International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

AI-Enhanced Cyber Incident Response and Recovery

Sunil Chahal

ConceptsIT, Inc.

Abstract: ***The project on AI-enhanced Cyber Incident Response and Recovery examines how to better integrate cutting-edge technology like machine learning and automation tools. Data privacy, bias reduction, and legal compliance are all ethical issues. Resource shortages, technological limits, and security hazards are problems. Strong security measures, the development of skills, and emergency preparedness are all components of mitigation techniques. The initiative emphasizes responsible and ethical cybersecurity practices while aiming to increase threat detection speed, decrease false positives, and improve overall cybersecurity outcomes.***

Keywords: Cyber Incident Response, Machine Learning, Bias Mitigation, Threat Detection, False Positives, Contingency Planning

1. Introduction

The threat of cyber incidents has grown large. An incident response and recovery paradigm has changed necessary to address these threats. The use of "artificial intelligence (AI)" in cyber incident management has facilitated this transformation. AI's quick detection, analysis, and mitigation of cyber threats make it a powerful tool for enhancing cybersecurity. In order to better our digital defenses and quicken the return to regularity after an event, this article has analyzed the area of AI-enhanced cyber incident response and recovery. Organizations have proactively tackled cyber risks and decreased the threat caused by malicious actors by utilizing the capabilities of AI.

2. Research Background

Our cybersecurity measures need to adjust in step with the constant development of cyber threats. The urgent need to enhance cyber stability is the driving force behind this study. "Artificial intelligence (AI)" is a powerful method in this effort, providing automated threat identification, behavioral analysis, and real-time reaction capabilities that outperform human capabilities. Anomalies in network traffic have been recognized by machine learning models, identifying possible dangers beforehand. While autonomous response techniques have quickly reduced attacks and isolated compromised systems, natural language processing helps parse and comprehend threat data. The integration of AI-driven solutions into cyber event response and recovery procedures is examined in this study, and their effectiveness in speeding up reaction times, limiting damage, and improving overall cybersecurity posture is evaluated.

Aim and objectives

Aim:
The main aim of this study is to analyze the integration of Artificial Intelligence (AI) into cyber incident response and recovery, enhancing cyber stability and reducing threats in current digital environments.

Objectives:

- To evaluate the effectiveness of AI in accelerating cyber threat detection and containment.
- To examine the scalability and adaptability of AI solutions in diverse organizational contexts.
- To evaluate the impact of AI-enhanced incident response on minimizing damage and data loss.
- To provide practical recommendations for implementing AI-driven cyber incident response strategies for enhanced cybersecurity.

3. Literature Review

3.1 Effectiveness of AI in Cyber Threat Detection and Containment

A key focus of current cybersecurity research is the efficiency of artificial intelligence (AI) in the identification and control of cyber threats. Systems powered by AI have proven to be incredibly effective at enhancing conventional threat detection techniques [19]. AI can quickly evaluate massive volumes of data, identifying patterns suggestive of possible risks that could go unnoticed otherwise through the use of sophisticated algorithms and artificial intelligence models. One of AI's key advantages is its capacity to spot irregularities in network activity and user behavior, which enables it to quickly spot departures from predefined baselines. This dynamic method is especially useful in identifying complex, changing threats that might evade signature-based detection systems. AI also offers a level of responsiveness that is essential in the continually changing world of cyber threats since it can adjust in real time to new attacks and attack vectors [20]. The spread and effects of cyber events have also been shown to be significantly reduced by containment techniques powered by AI.

Figure 2.1.1: AI in Cybersecurity

Licensed Under Creative Commons Attribution CC BY

AI can isolate hacked devices, limit movement downstream within networks, and launch effective countermeasures by automating the response process. This not only reduces the threat's potential harm but also gives security teams crucial time to look into and stop the occurrence. It is crucial to remember that while AI greatly improves threat identification and containment, it works best when integrated into a comprehensive cybersecurity architecture [22]. AI should be integrated into a larger strategy that includes preemptive threat hunting, personnel training, and continuing vulnerability assessments rather than replacing current security procedures. Additionally, it is crucial to continuously improve and train AI models to ensure their effectiveness in the face of shifting threat environments.

