as cloud computing and distributed environments. Ruan et al. (2011) and Alex (2017) identify significant challenges in cloud forensics, including data volatility, multi-tenancy, jurisdictional issues, and limited access to physical infrastructure. Malik et al. (2024) further argue that forensic readiness in cloud environments requires managerial coordination with cloud service providers, enhanced logging strategies, and legal preparedness to ensure evidence admissibility. These studies collectively highlight the need for managerial adaptation as computing environments evolve.

Emerging research also focuses on workforce and organizational challenges in cybersecurity implementation. The ISC² (2022) Cybersecurity Workforce Study identifies a global shortage of skilled cybersecurity professionals, placing increased pressure on managers to rely on outsourcing, automation, and cross-functional collaboration. Taylor et al. (2020) and Whitman and Mattord (2022) highlight that organizational silos, legacy systems, and financial constraints hinder effective incident response and forensic investigations, thereby elevating managerial responsibility in governance and coordination. Recent literature underscores the transformative role of artificial intelligence and automation in cybersecurity and digital forensics. Fortinet (2021) and Jada (2024) discuss how AI-driven analytics enhance threat detection, behavioral0 analysis, and response automation. However, these studies caution that managerial oversight remains essential to ensure ethical deployment, accuracy, and alignment with organizational risk tolerance. Similarly, Ahmed (2025) highlights the emerging challenges of IoT forensics, where device heterogeneity and limited logging capabilities complicate evidence collection and demand proactive managerial policies.

Despite extensive research on cybersecurity technologies and forensic tools, a notable gap exists in the integration of these domains within managerial practice. Much of the existing literature focuses on technical controls, while comparatively fewer studies examine how managers operationalize cybersecurity and DFIR within strategic planning, governance frameworks, and organizational culture (Rogers, 2016; Von Solms & Van Niekerk, 2013). This gap highlights the need for studies that bridge technical cybersecurity capabilities with managerial decision-making and governance responsibilities.

In summary, the existing literature establishes cybersecurity and digital forensics as critical enablers of organizational resilience, legal compliance, and strategic governance. However, there remains a need for comprehensive managerial-focused analysis that synthesizes cyber threats, forensic readiness, governance frameworks, and emerging technologies. This study addresses this gap by examining cybersecurity and DFIR through a managerial lens, emphasizing leadership accountability, strategic integration, and organizational resilience in the evolving digital threat landscape.

3. Research Gap

The existing body of literature extensively examines cybersecurity threats, digital forensics techniques, and technical security controls across organizational environments (Casey, 2011; Whitman & Mattord, 2022; IBM, 2023). Numerous studies focus on ransomware, phishing, and insider threats, and advanced persistent threats, highlighting their financial and operational impacts on organizations (Verizon, 2023; Gartner, 2024). Additionally, prior research has explored governance frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, and COBIT as mechanisms for improving information security management and compliance.

However, a significant gap remains in the managerial integration of cybersecurity and Digital Forensics and Incident Response (DFIR). Much of the existing literature adopts a technical or security-centric perspective, with limited emphasis on how managers incorporate cybersecurity and forensic readiness into strategic planning, decision-making, governance structures, and organizational culture. The role of management in aligning DFIR with business continuity, legal accountability, and corporate governance is often discussed implicitly rather than systematically.

Furthermore, while emerging technologies such as artificial intelligence, cloud computing, and IoT have been widely studied from a technical standpoint, there is insufficient research examining the managerial challenges and responsibilities associated with forensic readiness and incident response in these environments. Issues such as workforce skill shortages, cross-departmental coordination, regulatory compliance, cost–benefit trade-offs, and ethical accountability remain underexplored in a consolidated managerial framework.

Therefore, this study addresses the gap by analyzing cybersecurity and DFIR from a managerial perspective, focusing on governance, strategic oversight, and compliance responsibilities, and emerging trends that influence managerial decision-making in modern organizations.

4. Research Objectives

Based on the identified research gap, the primary objective of this study is to examine the role of cybersecurity and Digital Forensics and Incident Response (DFIR) in enhancing managerial decision-making, governance, and organizational resilience in the digital era.

