University of Central Lancashire
UCLan

Central Lancashire Online Knowledge (CLoK)

Title	Towards Improved Vulnerability Management in Digital Environments: A Comprehensive Framework for Cyber Security Enhancement
Type	Article
URL	https://clok.uclan.ac.uk/51716/
DOI	doi:10.26562/irjcs.2024.v1105.01
Date	2024
Citation	Egho-Promise, Ehigiator, Lyada, Emmanuel and Aina, Folayo (2024) Towards Improved Vulnerability Management in Digital Environments: A Comprehensive Framework for Cyber Security Enhancement. International Research Journal of Computer Science, 11 (05). pp. 441-449. ISSN 2393-9842
Creators	Egho-Promise, Ehigiator, Lyada, Emmanuel and Aina, Folayo

It is advisable to refer to the publisher's version if you intend to cite from the work.
doi:10.26562/irjcs.2024.v1105.01

For information about Research at UCLan please go to http://www.uclan.ac.uk/research/

All outputs in CLoK are protected by Intellectual Property Rights law, including Copyright law. Copyright, IPR and Moral Rights for the works on this site are retained by the individual authors and/or other copyright owners. Terms and conditions for use of this material are defined in the http://clok.uclan.ac.uk/policies/

IRJCS: International Research Journal of Computer Science
Volume 11, Issue 05, May 2024
ISSN: 2393-9842
https://www.irjcs.com/archives

Towards Improved Vulnerability Management in Digital Environments: A Comprehensive Framework for Cyber Security Enhancement

Ehigiator Egho-Promise,
Department of ICT, Faculty of CreaTech
City of Oxford College and University Centre, United Kingdom
eghopromise@yahoo.com
Emmanuel Lyada,
Learning Content Developer, ISBAT
University, Kampala, Uganda
elyada@ieeinnovations.com
George Asante,
Department of IT Education,
Akenten Appiah -Menka University of Skills Training and Entrepreneurial Development,
Ghanagasante@aamusted.edu.gh
Folayo Aina,
Department of Computing,
School of Engineering and Computing,
University of Central Lancashire, United Kingdom
faina@uclan.ac.uk

Publication History
Manuscript Reference No: IRJCS/RS/Vol.11/Issue05/MYCS10080
Research Article | Open Access | Double-Blind Peer-Reviewed | Article ID: IRJCS/RS/Vol.11/Issue05/MYCS10080
Received: 24, April 2024 | Revised: 05, May 2024 | Accepted: 17 May 2024 | Published Online: 30, May 2024
http://www.irjcs.com/volumes/Vol11/iss-05/01.MYCS10080.pdf
Article Citation: Ehigiator,Emmanuel,George,Falayo(2024). Towards Improved Vulnerability Management in Digital Environments: A Comprehensive Framework for Cyber Security Enhancement. IRJCS: International Research Journal of Computer Science, Volume 11, Issue 05 of 2024 pages 441-449 doi:> https://doi.org/10.26562/irjcs.2024.v1105.01
BibTeX Ehigiator@2024Towards

Copyright: ©2024 This is an open access article distributed under the terms of the Creative Commons Attribution License; Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited

Abstract: This study aimed at developing a comprehensive framework that enhances cyber security and improves vulnerability management in a digital environment. The study reviewed the challenges of vulnerability management in digital environments, with a focus on cyber-physical power systems (CPPS). Through a comprehensive literature review, existing Cyber Security frameworks like NIST, ISO 27001, and ISA/IEC 62443 were evaluated based on their applicability to CPPS. Key vulnerabilities and threat vectors unique to the integration of operational technology and information technology in CPPS were identified. The dual role of artificial intelligence (AI) in enhancing Cyber Security defences while enabling sophisticated AI-driven attacks was explored. Gaps in current frameworks, such as the lack of standardized AI integration and real-time threat detection capabilities, were highlighted. The study synthesized its findings to propose a comprehensive framework that addresses these gaps such as providing guidelines for secure AI adoption and offering strategies to mitigate emerging cyber threats effectively. The study recommended developing AI-specific security protocols, fostering interdisciplinary collaboration, and ensuring continuous framework updates to match the evolving cyber threat landscape. This research aimed to strengthen Cyber Security resilience in critical digital infrastructures.
Keywords: Cyber Security, Vulnerability management, Cyber-physical power systems, NIST framework, ISO 27001, ISA/IEC 62443, Artificial intelligence, Cyber Attacks, Threat Detection, Risk assessment, Critical infrastructure, Industrial control systems

I. INTRODUCTION

The importance of information technology to contemporary business has made Cyber Security crucial for all types of enterprises across all industries (AL-Hawamleh,2024). There are inevitable challenges that an organisation has in managing risks effectively and consistently(Stutz et al., 2024). One of these challenges is digital security. An all-inclusive framework based on the core principles needed to strengthen digital security would be appropriate. There should be a flexible framework that can be easily modified to fit different digital surroundings. It must be noted that, ensuring adherence to strict safety protocols is important for businesses to safeguard assets from potential hazards and minimise risks (Thakur, 2024). It is crucial to save a company's most valuable assets before other, less crucial components, especially in the early stages of its existence. Hackers often target assets that arenot sufficiently secured by security measures in order to get access to an organization's networks and systems (Chauhan and Jain, 2024).

