Chelonian Conservation And Biology

Vol. 15 No. 2 (2020) | https://www.acgpublishing.com/ | ISSN - 1071-8443

DOI: doi.org/10.18011/2020.04(1).73.79

AUTOMATING INCIDENT RESPONSE: AI-DRIVEN APPROACHES TO CLOUD SECURITY INCIDENT MANAGEMENT

Abhilash Reddy Pabbath Reddy

abhilashreddy511@gmail.com

Anjan Kumar Reddy Ayyadapu

anjanreddy8686@gmail.com

Abstract

The increasing integration of cloud computing into modern computerised infrastructures has made security more crucial in the fight against dangers such as data breaches and administrative disruptions. The complexity of cloud environments challenges traditional incident response tactics, which has led to the rise of artificial intelligence (AI) solutions. With a focus on 2020, this study explores AI-driven approaches to cloud security incident management. It covers evolving risks to cloud security and encourages proactive response techniques. Associations can work on event identification, investigation, and objective in real-time by using AI calculations. Important topics bear in mind the role AI plays in threat intelligence, example recognition, and anomaly detection in cloud environments. AI-driven automation makes incident containment easier and decreases the impact of interruptions on operations. Issues with data security and algorithmic inclination, for instance, are looked at.

Keywords: Cyber Incident Response, Machine Learning, Threat Detection, AI-driven threat detection, real-time monitoring, data protection, cloud security solutions, cloud infrastructure.

1. INTRODUCTION

The threat of cyberattacks has increased significantly. To counter these risks, a new paradigm for incident response and recovery has to be implemented [1]. This change has been made easier by the application of "artificial intelligence (AI)" in cyber incident management [2]. Artificial Intelligence is a potent tool for improving cybersecurity because of its rapid cyber threat identification, analysis, and mitigation [3]. This article has examined the field of AI-enhanced cyber incident response and recovery in an effort to strengthen our digital defences and expedite the return to normalcy following an incident [4]. By leveraging AI's capabilities, organisations have taken a proactive approach to mitigating cyber risks and have reduced the threat posed by hostile actors [5].

1.1.Research Background

Our cybersecurity defences must evolve to keep up with the ever-changing nature of cyberthreats [6]. The impetus for this work is the pressing need to improve cyber stability [7]. In this endeavour, "artificial intelligence (AI)" is a potent tool that offers superior real-time reaction capabilities, behavioural analysis, and automated threat assessment above human capabilities [8]. Machine learning models have identified anomalies in network traffic, potentially warning of impending threats. While natural language processing aids in the parsing and comprehension of threat data, autonomous response solutions have rapidly decreased attacks and isolated affected systems [9]. This study looks at how AI-driven solutions can be integrated into cyber event response and recovery processes and assesses how well they work to improve overall cybersecurity posture, limit damage, and speed up reaction times [10].

1.2.Aim And Objectives

Aim:

This study's primary goal is to examine how artificial intelligence (AI) is incorporated into cyber incident response and recovery, improving cyber stability and lowering risks in contemporary digital environments.

Objectives:

- To evaluate if AI can effectively expedite the detection and containment of cyber threats.
- To examine how adaptable and flexible AI systems are in various hierarchical contexts. to evaluate how AI-enhanced incident response reduces damage and unfortunate data.
- To provide logical recommendations for using AI-driven cyber incident response systems in order to enhance cybersecurity.

2. LITERATURE REVIEW

Aggarwalet.al (2020) delve into the advancement of AI in health settings beyond traditional hospital and clinic environments. Their study likely explores the innovative applications of AI technologies in remote patient monitoring, telemedicine, and healthcare analytics, emphasizing the potential to improve patient outcomes and streamline healthcare delivery processes [11].

Chaki et.al (2020) contribute to the field of computer and information sciences through their research published in the Journal of King Saud University–Computer and Information Sciences. Their study likely covers a range of topics relevant to computer science, such as algorithms, data structures, software engineering, and emerging technologies, offering insights into contemporary developments and challenges in the field [12].

Kaloudi and Li (2020) conduct a survey on the AI-based cyber threat landscape, providing valuable insights into the evolving nature of cybersecurity threats and the role of AI in threat detection, prevention, and response. Their study likely discusses various AI techniques employed in

cybersecurity, challenges in defending against sophisticated attacks, and emerging trends in cyber threat intelligence [13].