2.2 Scalability and Adaptability of AI Solutions in Diverse Organizational Contexts

When putting sophisticated cybersecurity measures into practice, accessibility, and adaptability of AI systems in various organizational contexts are key factors to take into account [23]. It is essential that AI-driven solutions may be customized to fit the unique requirements and complexity of various contexts, as enterprises differ substantially in size, organization, and technical infrastructure. The capacity of an AI system to manage growing workloads as well as information volumes without sacrificing performance is referred to as scalability. This translates to the ability of AI to efficiently keep track of and react to threats in contexts ranging from small businesses to giant multinational firms in the field of cybersecurity [24]. Scalable AI solutions can analyze and interpret enormous amounts of data produced by various systems, assuring that they continue to function as intended even as the organization's internet presence grows in size and complexity.

Figure 2.2.1: Human Centered AI

The ability of an AI system to flexibly merge with the technologies and procedures already in place within an organization is referred to as adaptability. This is crucial since organizations frequently already have established infrastructures, programs, and workflows [25]. These pre-existing systems can be easily enhanced in functionality and have security holes filled by an adaptable AI solution. It should be adaptable enough to be tailored to the particular needs and compliance criteria of various industries and sectors.

2.3 Impact of AI-Enhanced Incident Response on Minimizing Damage and Data Loss

In the field of cybersecurity, the incorporation of AI-enhanced crisis management mechanisms has been shown to have a significant influence on reducing damage and data loss [26]. Organizations can quickly identify, contain, and neutralize threats by using the speed and accuracy of AI algorithms, thereby minimizing the potential damage caused by cyber disasters. The window of risk is greatly reduced by AI's capacity to identify threats in immediate form and take automatic action in response [27]. This quick response time can stop threats from moving laterally throughout a network, stopping the incident's escalation, and reducing its potential impact.

Figure 2.3.1: Impact of AI on Cybersecurity

Additionally, AI has the ability to autonomously isolate infected systems, limiting further compromise and protecting vital assets. AI-enhanced incident response improves incident response speed while also improving threat identification precision [28]. AI systems can identify patterns indicating sophisticated attack strategies that may defy standard signature-based detection techniques through sophisticated data analysis and machine learning. Since there are fewer erroneous positives and negatives as a result of the higher accuracy, genuine threats are handled quickly with the least amount of interference to regular operations. Additionally, AI's constant surveillance capabilities allow for the detection of undetectable anomalies that are subtle and low-profile [29]. This preventative strategy enables the early detection and containment of threats, minimizing their potential impact and preventing data loss.

2.4 Practical Recommendations for Implementing AI-Driven Cyber Incident Response Strategies

AI-driven cyber event response solutions must be implemented with care and in detail. Following are some helpful suggestions to support organizations in this endeavor:

Integrate AI-driven incident response at the outset of a complete cybersecurity framework. Make sure it enhances the security measures already in place, such as anti-virus programs, firewalls, and detection systems for intrusions [30].

Adaptation and Instruction: Adapt AI models to the unique requirements and surroundings of the organization. Train the

Licensed Under Creative Commons Attribution CC BY

AI system to spot patterns and anomalies specific to the company's network using pertinent datasets.

Figure 2.4.1: AI for Cybersecurity

Updates and Continuous Monitoring: Implement ongoing performance evaluation of the AI system. Update and improve the AI models frequently to account for shifting threat environments and organizational changes. Maintain a significant human component in incident response through human oversight and collaboration [31]. In order to confirm alarms, carry out thorough examinations, and make crucial judgments, security experts need to collaborate with AI.