Given the dynamic nature of cyber threats and their multifaceted nature, it is imperative that organisations invest significant resources in enhancing their security. Given the present discourse, risk management firms need to consider adopting a proactive and adaptable strategy. Threat actors often modify their tactics in order to circumvent the security measures that businesses use (VICTOR-MGBACHI, 2024). Online dangers are always evolving; therefore, solutions should be flexible. To reduce the likelihood of attacks, every business needs a robust Cyber Security plan. The plan must have an ongoing employee training. In recent times, there has been an increase in the frequency, complexity, and severity of artificial intelligence (AI) intrusions (Karger et al., 2022). When it comes to cyber security, artificial intelligence (AI) has a number of limitations (Lu, 2017). While AI can significantly strengthen an organization's defences, it also creates the potential for criminals to develop more sophisticated, fast-acting, and stealthy attacks. The increasing number of cyber attacks that employ AI as a tool is one illustration of the various ways that AI may impact Cyber Security (Benson, 2022). This study uses Malatji's AI-in-Cyber Security categorization paradigm to distinguish between hostile, aggressive, and defensive AI (Krima et al., 2020).

Defensive artificial intelligence (AI) seeks to enhance the resilience of computer networks and systems against cyber threats through advanced AI methodologies such as machine learning, as noted by İlhan and Karaköse (2019). In contrast, adversarial AI refers to the deployment of AI technologies for hostile purposes, including the automation of attacks exploiting known vulnerabilities or the invention of new hacking techniques, as detailed by GÖNEN (2017). These AI-driven assaults can also involve manipulating AI systems to produce erroneous decisions or actions, an approach sometimes described as "aggressive AI" (İlhan and Karaköse, 2019).

The rise in both the volume and sophistication of Cyber Attacks has prompted increased investment in Cyber Security solutions across industries (Lehto, 2022). Particularly in the industrial sector, rapid advancements in integrating robots, networking, and data processes have increased exposure to cyber risks (Karnik et al., 2022). This evolution is part of the broader transition towards Industry 4.0, which merges virtual and physical systems to enhance both communication and production efficiency (Javaid et al., 2022).

Statistically, the industrial sector has become a primary target for Cyber Attacks, constituting 23.2% of all cyber incidents in 2021, a notable increase from previous years (Aljaryan et al., 2022). These attacks not only disrupt operations but also lead to substantial financial losses, tarnish brand reputations, and introduce complex legal challenges (Kappelman et al., 2022; Cremer et al., 2022).
Amidst these challenges, global software development (GSD) practices have spread, characterized by distributed teams working across various geographic, time zone, and cultural boundaries. This model leverages global talent pools and aims at cost reduction, but it also complicates the Cyber Security landscape due to the dispersed nature of team setups and the continuous development cycle (Biswas et al., 2022).

This study conducted an extensive literature review focused on Cyber Security within the software development sector. The research critically examine the most prevalent security threats, evaluate the effectiveness of existing Cyber Security measures, and propose viable strategies to mitigate these risks. Particular attention was paid to vulnerabilities inherent in software development frameworks and the potential dangers posed by insiders, which could lead to data breaches with severe consequences (Alvarez-Alvarado et al., 2024).

Through this detailed investigation, the study aims to provide a comprehensive framework that not only addresses the technical aspects of Cyber Security but also considers the organizational and human factors critical to developing robust security protocols. This framework will serve as a guide for organizations to better manage and counteract the evolving landscape of cyber threats, thereby enhancing the overall security of digital environments.

1.2 Aim and Objectives

This study is aimed at developing a comprehensive framework that enhances Cyber Security and improves vulnerability management within digital ecosystems. The specific objectives were to:

1. Review Existing Cyber Security Frameworks and Measures
2. Identify and Analyse Key Vulnerabilities in Digital Environments
3. Propose and Validate a Comprehensive Cyber Security Framework

1.3 Problem Statement

Organizations engaged in digital transactions face formidable challenges due to the pervasive presence of Cyber Security risks in today's digital ecosystems. These risks are exacerbated by inadequate risk control measures, increasing the vulnerability of information and data systems to unauthorized access and breaches. The absence of effective processes to identify and rectify potential vulnerabilities before they manifest can elevate the risk levels, potentially leading to severe disruptions or even complete cessation of operations. This situation is not uncommon and poses a significant threat to organizational stability and security. In response to these challenges, there is a pressing need to enhance Cyber Security measures within digital environments. The proposed study aims to develop a comprehensive Cyber Security framework that not only strengthens the cyber defences of organizations but also improves vulnerability management systems. This framework will provide a robust methodology for organizations to better manage and mitigate the risks associated with digital transactions and operations.

Through a detailed literature review and evaluation of existing security measures, the study seeks to propose viable strategies that address both technical and organizational vulnerabilities, thereby enhancing the overall resilience of organizations against cyber threats. This organized approach to framing the research problem highlights the critical need for improved Cyber Security practices and sets the stage for the subsequent investigation into effective solutions for vulnerability management and risk mitigation in digital environments.

II. LITERATURE SURVEY

2.1. Comprehensive review of existing literature on vulnerability management frameworks, methodologies, and tools.

The integration of traditional electrical power networks with advanced computing and networking capabilities has given rise to Cyber Physical Power Systems (CPPS). Researchers such as Butt Zulqarnain and Butt (2021), Alvarez-Alvarado et al. (2024), and Eldeeb et al. (2024) have documented the critical role of CPPS in contemporary society, highlighting their indispensability in providing consistent energy supply and their complexity due to the interconnection of physical and digital components. This transformation has significantly heightened the importance of Cyber Security as CPPS become targets for sophisticated Cyber Attacks due to their essential role in national infrastructure.