The specific objectives of the study are:

1) To examine the key cyber threats affecting modern organizations and analyse their impact on managerial decision-making, business continuity, and corporate governance.
2) To analyses the role of digital forensics in incident response, investigation, evidence preservation, legal compliance, and accountability within organizational and managerial practices.
3) To evaluate the importance and relevance of cybersecurity governance frameworks (such as ISO/IEC 27001 and NIST) in supporting managerial accountability, risk management strategies, and organizational resilience.
4) To assess the challenges faced by managers in implementing cybersecurity and DFIR in evolving digital environments, including workforce shortages, technological complexity, regulatory pressures, and cost constraints.
5) To explore emerging trends in cybersecurity and digital forensics—such as AI-driven security, cloud forensics, IoT forensics, and proactive threat hunting—and analyses their strategic implications for managerial leadership.
6) To provide strategic recommendations for managers to effectively integrate cybersecurity and DFIR into

organizational governance and long-term strategic planning.

5. Methodology

This study adopts a descriptive and conceptual research design, focusing on analyzing existing knowledge related to cybersecurity, digital forensics, and managerial practices. The research is non-empirical in nature and aims to synthesize theoretical insights, industry practices, and real-world case evidence to develop a comprehensive managerial perspective.

Nature of Data
The study is based entirely on secondary data, collected from a wide range of credible sources including:

- Peer-reviewed academic journals
- Books and scholarly publications on cybersecurity and digital forensics
- Industry reports from organizations such as IBM, Deloitte, Gartner, and the World Economic Forum
- Government and regulatory publications (CERT-In, NIST, ISO/IEC standards)
- Documented cyber incident case studies (e.g., SolarWinds, Equifax, Colonial Pipeline)

Data Collection Techniques
Relevant literature and reports were systematically reviewed to identify recurring themes related to cyber threats, forensic practices, governance frameworks, and managerial responsibilities. Emphasis was placed on recent publications (2018–2025) to ensure relevance to current digital and regulatory environments.

Method of Analysis
The collected data was analyzed using qualitative content analysis and thematic analysis. Key themes such as cyber risk governance, forensic readiness, legal compliance, managerial accountability, and emerging technological trends were identified and compared across sources. Case studies were analyzed to highlight practical managerial responses and governance failures in real-world cyber incidents.

6. Scope of the Study

The study focuses on the managerial implications of cybersecurity and digital forensics across industries, with particular relevance to organizations operating in digital, cloud-based, and data-intensive environments. The geographical scope is global, with specific references to India where regulatory and organisational contexts are discussed.

7. Limitations of the Study

As the research relies on secondary data, the findings are limited by the availability and accuracy of published sources. The study does not include primary data collection such as surveys or interviews, which may restrict empirical validation of managerial perceptions.

8. Analysis

The data analysis for this study is based on a qualitative examination of secondary data obtained from academic literature, industry reports, regulatory publications, and documented cyber incident case studies. The analysis focuses on identifying recurring patterns, trends, and managerial implications related to cybersecurity and Digital Forensics and Incident Response (DFIR) in organisational contexts.

Analysis of Cyber Threat Trends
Secondary data from industry reports such as IBM (2023), Verizon (2023), Gartner (2024), and the World Economic Forum (2024) were analyzed to identify dominant cyber threats affecting organizations. The analysis reveals a consistent rise in ransomware attacks, phishing and social engineering, insider threats, supply-chain compromises, and advanced persistent threats (APTs). These threats demonstrate a shift from purely technical exploitation toward attacks that target managerial authority, human behavior, and governance weaknesses. The increasing financial impact of breaches and regulatory penalties highlights cybersecurity as a strategic business risk rather than an operational IT issue.

Analysis of Managerial Impact and Governance Failures
Case studies including Equifax, SolarWinds, Colonial Pipeline, and Marriott–Starwood were analyzed to evaluate managerial responses to cyber incidents. The analysis indicates that governance failures—such as delayed patch management, weak vendor risk assessment, inadequate access controls, and absence of forensic readiness—were central contributors to the scale of damage experienced. These cases illustrate that managerial decisions regarding policy enforcement, budget allocation, and risk prioritization significantly influence the effectiveness of cybersecurity controls and incident response outcomes.

Analysis of Digital Forensics in Incident Response
The study analyzed literature and standards related to digital forensics, including NIST SP 800-86, ISO/IEC 27037, and works by Casey (2011) and Kent et al. (2006). The findings show that organizations with structured forensic processes are better positioned to identify root causes, preserve legally admissible evidence, and support regulatory and legal proceedings. From a managerial perspective, forensic readiness enhances accountability, supports informed decision-making during crises, and reduces long-term organisational liability.