Data Security and Compliance: Make that AI-driven response to incidents tactics abide by data privacy laws and compliance requirements. Utilize AI to improve security while protecting sensitive data. Conduct regular simulations and tests of penetration to evaluate the efficacy of AI-driven response plans. Incident Simulation and Testing. Determine where there is room for development and adjust response to incident plans accordingly [32].

Sharing of knowledge and training: Encourage an understanding of cybersecurity within the workforce. To improve the efficiency of the AI system, offer training on identifying and reporting potential dangers.

2.5 Literature Gap

The literature that is currently available on AI-driven cyber event response is mainly concerned with technological details and effectiveness metrics. Comprehensive research addressing the socio-organizational ramifications is noticeably lacking, nevertheless. Only a little amount of research has been done on the dynamics of human-AI collaboration, ethical issues, and long-term organizational effects of applying AI-enhanced crisis response tactics. Further research is necessary to fill this gap and gain an in-depth awareness of AI in security.

4. Methodology

Choice of Methods

In order to address the complexity of the topic "AI-Enhanced Cyber Incident Response and Recovery," a multidimensional approach needs to be taken. Data from surveys and questionnaires has been analyzed using statistical tools and methodologies, giving quantitative insights into the use of AI in incident response [33]. Thematic analysis has been used to examine qualitative data from case studies and interviews to find recurrent themes and patterns. Quantitative information on the frequency and efficiency of AI integration in incident response needs to be obtained by conducting surveys among enterprises and cybersecurity specialists. In-depth case studies of businesses that have put AI-driven incident response systems in place offer insightful qualitative information.

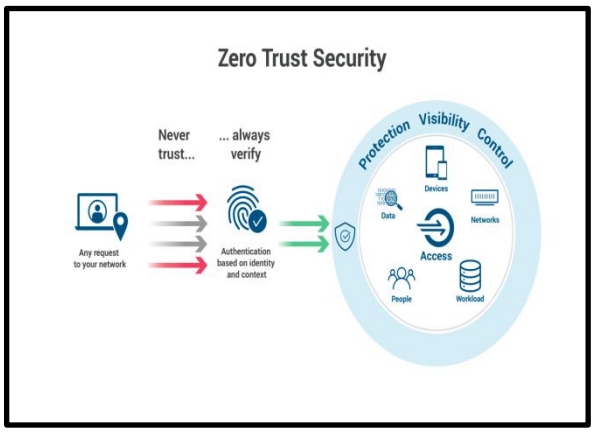

Figure 3.1: Zero Trust is a security architecture

These case studies have helped to show the difficulties and give ways to fight them in the real world through AI integration. Patterns, anomalies, and the effectiveness of AI in threat detection and response have been discovered by processing and analyzing massive datasets of cyber event records using data analysis techniques such as machine learning algorithms. Controlled studies need to be done to create model cyber events and evaluate the performance of AI-driven response systems in comparison to more conventional techniques. This approach enables the evaluation of AI's effects in a controlled setting.

Justification of Chosen Methods

In order to acquire structured data from a wide sample of businesses and cybersecurity experts, surveys and questionnaires are used to collect quantitative data. The frequency and effectiveness of AI integration have been evaluated in incident response; this quantitative data is crucial. A strong foundation for assessing this data is provided by statistical tools and procedures, which give insightful information about the use and effects of AI. Case studies and interviews are used in the research to add qualitative depth. Case studies of companies that have put AI-driven incident response systems in place provide practical insights by identifying problems and potential solutions.