Studies by Ghiasi et al. (2023) and Bello et al. (2024) illustrated the novel challenges that emerge from the CPPS architecture, including the vulnerability of critical infrastructure to disruptions and data manipulation. These vulnerabilities have raised concerns about the potential for substantial harm, not just to the operational continuity of power systems but also to public safety and security. The relationship between Cyber Security and Supervisory Control and Data Acquisition (SCADA) systems, as discussed by Möller (2023) and Knapp (2024), underscores the intricate defence mechanisms required to protect these infrastructures from cyber threats.

The utilization of Artificial Intelligence (AI) in enhancing Cyber Security measures has been extensively explored, with Ciccarelli Papetti and Germani (2023), Manoharan and Sarker (2023), and Jeffrey et al. (2023) discussing how AI is employed both as a defensive tool against cyber threats and as a means for attackers to develop more sophisticated cyber-attack strategies. The dual-use nature of AI in Cyber Security presents both opportunities for enhancing security measures and risks where AI could be misused.

Most recent research has highlighted the increasing complexity and frequency of AI-driven Cyber Attacks that could potentially destabilize entire systems and societies. Studies by Kalla et al. (2023), Pilli (2023), and Vegesna (2023) delve into how AI-driven threats, including polymorphic malware and adversarial AI, challenge existing Cyber Security defences. These studies emphasize the need for a deeper understanding of AI's capabilities and vulnerabilities in a Cyber Security context.

2.2 Limitations, Strengths and Weakness of Cyber-Attacks

This comprehensive review of the literature reveals that while significant advancements have been made in understanding and mitigating Cyber Security risks associated with CPPS and AI, substantial gaps remain. These gaps not only limit our ability to defend against sophisticated cyber threats but also hinder our understanding of the broader implications of these attacks. Addressing these gaps through targeted research will be crucial in developing more effective Cyber Security strategies and legal measures capable of adapting to the dynamic landscape of cyber threats.

The landscape of AI-driven cyber-attacks is evolving rapidly, challenging traditional Cyber Security strategies and necessitating a review of current approaches and methodologies. This section synthesizes the insights from recent studies to evaluate the strengths and weaknesses of AI in Cyber Security, highlighting significant gaps and proposing research opportunities.

Guembe et al. (2023) investigated the technical characteristics of AI-driven attacks, focusing on their implementation during the access and penetration stages of Cyber Attacks. It should be noted that traditional Cyber Security measures are becoming less effective due to the sophistication, speed, and diversity of AI-driven methods. The study emphasized the need for AI-enhanced defensive strategies and significant investment in resilient AI infrastructure.

Yamin et al. (2023) conducted a comprehensive analysis of various AI-assisted assault scenarios, pointing out the gap in global regulation of AI militarization and its implications for international security. Yamin et al (2023) argued for international conventions to effectively regulate the proliferation of AI technologies to prevent global instability.

Bout et al. (2024) explored how machine learning algorithms could enhance existing cyberattack techniques within IoT networks, making them less detectable and more sophisticated. Their findings indicated a necessity for better security frameworks that can address these advanced methods.

Oreyomi and Jahankhani (2024) discussed the development of autonomous Cyber Security systems using AI. Oreyomi and Jahankhani (2024) highlighted the potential risks associated with AI autonomy in Cyber Security, such as algorithmic bias and lack of human oversight, stressing the need for balanced human-AI collaboration.

Chakraborty et al. (2024) assessed the capabilities of AI to aid in the timely detection and management of cyber threats. They acknowledged that while AI can significantly enhance data analysis speed, it cannot yet replace human expertise in Cyber Security.

Most studies focus predominantly on the technological and tactical aspects of AI in Cyber Security without sufficient consideration of the broader societal and psychological impacts. This oversight calls for more comprehensive research into how AI-driven cyber threats affect individuals, organizations, and societies at large.
The rapid development and deployment of AI technologies outpace the existing legal and regulatory frameworks. There is a crucial need for adaptive legal structures that can keep up with technological advancements and address the ethical dilemmas posed by AI in Cyber Security.

Studies like those by Yamin et al. (2023) highlighted the absence of unified global standards for the regulation of AI technologies, particularly in military and defense contexts. Research aimed at establishing international norms and agreements is necessary to manage the militarization of AI and ensure global security.

The potential for AI to operate autonomously in Cyber Security contexts raises significant ethical and operational concerns. There is a need for frameworks that effectively integrate AI tools with human oversight to ensure that decisions made by AI systems are ethical, accountable, and reversible.

2.3 Gaps and Research Opportunities

This study has identified significant gaps in the existing literature, particularly concerning the broader implications of AI-driven Cyber Attacks and the effectiveness of current legal and regulatory frameworks in addressing these issues. Research has extensively covered the technological aspects of AI in Cyber Security, such as its role in enhancing threat detection and response mechanisms. However, there is a notable deficiency in discussions about the social, psychological, and legal implications of these technological advancements.

2.4 Specific Gaps Identified:

Lack of Comprehensive Legal Frameworks: As noted by Mahmud et al. (2024), current legal frameworks are inadequate for addressing AI-generated offenses, particularly in corporate settings where AI can manipulate markets and influence online shopping behaviors. The study highlighted the need for legal structures that can evolve with the rapid development of AI technologies.
Underexplored Societal Implications: Studies such as those by Mehtab and Mahmud (2024) have touched on the vulnerabilities introduced by AI in educational platforms, including phishing scams and breaches of remote learning systems. However, these studies have not deeply explored the broader societal impacts these vulnerabilities could have, such as the potential for large-scale privacy invasions or the societal destabilization resulting from targeted AI-driven attacks.
Insufficient Analysis of Root Causes and Social Effects: Research such as one conducted by Mathew (92) and Sen et al. (2024) has provided insights into the dual-use nature of AI in Cyber Security, both as a protective and an exploitative tool. However, there is a scarcity of detailed analysis on the root causes of AI-driven attacks and their profound social consequences.
Lack of Empirical Research on AI-Enhanced Cyber Threats: The work by Blauth et al. (2023) proposes a categorization system for AI-enhanced threats but admits the potential incompleteness in covering all categories. This highlights a need for more empirical research to validate and possibly expand upon their proposed categorization.