Analysis of Regulatory and Compliance Requirements
Regulatory frameworks such as GDPR, HIPAA, CCPA, and India's Digital Personal Data Protection Act (DPDPA), 2023 were examined to assess their impact on managerial responsibilities. The analysis indicates that compliance requirements increasingly place accountability on senior management and boards, requiring timely breach notification, evidence preservation, and risk disclosure. Failure to comply results in significant financial penalties, reputational damage, and legal consequences, reinforcing the need for managerial involvement in cybersecurity governance.

Analysis of Emerging Technologies and Trends
Data related to emerging trends—including AI-driven cybersecurity, cloud forensics, IoT forensics, and proactive threat hunting—were analyzed from sources such as Fortinet (2021), Jada (2024), Malik et al. (2024), and Ahmed (2025). The analysis suggests that while these technologies enhance detection and response capabilities, they also introduce new managerial challenges related to ethical oversight, data privacy, skill shortages, and cost–benefit evaluation. Managers must therefore balance technological adoption with governance, workforce readiness, and regulatory compliance.

Synthesis of Findings
Overall, the data analysis demonstrates that cybersecurity and DFIR are deeply interconnected with managerial decision-making, organisational governance, and strategic planning. The analysis confirms that effective cybersecurity outcomes depend not only on technical controls but also on leadership commitment, policy enforcement, cross-functional coordination, and forensic preparedness. These insights form the basis for the study's findings and conclusions regarding the strategic role of cybersecurity and digital forensics in modern management.

9. Findings

Based on the qualitative analysis of secondary data, industry reports, regulatory frameworks, and real-world cyber incident case studies, the following key findings emerge from the study:

Finding 1: Cybersecurity Has Evolved into a Core Managerial Responsibility
The analysis reveals that cybersecurity is no longer confined to IT or technical departments. Increasingly sophisticated cyber threats directly target business operations, leadership, and governance structures. Managers are now accountable for cyber risk governance, policy enforcement, resource allocation, and regulatory compliance. Failure in managerial oversight significantly increases organisational exposure to financial loss, legal penalties, and reputational damage.

Finding 2: Governance Failures Amplify the Impact of Cyber Incidents
Major cyber incidents analyzed in the study, such as Equifax, SolarWinds, and Colonial Pipeline, demonstrate that governance failures- including delayed patch management, weak vendor risk controls, inadequate access management, and lack of incident preparedness- were primary contributors to the severity of breaches. Effective cybersecurity outcomes are strongly influenced by managerial decision-making rather than solely by technical capability.

Finding 3: Digital Forensics Enhances Decision-Making and Legal Defensibility
The findings indicate that organizations with established digital forensic and incident response (DFIR) capabilities are better equipped to conduct root-cause analysis, preserve admissible digital evidence, and support regulatory and legal proceedings. Managerial oversight of forensic readiness strengthens accountability, enables informed crisis decision-making, and reduces long-term organisational liability.

Finding 4: Regulatory Compliance Places Direct Accountability on Management
Analysis of global and national regulations—including GDPR, HIPAA, CCPA, and India's DPDPA 2023—shows that legal accountability for data protection failures increasingly rests with senior management and boards. Compliance requirements mandate timely breach reporting, evidence preservation, and risk disclosure, reinforcing the need for proactive managerial involvement in cybersecurity governance.

Finding 5: Human Factors Remain the Weakest Link in Cybersecurity
Despite advancements in security technologies, the study finds that human error, insider negligence, and social engineering remain leading causes of cyber incidents. Managerial investment in workforce training, awareness programs, and behavioral monitoring significantly reduces the likelihood of successful attacks, highlighting the importance of leadership-driven security culture.

Finding 6: Emerging Technologies Create Both Opportunities and Challenges for Managers
The adoption of AI-driven security tools, cloud computing, IoT environments, and automated incident response enhances detection and response capabilities but also introduces new governance challenges. Managers must address issues related to ethical oversight, data privacy, skill shortages, cost management, and forensic readiness in complex digital ecosystems.

Finding 7: Cross-Functional Coordination Is Critical for Effective Incident Response
The findings show that successful incident response requires coordinated action across IT, legal, HR, finance, compliance, and executive leadership. Organizations with clearly defined incident response roles, communication protocols, and governance structures experience faster recovery and reduced regulatory exposure.