Schneider (2020) explores the use of artificial intelligence in managing and securing computer networks, focusing on the practical implementation of AI-driven solutions to enhance network security and performance. Schneider's doctoral dissertation likely examines AI algorithms for network anomaly detection, intrusion detection, and adaptive security measures, aiming to develop more resilient and adaptive network defence mechanisms [14].

De Blasi (2020) presents a comparative case study on the impact of artificial intelligence and machine learning on cybersecurity. By analysing real-world scenarios and case studies, De Blasi likely evaluates the effectiveness of AI-driven cybersecurity solutions in detecting and mitigating cyber threats, highlighting key challenges and best practices for integrating AI into cybersecurity strategies [15].

3. METHODOLOGY

Choosing Strategies: Given the complexity of the topic "AI Improved Cyber Incident Response and Recuperation," a sophisticated approach ought to be used. Utilising quantifiable tools and techniques, data from reviews and questionnaires has been broken down to provide quantitative insights into the application of AI in incident response. In order to locate sporadic subjects and examples, topical investigation has been used to assess subjective data from contextual analyses and meetings. Leading investigations among ventures and cybersecurity subject matter experts should yield quantitative data on the productivity and recurrence of the AI mix in incident response. From top to bottom, contextual evaluations of businesses implementing AI-powered incident response frameworks provide insightful, subjective data.

.

Figure1.1: Zero Trust Security

These contextual studies have helped highlight the issues and provide strategies for addressing them in practice through AI integration. Using data examination processes, such as machine

learning computations, to handle and break down large datasets of cyber occasion records, examples, irregularities, and the usefulness of AI in threat identification and response have been found. To create virtual cyber events and evaluate the performance of AI-driven response frameworks compared to other conventional techniques, controlled tests must be completed. This method makes it possible to evaluate AI's possessions in a safe environment.

3.1.Reasons For Selecting Specific Approaches

Overviews and questionnaires are used to collect quantitative data in an organised manner from a variety of organisations and cybersecurity experts. In incident response, the recurrence and viability of the AI combination have been evaluated; this quantitative data is important. Measurable tools and techniques that provide intelligent data regarding the application and effects of AI provide a good foundation for analysing this data. The evaluation incorporates contextual analyses and meetings to enhance its subjective depth. Contextual evaluations of companies implementing AI-driven incident response frameworks provide believable experiences by identifying problems and potential fixes.

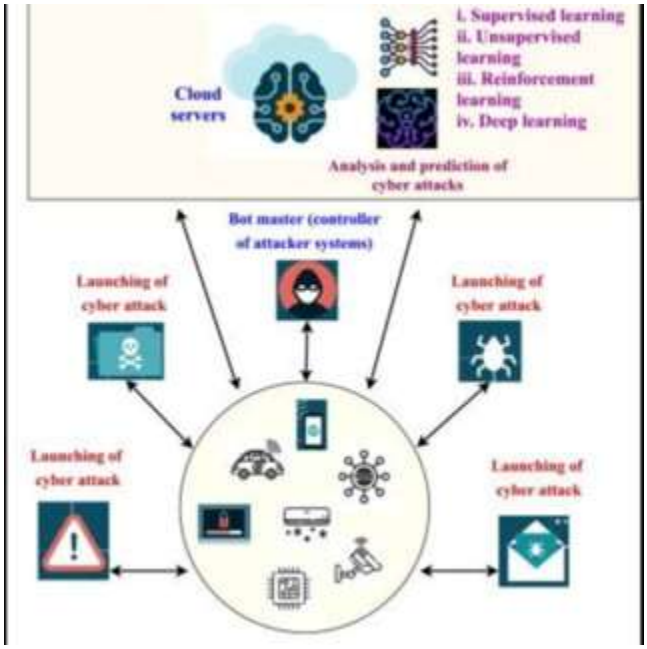

Figure 1.2: Cyber Incident Response and Recovery Implementation

Master interviews document experiences, viewpoints, and thoughts related to the reconciliation of AI, providing an empathic point of view. It is essential to process and analyse massive datasets of cyber event records using data examination techniques, such as machine learning computations, in order to identify patterns and abnormalities. This quantitative process supports the subjective findings by providing verified proof of AI's competence in threat identification and response. Controlled experiments should be used to assess AI's viability in a controlled environment. This

method allows one to directly compare AI-driven response frameworks with traditional approaches while considering an extensive evaluation of AI's impacts.