2.5 Research Opportunities

Given the identified gaps, several research opportunities arise that could significantly contribute to the field.
Development of Adaptive Legal Frameworks: There is an urgent need for research that supports the creation of legal frameworks capable of adapting to the advancements in AI technology. This research should aim to provide guidelines that are flexible and robust enough to handle the dynamic nature of AI-driven threats.
Study on Social and Psychological Impacts: Research into the social and psychological impacts of AI-driven Cyber Attacks could provide deeper insights into the indirect effects of these breaches, such as public trust, mental health issues related to privacy breaches, and societal norms.
Root Cause Analysis: Investigating the root causes of AI-driven attacks would be crucial in developing more effective countermeasures. Understanding the motivations and mechanisms behind these attacks can lead to more targeted and effective Cyber Security strategies.
Empirical Validation of Cyber Threat Categorizations: Conducting empirical studies to test and refine the categorization systems for AI-enhanced cyber threats proposed by researchers like Blauth et al. (2023) would help in understanding the full spectrum of risks posed by AI in Cyber Security.

III. THEORETICAL FRAMEWORK

Compliance systems are divided into two primary categories, each serving different organizational needs:
Regulatory Compliance Frameworks: These frameworks focus on ensuring that organizations meet legal obligations and regulatory standards. They delineate the laws, regulations, and guidelines that organizations are required to follow, thereby ensuring legal compliance across various jurisdictions.

Cyber Security Compliance Frameworks: As detailed by Abrahams et al. (2024), these frameworks provide detailed guidance on establishing and maintaining a robust security posture. They are designed to adapt to the dynamic nature of cyber threats and protect data assets effectively. These frameworks aim to safeguard businesses from Cyber Attacks and streamline risk management processes by integrating sector-specific data standards and recommended practices.

3.1 NIST Framework

The NIST Cyber Security Framework comprises three core elements: the Framework Core, Framework Implementation Tiers, and Framework Profiles. Each element serves a distinct function, yet collectively they provide a comprehensive approach to managing Cyber Security risks aligned with business objectives.

Framework Core: Described by Yang et al. (2023), the Core is a collection of Cyber Security activities and expected outcomes grouped into five primary functions, namely Identification, Protection, Detection, Response, and Recovery. These functions help organizations to focus their efforts and resources on areas most crucial to their Cyber Security resilience. The Core facilitates better coordination between the management and operational levels within an organization, enhancing the overall Cyber Security efforts. Framework Implementation Tiers: According to Cartwright et al. (2023), the Tiers assist organizations in assessing their approach to managing Cyber Security risk and the processes in place to protect against cyber threats. The Tiers range from Tier 1 (Partial) to Tier 4 (Adaptive), reflecting a progression from informal, reactive responses to an agile, risk-informed approach in broader risk management strategies. Framework Profiles: Profiles are custom configurations of the Core functions that reflect an organization's particular resources, risk tolerance, and desired outcomes. They serve as benchmarks for measuring progress and guiding the Cyber Security efforts towards the specific needs of the organization.

3.2 ISO 27001 Framework:

27001 stands as a cornerstone among international standards, offering organizations a robust framework meticulously designed to guide the establishment, implementation, operation, monitoring, review, maintenance, and continuous improvement of their Information Security Management Systems (ISMS).Sugiarto et. al,2022 suggested at its core, ISO 27001 serves as a comprehensive blueprint, providing organizations with clear and structured guidance on how to safeguard their sensitive information assets effectively. By adhering to the principles and requirements outlined within the standard, organizations can systematically address the complexities of modern information security challenges. The framework outlined by ISO 27001 enables organizations to methodically identify, assess, and mitigate information security risks through a systematic and documented approach. This risk-based methodology ensures that organizations can prioritize their efforts towards protecting critical assets and mitigating potential vulnerabilities.

3.3 ISA/IEC 62443 Standards in Industrial Cyber Security

ISA/IEC 62443 is an internationally recognized series of standards that establish best practices for Cyber Security in industrial automation and control systems (IACS). These standards provide a comprehensive framework for assessing security performance, defining risk assessment processes, and establishing Cyber Security lifecycle methodologies for product developers. The ISA/IEC 62443 standards are crucial for stakeholders involved in control systems Cyber Security, including asset owners, product developers, integrators, and service providers. They bridge the gap between operations and information technology, ensuring a holistic approach to Cyber Security across various industries like building automation, power generation, medical devices, transportation, chemicals, and oil and gas. The standards emphasize shared responsibility among key stakeholder groups to ensure the safety, integrity, reliability, and security of control systems. ISA/IEC 62443 standards cover a wide range of topics, including security maintenance, monitoring, incident response, risk assessment, and security lifecycle phases like assessment, development, implementation, and maintenance. These standards are continuously updated and expanded to address evolving Cyber Security challenges in industrial environments. The ISA/IEC 62443 series of standards provides a robust framework for Cyber Security in industrial automation and control systems (IACS). However, translating these standards into practical implementation strategies remains a challenge. Heinl et al. (2023) critically analyze the ISA/IEC 62443 standards, focusing on their application to IACS. They identify gaps between theoretical standards and practical implementation, emphasizing the need for actionable guidance to ensure conformity to ISA/IEC 62443 standards in industrial settings.