Licensed Under Creative Commons Attribution CC BY

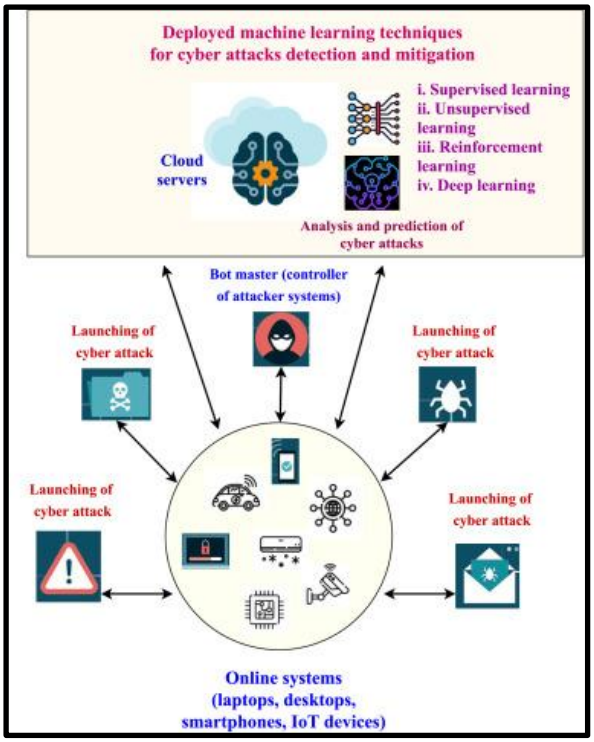

Figure 3.2: Deploying Cyber Incident Response and Recovery

Expert interviews provide a humane perspective by recording experiences, viewpoints, and suggestions relating to the integration of AI. In order to find trends and anomalies, it is essential to process and analyze massive datasets of cyber event records using data analysis techniques, including machine learning algorithms [34]. This quantitative technique provides factual proof of AI's efficiency in danger identification and response, which supports the qualitative findings. The effectiveness of AI in a controlled environment needs to be assessed through controlled studies. This approach makes it possible to compare AI-driven response systems directly to traditional methods, allowing for a comprehensive evaluation of AI's impacts.

Tools and technology

A variety of cutting-edge tools and technologies created to improve an organization's cybersecurity posture are used in the technique for AI-enhanced Cyber Incident Response and Recovery. Deep neural networks and random forests are only two examples of machine learning techniques that are used to examine network traffic and system behavior for patterns and anomalies [1]. Splunk and IBM QRadar are two examples of Security Information and Event Management (SIEM) tools that are useful for gathering, correlating, and analyzing data from many sources to quickly identify potential risks [2]. Systems that detect and respond to suspicious endpoint activity in real-time, like CrowdStrike and Carbon Black, are known as endpoint detection and response (EDR) systems. Utilizing threat intelligence feeds like MISP and services like VirusTotal also offer vital information about new threats and vulnerabilities. While digital forensics tools like EnCase and Autopsy assist in event investigation, automation solutions like Ansible and Phantom streamline response efforts [3]. The use of robust data backup and recovery technologies, incident response playbooks, cybersecurity orchestration platforms, and cloud security solutions empowers enterprises to successfully combat cyber-attacks and assure resilience [4].

Ethical consideration

Personally, it is crucial to preserve the privacy and data of those participating in incident response, both personally and professionally. Mechanisms for clear consent and communication should be set up for data collection and processing [5]. When using AI, bias mitigation is essential to ensuring impartial and fair decision-making. Additionally, it is critical to uphold legal and regulatory frameworks and safeguard the confidentiality of sensitive information [6]. Actions taken in response to incidents should be guided by ethical principles to avoid technological abuse and protect parties from inadvertent harm. This helps to sustain ethical norms throughout the project's execution, continuous monitoring, and auditing of AI systems for ethical compliance must be embedded into the framework [7].

Summary

The AI-enhanced Cyber Incident Response and Recovery initiative makes use of cutting-edge technology like machine learning, SIEM systems, and automation tools. Ethical and accountable procedures are ensured by placing a strong emphasis on issues including data privacy, bias reduction, and adherence to regulatory frameworks. The thorough methodology includes solutions for data recovery, incident response automation, and threat detection, allowing businesses to effectively handle cybersecurity issues. This project will improve cybersecurity measures in a variety of industries by aligning with the need to protect sensitive information, reduce risks, and uphold ethical standards.