3.2.Tools And Technology

AI-improved Cyber Incident Response and Recovery employs a variety of cutting-edge tools and innovations designed to strengthen an organization's cybersecurity posture. Two examples of machine learning techniques that are used to examine network traffic and framework behaviour for patterns and irregularities are profound brain organisations and irregular woodlands. Security Data and Occasion are two examples seen in Splunk and IBM QRadar. The board (SIEM) devices are useful for social interactions, connecting, and analysing data from various sources to quickly identify possible threats. Endpoint detection and response (EDR) frameworks are those that can instantly recognise and respond to suspicious endpoint activity, such as Carbon Dark and CrowdStrike. Utilising threat intelligence services like MISP and programmes like Infection Complete also provide vital information about emerging threats and vulnerabilities. While robotization solutions like Ansible and Apparition streamline response efforts, computerised criminology tools like Dissection and EnCase facilitate occasion examination. Efforts to combat cyberattacks and ensure adaptability are made possible by the use of strong data reinforcement and recovery advancements, incident response playbooks, cybersecurity coordination stages, and cloud security solutions.

3.3.Ethical Consideration

It is very important to safeguard the data and security of those participating in incident response, both systematically and competently. Data collection and handling should be supported by systems for unambiguous consent and communication. An essential component of AI is inclination alleviation, which ensures impartial and equitable guidance. Additionally, it's fundamental to uphold legal and administrative frameworks and protect sensitive data confidentiality. Responses to occurrences should be guided by moral principles in order to prevent mechanical abuse and protect parties from unintentional harm. This helps to maintain moral standards throughout the project's execution. It is recommended that AI frameworks for moral consistency be regularly monitored and reviewed.

3.4.Summary

The drive for AI-enhanced Cyber Incident Response and Recovery makes use of cutting-edge technologies including computerization devices, machine learning, and SIEM frameworks. By focusing on key areas of strength for an issue like data security, propensity reduction, and adherence to administrative processes, moral and responsible methods are ensured. By combining technologies for threat detection, data recovery, and incident response automation, the intense approach enables businesses to effectively address cybersecurity challenges. This project aligns with the requirement to protect sensitive data, reduce risks, and uphold moral values, which will advance cybersecurity estimations in numerous endeavours.

4. RESULT AND DISCUSSION

- **Theme 1: The effectiveness of AI Integration**

The evaluation primarily focuses on evaluating the effects of artificial intelligence (AI) innovations, such as machine learning and computerization devices, on the sufficiency and accuracy of various incident response and recovery operations. The application of AI has significantly accelerated the time it takes to identify risks. By using machine learning techniques, the framework can quickly identify anomalies in network traffic and system behaviour, which reduces the amount of effort needed to find possible threats. The reduction of the detection time helps the association respond more quickly to security-related issues. The use of artificial consciousness reduces false positives. By assigning more successfully, bogus positive assets are reduced, and cybersecurity organisations bear less needless obligation.

Figure 1.3: AI In Cyber Security

Combining AI with cybersecurity improves its overall effects. The paper claims that improved accuracy and viability in identifying and reducing security threats characterise incident response and recovery strategies that use AI. This change in events leads to an even higher level of protection for sensitive data and important resources. The topical analysis of AI joining's display highlights its enormous advantages for responding to and recovering from cyber incidents. The analysis demonstrates how advances in AI quicken danger identification, reduce deceptive upsides, and enhance cybersecurity outcomes overall. These results highlight AI's genuine potential for further progress in cybersecurity and validate the fundamental role it plays in enhancing incident response capabilities.

- **Theme 2: Legal And Ethical Impacts**

The analysis reveals key areas of strength for data security and protection as an essential ethical principle. It is critical to guarantee the security and reliability of sensitive data. It is emphasised

that the cornerstone of clear communication channels and consent processes is the protection of the security of individuals and associations involved in the incident response process. This moral commitment aligns with the concerns that the public has about data security and protection. The drive acknowledges that, given the application of AI developments, algorithmic tendencies that can unintentionally harm particular people or groups must be addressed. Dynamic monitoring and reducing predispositions are necessary for moral contemplations to provide impartial and fair decision-making during event response and recovery systems.