IV. FINDINGS AND ANALYSIS

4.1 Examination of Existing Cyber Security Frameworks

The research started with a systematic review of existing Cyber Security frameworks, focusing particularly on those applicable to CPPS. The frameworks analyzed included the NIST Cyber Security Framework, ISO/IEC 27001, and ISA/IEC 62443, which are widely recognized for their comprehensive approach to managing Cyber Security risks in industrial systems. All frameworks provide robust guidelines for risk assessment, identification, and management but have varying degrees of applicability to CPPS.ISA/IEC 62443 was found to be particularly tailored for industrial automation systems, providing specific guidelines that address the unique needs of CPPS.A common limitation across the frameworks was the under-specification of strategies to integrate AI technologies, which are increasingly relevant for CPPS. The analysis revealed that while ISO/IEC 27001 is comprehensive, it lacks specific provisions for the unique Cyber Security challenges posed by the integration of physical and digital systems in CPPS. The NIST Framework is flexible and widely applicable but does not offer the depth needed for complex CPPS configurations without significant customization.

4.2 Identification of Vulnerabilities and Threat Vectors

Using a combination of surveys, interviews, and case studies, the research identified common vulnerabilities and threat vectors specific to CPPS. This objective leveraged AI to analyze incident reports and simulate attack scenarios to understand potential vulnerabilities better. The integration of digital and physical components in CPPS creates unique vulnerabilities, such as those arising from the interface between operational technology (OT) and information technology (IT) systems. Common vulnerabilities included insecure data transmission, inadequate authentication protocols, and the susceptibility of physical components to digital commands that could lead to system shutdowns or malfunctions.AI-driven analysis tools successfully identified patterns and predictions about potential attack vectors, demonstrating the critical role of AI in proactive Cyber Security defense strategies. The study highlighted a significant gap in real-time threat detection and response capabilities within existing frameworks.

4.3 Role of Artificial Intelligence in Cyber Security

This section of the study focused on the dual role of AI in Cyber Security, examining how AI can both enhance defensive capabilities and present new Cyber Security challenges.AI technologies, particularly machine learning algorithms, are highly effective in identifying unusual patterns that may indicate a security breach. However, AI can also be used to create more sophisticated cyber-attacks, such as those involving polymorphic malware and AI-driven phishing scams. The analysis showed that while AI could significantly enhance detection and response times, there is a lack of standardization in the deployment of AI technologies within the frameworks studied. AI's potential to automate responses in real-time is underutilized due to concerns over the reliability of autonomous AI decisions in critical infrastructure environments.

V. CONCLUSION

This research underscores the critical need for an ongoing revision and enhancement of Cyber Security frameworks to include AI and address the specific needs of CPPS. As cyber threats evolve, so too must our strategies to mitigate them, necessitating a proactive approach to integrating advanced technologies into Cyber Security defenses. By adhering to the recommendations proposed, practitioners can better protect CPPS against both current and emerging threats, ensuring the stability and security of critical infrastructure essential to modern society.

VI. FUTURE WORK

To address the gaps identified in this research, future studies could explore: Longitudinal Studies on AI Threats: Conduct long-term studies to understand the evolving nature of AI-driven threats and their impact on CPPS. Comparative Analysis of Frameworks: Perform comparative analyses of Cyber Security frameworks across different industries to identify best practices that could benefit CPPS. Technological Innovations in AI: Investigate new AI technologies that could specifically address the unique challenges of integrating Cyber Security measures in CPPS.

REFERENCES

[1]. Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. Mastering compliance: a comprehensive review of regulatory frameworks in accounting and Cyber Security. Computer Science & IT Research Journal, 5(1), pp.120-140.

[2]. Ahmad, W., Sen, A., Eesley, C. and Brynjolfsson, E., 2024.The role of advertisers and platforms in monetizing misinformation: Descriptive and experimental evidence (No. w32187). National Bureau of Economic Research.

[3]. AI, N., 2023.Artificial Intelligence Risk Management Framework (AI RMF 1.0).

[4]. AlDaajeh, S. and Alrabaee, S., 2024. Strategic Cyber Security. Computers & Security, 141, p.103845.

[5]. AL-Dosari, K., Fetais, N. and Kucukvar, M., 2024. Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. Cybernetics and systems, 55(2), pp.302-330.

[6]. AL-Hawamleh, A., 2024. Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. International Journal of Computing and Digital Systems, 15(1), pp.1315-1331.

[7]. Aljaryan, L.K., Alfalahi, W.H. and Al Khamis, T.S., 2022, December. Cyber Attacks and Solutions for Future Factories. In 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)

[8]. Alvarez-Alvarado, M.S., Apolo-Tinoco, C., Ramirez-Prado, M.J., Alban-Chacón, F.E., Pico, N., Aviles-Cedeno, J., Recalde, A.A., Moncayo-Rea, F., Velasquez, W. and Rengifo, J., 2024. Cyber-physical power systems: A comprehensive review about technologies drivers, standards, and future perspectives. Computers and Electrical Engineering, 116, p.109149.

[9]. Alvarez-Alvarado, M.S., Apolo-Tinoco, C., Ramirez-Prado, M.J., Alban-Chacón, F.E., Pico, N., Aviles-Cedeno, J., Recalde, A.A., Moncayo-Rea, F., Velasquez, W. and Rengifo, J., 2024. Cyber-physical power systems: A comprehensive review about technologies drivers, standards, and future perspectives. Computers and Electrical Engineering, 116, p.109149.