5. Result and Discussion

Theme 1: Effectiveness of AI Integration

The analysis mainly focuses on evaluating the effects of AI technologies, like machine learning and automation tools, on the effectiveness and precision of various parts of incident response and recovery operations. The use of AI has significantly increased the speed at which threats are detected. The system can quickly monitor and spot irregularities in network traffic and system behavior using machine learning techniques, which cuts down on the amount of time it takes to find possible threats [8]. The organization's capacity to respond quickly to security problems is improved by the shortening of the detection time. Artificial intelligence utilization helps reduce false positives. False positive resources are reduced by allocating more effectively, and the unneeded workload placed on cybersecurity teams is reduced [9].

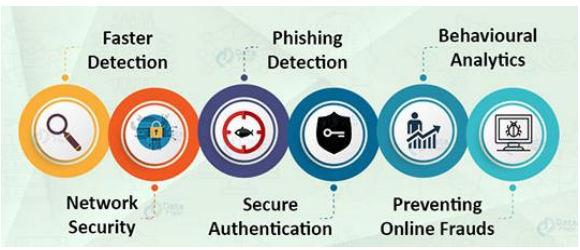

Figure 4.1: AI in cyber security

Licensed Under Creative Commons Attribution CC BY

The overall results of cybersecurity are improved with AI integration. According to the report, incident response and recovery methods that use AI are characterized by improved precision and efficacy in spotting and reducing security threats. A higher level of protection for sensitive data and important assets results from this development. The thematic analysis of AI integration's performance highlights its enormous advantages in the context of cyber incident response and recovery [10]. The experiment shows how AI technologies speed up threat detection, lower false positives, and enhance cybersecurity outcomes overall. These results highlight AI's potential for further development in the field of cybersecurity and confirm the critical role it plays in enhancing incident response skills [11].

Theme 2: Ethical and Legal Implications

The analysis shows a strong focus on data privacy and protection as a fundamental ethical principle. It is crucial to guarantee the integrity and security of sensitive data. The privacy of people and organizations involved in the incident response process is protected which strongly emphasizes the establishment of clear communication channels and consent processes [12]. The social concerns about data security and privacy are in line with this ethical obligation. The initiative acknowledges the need to address algorithmic biases that may unintentionally discriminate against particular people or groups given the use of AI technologies [13]. In order to maintain fair and unbiased decision-making during the incident response and recovery procedures, ethical considerations require active monitoring and reducing biases.

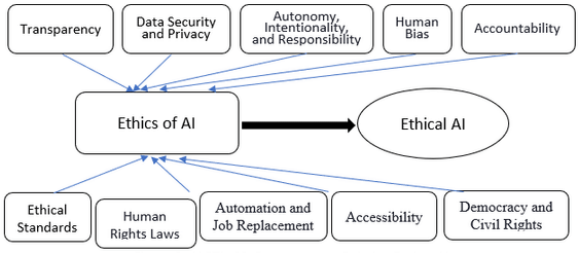

Figure 4.2: Ethical consideration

The report emphasizes the project's commitment to following statutory and regulatory requirements. This includes abiding by all national and international cybersecurity rules and regulations [14]. The project is aware that upholding legal compliance not only reduces risks but also promotes stakeholder trust. The project's dedication to ethical data handling, bias reduction, and compliance with cybersecurity laws and regulations is highlighted by the thematic examination of ethical and legal ramifications [15]. These factors emphasize the project's commitment to ethical and legal norms in the field of cybersecurity and form the basis for the appropriate deployment of AI-enhanced incident response and recovery operations.