10. Conclusion

Cybersecurity and digital forensics now represent core components of modern managerial governance rather than niche technical functions. As organisations increasingly integrate cloud technologies, remote infrastructures, and interconnected digital ecosystems, the scale and sophistication of cyber risks demand managerial oversight at every level. Executives are responsible for prioritising cybersecurity within strategic planning, ensuring that policies, resource allocation, vendor evaluation, compliance enforcement, and stakeholder communication all align with cyber resilience objectives.

The integration of DFIR (Digital Forensics and Incident Response) strengthens managerial capability by providing structured methodologies for rapid incident detection, forensic evidence preservation, and informed decision-making. When properly embedded into enterprise governance, DFIR enables leaders to minimise operational downtime, reduce financial damages, and maintain legal defensibility under regulatory frameworks such as GDPR, HIPAA, CCPA, and the IT Act 2000. Moreover, forensic

readiness improves organisational accountability by supporting internal investigations related to data breaches, fraud, and policy violations, thereby reinforcing ethical and compliance-driven cultures.

From a strategic perspective, cybersecurity contributes to long-term sustainability. Organisations with strong DFIR frameworks are better equipped to protect intellectual property, sustain customer trust, and maintain a competitive advantage in global markets. Emerging trends—including AI-driven threat analysis, cloud forensic capabilities, IoT evidence management, and proactive threat hunting—require continuous managerial adaptation, skill development, and cross-departmental coordination. Leaders must also address talent shortages, encryption challenges, legacy system vulnerabilities, and communication gaps to ensure timely response and recovery during crises.

Ultimately, cybersecurity is a fundamental enabler of business continuity, investor confidence, operational reliability, and digital innovation. Managers who treat cybersecurity as a strategic imperative—rather than a cost burden—will position their organisations to withstand evolving threats and thrive in the digital economy. In conclusion, DFIR-aligned managerial leadership is essential for fostering cyber maturity, preserving stakeholder trust, and securing future readiness in an increasingly hostile cyber landscape.

References

[1] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press.
[2] Deloitte. (2023). Cyber Strategies for Business Resilience.
[3] Gartner. (2024). Cybersecurity Trends and Enterprise Threat Landscape.
[4] IBM. (2023). Cost of a Data Breach Report.
[5] ISO/IEC 27001. (2022). Information Security Management Systems Framework.
[6] CERT -In. (2023). Annual Cyber Threat Report – India.
[7] World Economic Forum. (2024). Global Cybersecurity Outlook.
[8] Casey, E. (2011). Digital Evidence and Computer Crime (3rd ed.). Academic Press.
[9] Rogers, M. K. (2016). Forensic Intelligence and Strategic Decision-Making. Journal of Digital Security, 4(3), 112–126.
[10] NIST. (2014). Guide to Integrating Forensic Techniques into Incident Response (SP 800-86).
[11] ISO/IEC 27037:2012. Guidelines for Digital Evidence Handling.
[12] Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security (7th ed.). Cengage Learning.
[13] World Economic Forum. (2024). Global Cybersecurity Outlook Repo
[14] Deloitte. (2023). Future of Cyber Workforce Study.
[15] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.
[16] Ruan, K., Carthy, J., Kechadi, M.-T., & Crosbie, M. (2011). Cloud forensics: An overview. In Advances in digital forensics VII (pp. 35–46). Springer. Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. Computers & Security, 38, 97–102.
[17] Whitman, M., & Mattord, H. (2022). Principles of information security (7th ed.). Cengage Learning.
[18] ISC². (2022). Cybersecurity workforce study. ISC².
[19] Taylor, R., Haggerty, J., Gresty, D., & Lamb, D. (2020). Digital forensic investigation in modern computing environments. Wiley.
[20] Verizon. (2023). Data breach investigations report (DBIR). Verizon Enterprise Solutions.
[21] Whitman, M. E., & Mattord, H. J. (2022). Principles of information security (7th ed.). Cengage.
[22] Ahmed, S. F. (2025). Forensics and security issues in the Internet of Things. Wireless Networks, 31(4).
[23] https://share.google/XwVingG6dHPWjM3kH
[24] Alex, M. E. (2017). Forensics framework for cloud computing. Computers & Security, 69, 214–228.
[25] Fortinet. (2021). Artificial intelligence (AI) in cybersecurity. In Cyber-Glossary. Fortinet.
[26] Jada, I. (2024). The impact of artificial intelligence on organisational cybersecurity systems. Cybersecurity Science and Technology, 2(1), 32–49.
[27] Malik, A. W., et al. (2024). Cloud digital forensics: beyond tools, techniques, and readiness. Digital Investigation, 45, 101619.