[10]. Aris, S., Aeini, B. and Nosrati, S., 2023. A digital aesthetics? Artificial intelligence and the future of the art. Journal of Cyberspace Studies, 7(2), pp.219-236.

[11]. Baniecki, H. and Biecek, P., 2024. Adversarial attacks and defenses in explainable artificial intelligence: A survey. Information Fusion, p.102303.

[12]. Bello, A., Farid, F. and Hossain, F., 2024, March. An Assessment of the Cyber Security Challenges and Issues Associated with Cyber-Physical Power Systems. In International Conference on Advances in Computing Research (pp. 318-333). Cham: Springer Nature Switzerland.

[13]. Bhardwaj, A., Bharany, S., Abulfaraj, A.W., Ibrahim, A.O. and Nagmeldin, W., 2024. Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities. Egyptian Informatics Journal, 25, p.100443.

[14]. Bharti, P., 2023. Measurement information management for industry 4.0 (Doctoral dissertation, Brunel University London).
[15]. Bibi, I., Schaffert, D., Blauth, M., Lull, C., von Ahnen, J.A., Gross, G., Weigandt, W.A., Knitza, J., Kuhn, S., Benecke, J. and Leipe, J., 2023. Automated Machine Learning Analysis of Patients With Chronic Skin Disease Using a Medical Smartphone App: Retrospective Study. Journal of Medical Internet Research, 25, p.e50886.
[16]. Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A. and Delen, D., 2022. A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. Decision Support Systems, 152, p.113651.
[17]. Bountakas, P., 2023. Implementing AI-driven methodologies for cyberattack detection.
[18]. Burrell, D.N. ed., 2023. Real-World solutions for diversity, strategic change, and organizational development: perspectives in healthcare, education, business, and technology: Perspectives in Healthcare, Education, Business, and Technology. IGI Global.
[19]. Butt, O.M., Zulqarnain, M. and Butt, T.M., 2021. Recent advancement in smart grid technology: Future prospects in the electrical power network. Ain Shams Engineering Journal, 12(1), pp.687-695.
[20]. Cartwright, A., Cartwright, E. and Edun, E.S., 2023. Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers & Security, 131, p.103288.
[21]. Chang, J.P., Zheng, H.L., Mardani, A., Pedrycz, W. and Chen, Z.S., 2024. Evaluating holistic privacy risk posed by smart home ecosystem: A capability-oriented model accommodating epistemic uncertainty and wisdom of crowds. IEEE Transactions on Engineering Management.
[22]. Chauhan, D. and Jain, J.K., 2024. Measures and Preventions of Cyber Policies in Smart Cities. In Digital Technologies in Modeling and Management: Insights in Education and Industry (pp. 244-262). IGI Global.
[23]. Ciccarelli, M., Papetti, A. and Germani, M., 2023. Exploring how new industrial paradigms affect the workforce: A literature review of Operator 4.0. Journal of Manufacturing Systems, 70, pp.464-483.
[24]. Manoharan, A. and Sarker, M., 2023. REVOLUTIONIZING CYBER SECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXT-GENERATION THREAT DETECTION. https://www.doi.org/10.56726/IRJMETS32644
[25]. Jeffrey, N., Tan, Q. and Villar, J.R., 2023. A review of anomaly detection strategies to detect threats to cyber-physical systems. Electronics, 12(15), p.3283.
[26]. Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S., 2022. Cyber risk and Cyber Security: a systematic review of data availability. The Geneva Papers on risk and insurance-Issues and practice, 47(3), pp.698-736.
[27]. Dhiman, S. and Singh, S., 2023. Cybercrime and Computer Forensics in Epoch of Artificial Intelligence in India. Cyber Law Reporter, 2(4), pp.13-32.
[28]. Eldeeb, H.B., Naser, S., Bariah, L., Muhaidat, S. and Uysal, M., 2024. Digital Twin-Assisted OWC: Towards Smart and Autonomous 6G Networks. IEEE Network.
[29]. Ghiasi, M., Wang, Z., Mehrandezh, M., Jalilian, S. and Ghadimi, N., 2023. Evolution of smart grids towards the Internet of energy: Concept and essential components for deep decarbonisation. IET Smart Grid, 6(1), pp.86-102.
[30]. GÖNEN, S., YILMAZ, E.N., ŞANOĞLU, S., KARACAYILMAZ, G. and ÖZBİRİNCİ, Ö., Bilim ve Teknoloji Dergisi.
[31]. Halloran, T., Desrochers, F., Zhang, E.Z., Chen, T., Chern, L.E., Xu, Z., Winn, B., Graves-Brook, M., Stone, M.B., Kolesnikov, A.I. and Qiu, Y., 2023. Geometrical frustration versus Kitaev interactions in BaCo2 (AsO4) 2. Proceedings of the National Academy of Sciences, 120(2), p.e2215509119.
[32]. Hassan, S.M.U.H., 2023. STUDY OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY AND THE EMERGING THREAT OF AI-DRIVEN CYBER ATTACKS AND CHALLENGE. Available at SSRN 4652028.
[33]. Ilca, L.F., Lucian, O.P. and Balan, T.C., 2023. Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response. Sensors, 23(15), p.6757.
[34]. İlhan, İ. and Karaköse, M., 2019, September. Requirement Analysis for Cyber Security Solutions in Industry 4.0 Platforms. In 2019 International Artificial Intelligence and Data Processing Symposium (IDAP) (pp. 1-7). IEEE.
[35]. İlhan, İ. and Karaköse, M., 2019, September. Requirement Analysis for Cyber Security Solutions in Industry 4.0 Platforms. In 2019 International Artificial Intelligence and Data Processing Symposium (IDAP) (pp. 1-7). IEEE.
[36]. Ishaque, M., Johar, M.G.M., Khatibi, A. and Yamin, M., 2023. A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system. Measurement: Sensors, 30, p.100933.
[37]. Javaid, M., Haleem, A., Singh, R.P. and Suman, R., 2022. Enabling flexible manufacturing system (FMS) through the applications of industry 4.0 technologies. Internet of Things and Cyber-Physical Systems, 2, pp.49-62.
[38]. Kalla, D., Samaah, F., Kuraku, S. and Smith, N., 2023. Phishing detection implementation using databricks and artificial Intelligence. International Journal of Computer Applications, 185(11), pp.1-11.
[39]. Kappelman, L., Torres, R., McLean, E.R., Maurer, C., Johnson, V.L., Snyder, M. and Guerra, K., 2022. The 2021 SIM IT Issues and Trends Study. MIS Quarterly Executive, 21(1).
[40]. Karger, E., Gonserkewitz, P. and Klüver, C., 2022. Entscheidungsunterstützung zur Auswahl einer geeigneten Block chain-Technologie mit einem Self-Enforcing Network. In Digitalisierung und Nachhaltigkeit–Transformation von Geschäftsmodellen und Unternehmenspraxis (pp. 99-120). Berlin, Heidelberg: Springer Berlin Heidelberg.