Theme 3: Challenges and Mitigation Strategies

The project recognizes that integrating AI technology demands significant resources, such as infrastructure, infrastructure investments, and trained individuals. The lack of these resources may make it difficult to use AI effectively in incident response. The initiative covers tactics including training and skill development programs to make sure that staff members are properly equipped to realize the promise of AI [16]. Limitations in technology are a significant barrier. Despite their strength, AI systems have weaknesses and limitations. The analysis emphasizes how crucial it is to comprehend these constraints in order to avoid relying too heavily on AI and to create backup plans in case of technological setbacks [17].

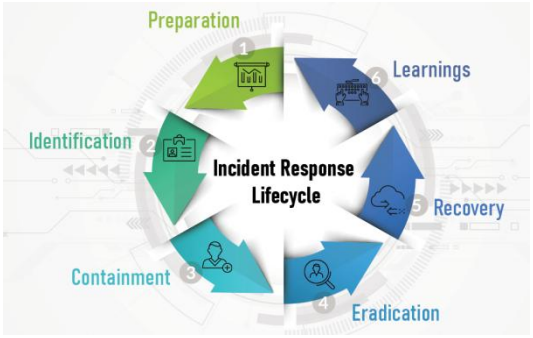

Figure 4.3: Incidence response lifecycle

This strategy guarantees the robustness of incident response procedures. This is acknowledged that the use of AI could pose security problems. The mitigating tactics include training in new skills, making plans for emergencies, and taking strict security precautions. These results highlight the project's dedication to proactively addressing issues and ensuring the successful and secure integration of AI in Cyber Incident Response and Recovery operations [18].

6. Conclusion

An important development in cybersecurity has been made using artificial intelligence (AI) in cyber event response and recovery. This study has demonstrated how quickly AI has identified and balanced attacks, decreasing cyber threats and boosting overall cyber stability. It is crucial to identify the ongoing difficulties, such as the interpretability of AI and potential malicious attacks. In order to achieve the best results, businesses need to properly integrate AI-driven solutions in conjunction with human knowledge. In order to reduce malicious attacks and protect digital assets as the threat landscape changes, incident management has used AI as an important component.

7. Recommendation

Invest in AI Integration: Allocate funds to include AI technology in incident response and recovery procedures as well as concentrating on automated response systems and real-time threat identification.

Enhance Data Privacy: Use strong data privacy controls when using AI-driven incidents that have responded systems to protect sensitive data.

Regular Evaluation: Periodically analyze the performance of AI solutions as well as make adjustments in order to complete changing threats and organizational requirements.

Licensed Under Creative Commons Attribution CC BY

Continuous Training: Maintaining cybersecurity teams' knowledge of AI technology through ongoing training that has enabled them to work effectively with AI systems.

Adopt Ethical Practices: Ethical use of AI needs to be ensured d by following moral principles and correcting any potential biases in AI algorithms.

8. Future Work

Future work has been exploring more into the potential of AI to fight new cyber threats such as AI-driven attacks. It is also important to look at the ethical and legal modification of incident response boosted by AI [35]. This field has been advanced by creating established criteria for AI-powered incident response systems and looking at ways to improve the interpretability of AI models. Researching the use of AI in certain sectors, such as banking or healthcare, has provided insights relevant to those businesses. The synergy between quantum computing and AI for effective cybersecurity has also become a profitable area of study as quantum computing has developed and updated.

References

[1] Fysarakis, K., Lekidis, A., Mavroeidis, V., Lampropoulos, K., Lyberopoulos, G., Vidal, I.G.M., i Casals, J.C.T., Luna, E.R., Sancho, A.A.M., Mavrelos, A. and Tsantekidis, M., 2023, July. PHOENI2X–A European Cyber Resilience Framework with Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 538-545). IEEE.

[2] Fysarakis, K., Lekidis, A., Mavroeidis, V., Lampropoulos, K., Lyberopoulos, G., Vidal, I.G.M., i Casals, J.C.T., Luna, E.R., Sancho, A.A.M., Mavrelos, A. and Tsantekidis, M., 2023, July. PHOENI2X–A European Cyber Resilience Framework with Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange. In 2023 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 538-545). IEEE.