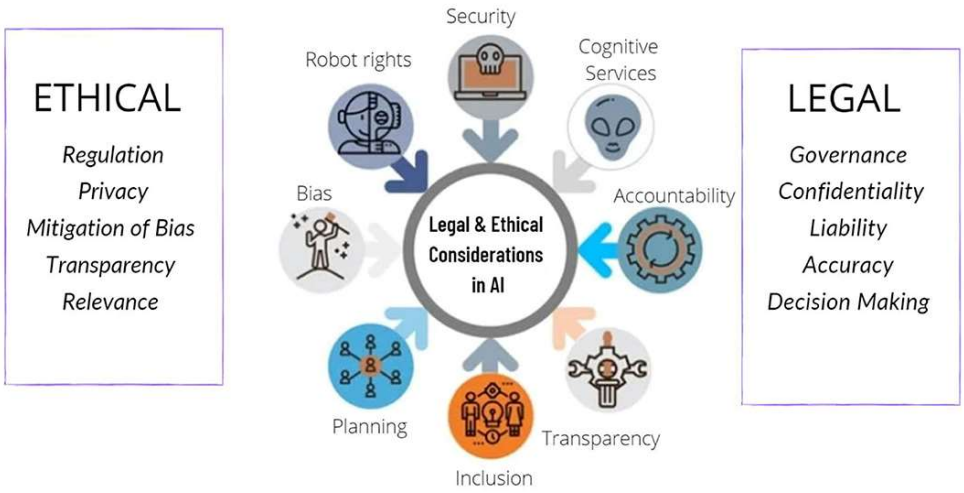

Figure 1.4: Ethical Consideration

The study emphasises that the undertaking must adhere to all administrative and legal requirements. This includes abiding by all national and international cybersecurity laws and regulations. The project is aware that upholding legal consistency fosters partner trust and reduces gambling. The relevant assessment of moral and legal ramifications highlights the undertaking's dedication to moral data handling, tendency decrease, and compliance with cybersecurity legislation and guidelines. These factors underscore the project's commitment to ethical and legal cybersecurity standards and provide the framework for the appropriate planning of AI-enhanced incident response and recovery operations.

- **Theme 3: Challenges And Strategies for Mitigation**

The business believes that implementing AI innovation will require significant resources, including trained personnel, infrastructure, and infrastructure speculation. Requiring these resources could make it difficult to successfully use AI to incident response. The campaign encompasses tactics such as training and projects aimed at improving ability to make sure employees are suitably equipped to meet AI's promise. A significant barrier stands in the way of innovation. AI frameworks, for all its unity, are not without flaws and limitations. The analysis highlights how important it is to comprehend these limitations in order to try to avoid relying too heavily on AI and to have backup plans in case of mechanical issues.

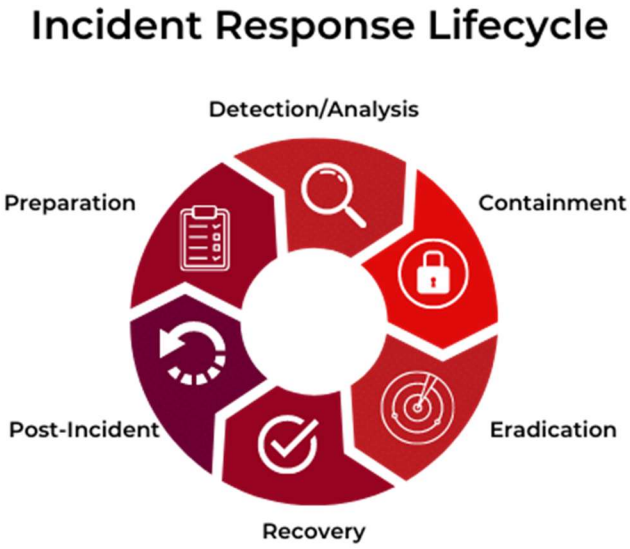

Figure 1.5: Incidence Response Lifecycle

The robustness of incident response techniques is ensured by this system. It is acknowledged that using AI could lead to security risks. The regulating methods include playing it safe, preparing for emergencies, and training for new skills. These results highlight the task's commitment to problem-solving proactively and ensuring the successful and safe integration of AI in Cyber Incident Response and Recovery operations.