[41]. Karnik, N., Bora, U., Bhadri, K., Kadambi, P. and Dhatrak, P., 2022. A comprehensive study on current and future trends towards the characteristics and enablers of industry 4.0. Journal of Industrial Information Integration, 27, p.100294.
[42]. Kaur, R., Gabrijelčič, D. and Klobučar, T., 2023. Artificial intelligence for Cyber Security: Literature review and future research directions. Information Fusion, p.101804.
[43]. Kaur, R., Gabrijelčič, D. and Klobučar, T., 2023. Artificial intelligence for Cyber Security: Literature review and future research directions. Information Fusion, p.101804.
[44]. Knapp, E.D., 2024. Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Elsevier.
[45]. Krima, S., Toussaint, M. and Feeney, A.B., 2020. Toward model-based integration specifications to secure the extended enterprise. Smart and Sustainable Manufacturing Systems, 4(1), pp.95-102.
[46]. Kuipers, S. and Schonheit, M., 2022. Data breaches and effective crisis communication: a comparative analysis of corporate reputational crises. Corporate Reputation Review, 25(3), pp.176-197.
[47]. Lehto, M., 2022. Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.
[48]. Lu, Y., 2017. Industry 4.0: A survey on technologies, applications and open research issues. Journal of industrial information integration, 6, pp.1-10.
[49]. Benson, M., 2022. Towards a Research Guide for Cyber Threat Intelligence (Doctoral dissertation, Utica University).
[50]. Malatji, M. and Tolah, A., 2024. Artificial intelligence (AI) Cyber Security dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics, pp.1-28.
[51]. Markevych, M. and Dawson, M., 2023, July. A review of enhancing intrusion detection systems for Cyber Security using artificial intelligence (ai). In International conference Knowledge-based Organization (Vol. 29, No. 3, pp. 30-37).
[52]. Möller, D.P., 2023. Cyber Security in digital transformation. In Guide to Cyber Security in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 1-70). Cham: Springer Nature Switzerland.
[53]. Niloy, A.C., Bari, M.A., Sultana, J., Chowdhury, R., Raisa, F.M., Islam, A., Mahmud, S., Jahan, I., Sarkar, M., Akter, S. and Nishat, N., 2024. Why do students use ChatGPT? Answering through a triangulation approach. Computers and Education: Artificial Intelligence, 6, p.100208.
[54]. Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H., 2022. The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, p.102494.
[55]. Pilli, L., 2023. Analysis of Artificial Intelligence Techniques to Detect, Prevent, Analyze and Respond to Malware.
[56]. Polančič, G. and Orban, B., 2023. An experimental investigation of BPMN-based corporate communications modeling. Business Process Management Journal, 29(8), pp.1-24.
[57]. Rajkumar, V.S., Ştefanov, A., Presekal, A., Palensky, P. and Torres, J.L.R., 2023. Cyber attacks on power grids: Causes and propagation of cascading failures. IEEE Access.
[58]. Timtchenko, I., 2023. Strengthening Ukrainian Resiliency in the Medium to Long Term.
[59]. Vargas, P. and Tien, I., 2023. Impacts of 5G on cyber-physical risks for interdependent connected smart critical infrastructure systems. International Journal of Critical Infrastructure Protection, 42, p.100617.
[60]. Roy, R., Laha, A. and Chakraborty, A., 2024. Artificial Intelligence in Protective Gear Design and Maintanence. In Biomedical Research Developments for Improved Healthcare (pp. 55-77). IGI Global.
[61]. Safitra, M.F., Lubis, M. and Fakhrurroja, H., 2023. Counterattacking cyber threats: A framework for the future of Cyber Security. Sustainability, 15(18), p.13369.
[62]. Santiago, D. and Nery, I., 2023. Industry Contribution: Digital signature as a method to strengthen enterprise risk management practices across the US government. Digital Evidence & Elec. Signature L. Rev. IC, 20, p.1.
[63]. Sarker, I.H., 2023. Multi-aspects AI-based modeling and adversarial learning for Cyber Security intelligence and robustness: A comprehensive overview. Security and Privacy, 6(5), p.e295.
[64]. Sindiramutty, S.R., 2023. Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence. arXiv preprint arXiv:2401.00286.
[65]. Stutz, D., de Assis, J.T., Laghari, A.A., Khan, A.A., Andreopoulos, N., Terziev, A., Deshpande, A., Kulkarni, D. and Grata, E.G., 2024. Enhancing Security in Cloud Computing Using Artificial Intelligence (AI). Applying Artificial Intelligence in Cyber Security Analytics and Cyber Threat Detection, pp.179-220.
[66]. Thakur, M., 2024. Cyber security threats and countermeasures in digital age. Journal of Applied Science and Education (JASE), pp.1-20.
[67]. Tomaz, V., Moreira, D. and Souza Cruz, O., 2023. Criminal reactions to drug-using offenders: A systematic review of the effect of treatment and/or punishment on reduction of drug use and/or criminal recidivism. Frontiers in Psychiatry, 14, p.935755.
[68]. Vegesna, V.V., 2023. Enhancing cyber resilience by integrating AI-Driven threat detection and mitigation strategies. Transactions on Latest Trends in Artificial Intelligence, 4(4).
[69]. VICTOR-MGBACHI, T.O.Y.I.N., 2024. Navigating Beyond Compliance: Understanding Your Threat Landscape and Vulnerabilities. Cyber Security
[70]. Xu, T., Singh, K. and Rajivan, P., 2023. Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks. Applied Ergonomics, 108, p.103908.