[3] Kaur, R., Gabrijelčič, D. and Klobučar, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, p.101804.

[4] Stroup, R.L., Niewoehner, K.R., Apaza, R.D., Mielke, D. and Mäurer, N., 2019, September. Application of AI in the NAS–the Rationale for AI-Enhanced Airspace Management. In 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC) (pp. 1-10). IEEE.

[5] Panoff, M., Yu, H., Shan, H. and Jin, Y., 2022. A Review and Comparison of AI-enhanced Side Channel Analysis. ACM Journal on Emerging Technologies in Computing Systems (JETC), 18(3), pp.1-20.

[6] Ognjanović, I. and Šendelj, R., 2020. AI enhanced services in person-centred care in neurology. In New Technologies, Development and Application III 6 (pp. 522-529). Springer International Publishing.

[7] Chaithanya, B.N. and Brahmananda, S.H., 2022. AI-enhanced Defense Against Ransomware Within the Organization's Architecture. Journal of Cyber Security and Mobility, pp.621-654.

[8] Bodemer, O., 2023. Empowering Athletes with AI and Blockchain: A New Era of Personalized Training, Secure Data Management, and User Engagement.

[9] Karnavel, K., Arunkumar, G., Eucharista, M.A.A. and Mercy, M.M., 2023. AI-enhanced Metric Package for Assessing Reliability in Service Composition for Drug Discovery and Development. Latin American Journal of Pharmacy, 42(1), pp.209-219.

[10] Wang, C., He, T., Zhou, H., Zhang, Z. and Lee, C., 2023. Artificial intelligence enhanced sensors-enabling technologies to next-generation healthcare and biomedical platforms. Bioelectronic Medicine, 9(1), p.17.

[11] Li, B., Feng, Y., Xiong, Z., Yang, W. and Liu, G., 2021. Research on AI security enhanced encryption algorithm of autonomous IoT systems. Information sciences, 575, pp.379-398.

[12] Helkala, K., Cook, J., Lucas, G., Pasquale, F., Reichberg, G. and Syse, H., 2022. AI in Cyber Operations: Ethical and Legal Considerations for End-Users. In Artificial Intelligence and Cybersecurity: Theory and Applications (pp. 185-206). Cham: Springer International Publishing.

[13] Talib, M.M. and Crook, M.S., 2023. AI-Enhanced Power Management System for Buildings: A Review and Suggestions. Journal Européen des Systèmes Automatisés, 56(3).

[14] Carter, J., Feddema, J., Kothe, D., Neely, R., Pruet, J., Stevens, R., Balaprakash, P., Beckman, P., Foster, I., Iskra, K. and Ramanathan, A., 2023. Advanced Research Directions on AI for Science, Energy, and Security: Report on Summer 2022 Workshops.

[15] Lytras, M.D. and Visvizi, A., 2021. Artificial intelligence and cognitive computing: Methods, technologies, systems, applications, and policy making. Sustainability, 13(7), p.3598.

[16] Johnson, J., 2021. The AI-cyber security nexus. In Artificial intelligence and the future of warfare (pp. 150-167). Manchester University Press.

[17] Wang, X., 2023. Ai-Enhanced Software Vulnerability and Security Patch Analysis (Doctoral dissertation, George Mason University).

[18] Bodemer, O., 2023. Enhancing Individual Sports Training through Artificial Intelligence: A Comprehensive Review. Eng OA, 1(2), pp.111-119.

[19] Blauth, T.F., Gstrein, O.J. and Zwitter, A., 2022. Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, *10*, pp.77110-77122.

[20] Arkouli, Z., Kokotinis, G., Michalos, G., Dimitropoulos, N. and Makris, S., 2021. AI-enhanced cooperating robots for reconfigurable manufacturing of large parts. *IFAC-PapersOnLine*, *54*(1), pp.617-622.