5. CONCLUSION

In order to effectively combat dynamic cyber threats, cloud security incident management has advanced significantly with the incorporation of AI-driven techniques. Using AI algorithms and machine learning to enhance issue detection and response in cloud environments became increasingly important in 2020. Organisations may quickly minimise security breaches, maintain customer trust, and ensure operational continuity by automating incident response processes. Nonetheless, issues like algorithmic bias, model interpretability, and data privacy emphasise the necessity of continued study and human-machine cooperation. In the future, adopting AI technologies helps businesses to strengthen resilience, keep cloud infrastructure integrity, and react proactively to changing threats. Sustained investment in AI-powered incident response capabilities is necessary to keep one step ahead of adversaries and guarantee a safe online environment for people and companies alike.

REFERENCES

1. Addo, A., Centhala, S., & Shanmugam, M. (2020). Artificial intelligence for security. Business Expert Press.

2. Asad, S. M., Ahmad, J., Hussain, S., Zoha, A., Abbasi, Q. H., & Imran, M. A. (2020). Mobility prediction-based optimisation and encryption of passenger traffic-flows using machine learning. Sensors, 20(9), 2629.

3. Ramagundam, S., Das, S. R., Biswas, S. N., Morton, S., Assaf, M. H., & Ozkarahan, I. (2013). AMBA-BASED AHB MASTER/SLAVE MEMORY CONTROLLER DESIGN. Transformative Science and Engineering, Business and Social Innovation, 23.

4. Hall, S., & Rebhuhn, A. (2020). Confronting Cyber Threats to Your Practice: How to prepare for—and respond to—a potential catastrophe. Oncology Issues, 35(6), 30-34.

5. Mohammed, I. A. (2020). Artificial intelligence for cybersecurity: A systematic mapping of literature. Artif. Intell, 7(9), 1-5.

6. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, 1-29.

7. Sodhro, A. H., Sodhro, G. H., Guizani, M., Pirbhulal, S., & Boukerche, A. (2020). AI-enabled reliable channel modeling architecture for fog computing vehicular networks. IEEE Wireless Communications, 27(2), 14-21.

8. Ramagundam, S., Das, S. R., Morton, S., Biswas, S. N., Groza, V., Assaf, M. H., & Petriu, E. M. (2014, May). Design and implementation of high-performance master/slave memory controller with microcontroller bus architecture. In 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings (pp. 10-15). IEEE.

9. Susila, N., Sruthi, A., & Usha, S. (2020). Impact of cloud security in digital twin. In Advances in Computers (Vol. 117, No. 1, pp. 247-263). Elsevier.

10. Tewari, S. H. (2020). Data Science and Its Application in Cyber Security (Cyber Security Data Science). Data Science in Cyber Security and cyber threat intelligence: Sikos, Leslie F, Choo. Kim kwang.[Upcoming challenges in Cyber Security Data Science]. Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools: Tariq Mahmood, Uzma Afzal [Definition of Cyber.

11. Wason, R. (2020). An integrated CASB implementation model to enhance enterprise cloud security.

12. Xiong, J., & Chen, H. (2020, November). Challenges for building a cloud native scalable and trustable multi-tenant AIoT platform. In Proceedings of the 39th International Conference on Computer-Aided Design (pp. 1-8).

13. Aggarwal, N., Ahmed, M., Basu, S., Curtin, J. J., Evans, B. J., Matheny, M. E., ... & Thadaney-Israni, S. (2020). Advancing artificial intelligence in health settings outside the hospital and clinic. NAM perspectives, 2020.

14. Chaki, J., Ganesh, S. T., Cidham, S. K., & Theertan, S. A. (2020). Computer and Information Sciences. Journal of King Saud University–Computer and Information Sciences, 32, 1158-1172.
15. Ramagundam, S. (2014). Design and Implementation of Advanced Microcontroller Bus Architecture High-performance Bus with Memory Controller in Verilog Hardware Description Language (Doctoral dissertation, Troy University).
16. Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.
17. Schneider, J. (2020). Using Artificial Intelligence to Manage and Secure Computer Networks (Doctoral dissertation).
18. De Blasi, S. (2020). Beyond the Hype: A Comparative Case Study of the Impact of Artificial Intelligence and Machine Learning on Cybersecurity.