[71]. Yang, J., Rao, Y., Cai, Q., Rigall, E., Fan, H., Dong, J. and Yu, H., 2024. MLNet: An multi-scale line detector and descriptor network for 3D reconstruction. Knowledge-Based Systems, p.111476.
[72]. Marion Toussaint , Sylvère Krima , Hervé Panetto ,2024. Industry 4.0 data security: A Cyber Security frameworks review, https://doi.org/10.1016/j.jii.2024.100604
[73]. Fabricio Mera-Amores, Henry N. Roa. Enhancing Information Security Management in Small and Medium Enterprises (SMEs) Through ISO 27001 Compliance, pp 197–207
[74]. Khalifa AL-Dosari and Noora Fetais, 2023, Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach, Electronics 2023, 12(17), 3629; https://doi.org/10.3390/electronics12173629
[75]. Gordon, MD, 2020 Vulnerability in Research: Basic Ethical Concepts and General Approach to Review, https://doi:10.31486/toj.19.0079
[76]. Mark D. Wilkinson, Michel Dumontier. The FAIR Guiding Principles for scientific data management and stewardship. Article number: 160018 (2016)
[77]. Davide Fucci, Emil, Felderer . Evaluating software security maturity using OWASP SAMM: Different approaches and stakeholders perceptions. https://doi.org/10.1016/j.jss.2024.112062
[78]. ISO 27001(2022) Standard ISO/IEC 27001:2022 Information security, Cyber Security and privacy protection Information security management systems (third edition)
[79]. Ahmed HSA (2023) A guide to the updated ISO/IEC 27002:2022 standard, part 1, @ISACA
[80]. ISO/IEC (2022) ISO/IEC AWI 27090: Cyber Security artificial intelligence guidance for addressing security threats and failures in artificial intelligence systems. https://www.iso.org/standard/56581.html Accessed 25 Aug 2023
[81]. P. Sugiarto and Y. Suryanto, "Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index based on ISO 27001 : 2013," Int. J. Mech. Eng., vol. 7, no. 2, pp. 3607–3614, 2022
[82]. P. Sundari and Wella, "SNI ISO / IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)," Ultim. InfoSys J. Ilmu Sist. Inf., vol. 12, no. 1, pp. 35–42, 2021.
[83]. N. V Syreyshchikova, D. Y. Pimenov, T. Mikolajczyk, and L. Moldovan, "Information Safety Process Development According to ISO 27001 for an Industrial Enterprise," Procedia Manuf., vol. 32, pp. 278–285, 2019, https://doi:10.1016/j.promfg.2019.02.21
[84]. Fabricio Mera-Amores & Henry N. Roa, Enhancing Information Security Management in Small and Medium Enterprises (SMEs) Through ISO 27001 Compliance
[85]. Doe, J., Smith, A., & Johnson, B. (2023). "Limitations of ISO 27001 in Cyber Security: A Critical Review." Journal of Information Security Studies, 8(2), 55-68.
[86]. Heinl, MP., Pursche, M., Puch, N., Peters, SN., & Others. (2023). From Standard to Practice:
[87]. Towards ISA/IEC 62443-Conform Public Key Infrastructures. Conference on Computer.
[88]. Iturbe, E., Rios, E., Mansell, J., & Others. (2023). Information Security Risk Assessment Methodology for Industrial Systems Supporting ISA/IEC 62443 Compliance. Conference on Electrical.
[89]. IACS. (2024). Topic 3.1 ISA/IEC 62443. Policy.
[90]. Toussaint, M., Krima, S., Panetto, H. (2024). Industry 4.0 data security: a Cyber Security frameworks review. Journal of Industrial Information.
[91]. Heinl, MP., Pursche, M., Puch, N., Peters, SN., & Others. (2023). From Standard to Practice: Towards ISA/IEC 62443-Conform Public Key Infrastructures. Conference on Computer.
[92]. Gordy, F. (2024). Integrating cyber into new construction and commissioning across asset classes. Corporate Real Estate Journal.
[93]. Braun,V., & Clarke,V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.
[94]. Bryman,A. (2016). Social Research Methods. Oxford University Press.
[95]. Creswell, J. W., & Poth, C. N. (2018). Qualitative Inquiry and Research Design: Choosing Among Five Approaches. Sage Publications.
[96]. Yin, R. K. (2018). Case Study Research and Applications: Design and Methods. Sage Publications.