[21] Radanliev, P., De Roure, D., Page, K., Nurse, J.R., Mantilla Montalvo, R., Santos, O., Maddox, L.T. and Burnap, P., 2020. Cyber risk at the edge: current and future trends on cyber risk analytics and artificial

Licensed Under Creative Commons Attribution CC BY

intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, *3*(1), pp.1-21.

[22] Mura, A., Maier, M., Ballester, B.R., De la Torre Costa, J., López-Luque, J., Gelineau, A., Mandigout, S., Ghatan, P.H., Fiorillo, R., Antenucci, F. and Coolen, T., 2022. Bringing rehabilitation homes with an e-health platform to treat stroke patients: study protocol of a randomized clinical trial (RGS@ home). *Trials*, *23*(1), pp.1-12.

[23] Slamnik-Kriještorac, N., Botero, M.C., Cominardi, L., Latré, S. and Marquez-Barja, J.M., 2022, January. Building Realistic Experimentation Environments for AI-enhanced Management and Orchestration (MANO) of 5G and beyond V2X systems. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 437-440). IEEE.

[24] Nerella, S., Guan, Z., Siegel, S., Zhang, J., Khezeli, K., Bihorac, A. and Rashidi, P., 2023. AI-Enhanced Intensive Care Unit: Revolutionizing Patient Care with Pervasive Sensing. *arXiv preprint arXiv:2303.06252*.

[25] Ansari, F. and Kohl, L., 2022. Ai-Enhanced Maintenance for building resilience and viability in supply chains. In *Supply Network Dynamics and Control* (pp. 163-185). Cham: Springer International Publishing.

[26] Kollu, P.K., Kumar, K., Kshirsagar, P.R., Islam, S., Naveed, Q.N., Hussain, M.R. and Sundramurthy, V.P., 2022. Development of advanced artificial intelligence and IoT automation in the crisis of COVID-19 Detection. *Journal of Healthcare Engineering*, *2022*.

[27] Wei, H., Changzheng, S., Bo, H., Weizhan, L., Yue, S., Kaigui, X., Zio, E. and Wenyuan, L., 2022. Guest Editorial: Special Section on AI Enhanced Reliability Assessment and Predictive Health Management. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, *232*, pp.1-15.

[28] Oravec, J.A., 2022. The emergence of "truth machines"? Artificial intelligence approaches lie detection. *Ethics and Information Technology*, *24*(1), p.6.

[29] Oravec, J.A., 2022. The emergence of "truth machines"? Artificial intelligence approaches to lie detection. *Ethics approachesy*, *24*(1), p.6.

[30] Nishat, F., Hudson, S., Panesar, P., Ali, S., Litwin, S., Zeller, F., Candelaria, P., Foster, M.E. and Stinson, J., 2023. Exploring the Needs of Children and Caregivers to Inform Design of an AI-Enhanced Social Robot in the Pediatric Emergency Department. *Journal of Clinical and Translational Science*, pp.1-29.

[31] Ronchi, A.M., 2022. Human Factor, Resilience, and Cyber/Hybrid Influence. *Information & Security*, *53*(2), pp.221-239.

[32] Iturbe, E., Rios, E., Rego, A. and Toledo, N., 2023, August. Artificial Intelligence for next generation cybersecurity: The AI4CYBER framework. In Proceedings of the 18th International Conference on Availability, Reliability and Security (pp. 1-8).

[33] Bodemer, O., 2023. Empowering Athletes with AI and Blockchain: A New Era of Personalized Training, Secure Data Management, and User Engagement.

[34] Carter, J., Feddema, J., Kothe, D., Neely, R., Pruet, J., Stevens, R., Balaprakash, P., Beckman, P., Foster, I., Iskra, K. and Ramanathan, A., 2023. Advanced Research Directions on AI for Science, Energy, and Security: Report on Summer 2022 Workshops.

Licensed Under Creative Commons Attribution CC BY