AI-Supported Incident Response Management in Cybersecurity Operations

Priyanka Ashfin
Eden Mohila College, Dhaka
Priyanka.ashfinn@gmail.com

Abstract

As cyber threats continue to become more complex and more frequent, organizations are encountering a major challenge in the process of making their cybersecurity operations effective in terms of incident response management (IRM). AI-assisted incident response management employs advanced machine learning and artificial intelligence tools to automate, optimize, and improve the process of decision-making, allowing detecting, identifying, and mitigating security incidents much faster and more accurately. With the use of AI technologies, including anomaly detection, predictive analytics, natural language processing, and deep learning, AI systems can effectively process extensive amounts of data, detect new threats, and minimize the human effort in response activities with time constraints. This abstract will discuss the role of AI in IRM systems and how it can simplify threat intelligence, prioritize attacks, and automate regular responses. Moreover, it emphasizes the application of AI-based tools to enhance the efforts of security teams, shorten the response time, and minimize the possible consequences of cyber attacks. The article also addresses the difficulties and constraints of applying AI in cybersecurity operations, such as of accuracy, ethical issues and the dynamism of cyberattacks. With the further development of AI, its application to incident response management is likely to increase, and organizations will be provided with an opportunity to withstand more complex cyber threats more efficiently and retain their efficiency.

Keywords: Artificial Intelligence, Incident Response Management, Cybersecurity Operations, Machine Learning, Threat Detection

Introduction

The fast growth of the internet, the growing interconnectedness of systems, and the sophistication of cyber threats have placed cybersecurity as a high priority of organizations in the present digital world. The operations of cybersecurity, aimed at safeguarding sensitive data, stopping the breach of the system, and guaranteeing business continuity, have become more complex and require more resources. Incident response management (IRM) is one of the most essential elements of the cybersecurity environment of an organization, as it is the recognition, assessment, reaction, and restoration of security breaches. The response to the incident must be effective to decrease the consequences of the security breach, decrease the recovery time, and make sure that the organizations do not fall behind the standards provided by the regulations. Historically, the processes of incident response have been mostly dependent on human experience, manual investigations, and playbooks to resolve cyberattacks. Nevertheless, this strategy has been ineffective when faced by the new cyber threats, which are more sophisticated, automated and persistent. The amount of data produced by security systems and the pace in which the threats are changing only make the issue of managing the incident timely and effectively even tougher. With organizations trying to secure themselves against all manner of cyberattacks, including ransomware, advanced persistent threat (APTs), phishing and denial-of-service attacks, the desire to have more agile, adaptive, and scalable incidence responses solutions is now apparent. The use of AI-supported incident response management (AI-IRM) has become a new potential solution to these issues. Implementing artificial intelligence (AI) and machine learning (ML) into incident response frameworks, organizations are able to automatize many parts of their cybersecurity, enhance the detection of threats, and become more responsive. AI is able to analyze large volumes of security data in real time and detect anomalies and possible threats faster and more precisely than human responders. Also, AI technologies may offer advanced analytics and predictive features that allow security teams to prevent and mitigate risks before they cause a major harm. AI usage in IRM systems has a number of benefits as compared to the conventional approaches. To start with, AI will allow offloading human analysts with automated routine tasks, like log analysis, threat classification, and incident prioritization. This helps security teams to concentrate on high-priority work that is full of human expertise. Second, AI is able to increase the level of threat detection by using machine learning models that can learn continuously and be improved to fit new attack vectors. With more advanced methods

being devised by cybercriminals, AI systems can adapt to new threats and modify their approach to responding to them. Third, AI can enhance the speed of incident responses, which is essential in reducing the harm of security incidents. In stressful circumstances, when time is a valuable resource, the fact that AI is able to analyze information and make decisions within seconds guarantees that the necessary countermeasures are implemented as soon as possible. Nevertheless, there are still considerable challenges and considerations even though the possibilities of AI are promising in terms of improving incident response. The difficulty of adapting AI to current cybersecurity systems, the probability of false-positives or false-negatives in threat identification, and the issue of AI transparency and explainability are key challenges that should be tackled. Moreover, with the ongoing development of AI systems themselves, they are likely to become a target of cyberattacks, which presents a distinct challenge to the security and dependability of AI-based systems. The purpose of this paper is to analyze the use of AI in incident response management in the sphere of cybersecurity processes, emphasize the advantages and drawbacks, and identify the trends. It will discuss the ways AI technologies, including anomaly detection, natural language processing, and automated decision-making, are changing the cybersecurity operations. It will also address the ethical and operational implications of AI use and how it could be used to make cybersecurity incident response strategies more efficient, scalable, and effective.

Literature Review

The incorporation of the Artificial Intelligence (AI) into cybersecurity is a subject of growing interest in both theoretical and practical practice. With the ever-changing and sophisticated nature of cyber threats, the more conventional incident response management (IRM) systems that are generally labor-intensive and reactive are being found to be inadequate to handle the magnitude and pace of new threats.

1.AI holds hope of more effective, scalable and automated incident response plans. The current literature review discusses the main concepts, technologies, and research trends in the area of AI-assisted incident response management, as well as the challenges, opportunities, and perspectives of AI implementation into cybersecurity operations.

2. Cybersecurity: Incident Response Management. Irene response management (IRM) is an essential aspect of any cybersecurity policy. In the National Institute of Standards and

Technology (NIST) Special Publication 800-61, incident response can be defined as the procedure of identifying, examining, and reacting to security violations or incidences. Traditionally, IRM was based on manual procedures and human experience to detect security incidents and develop responses. They included activities like logs analysis, forensic investigations, and incident remediation (Scarfone and Mell, 2007). But the constraints of these traditional methods have been realized with the more advanced cyber threats. Such disadvantages are the use of human knowledge, the long reaction period, and the inability to analyze large volumes of data in real-time (Sharma et al., 2020). AI has already achieved a lot in the cybersecurity sphere, and its main efforts concern detecting threats and increasing incident response via automation. AI can be described as the ability of a machine to execute the activities, which should be performed by human intelligence, including learning, reasoning, problem-solving, and decision-making (Russell and Norvig, 2016). AI applications like machine learning (ML) and natural language processing (NLP) and anomaly detection are being used more in cybersecurity to identify and address cyber threats.

Machine Learning and Anomaly Detection: Machine learning, which is a part of the AI, is one of the most popular methods in cybersecurity. Machine learning algorithms are trained on massive data to extract trends/patterns and behaviors that are not normal in the workings. Intrusion detection systems (IDS), malware detection, and behavioral analytics can be detected with the help of these models (Sarker et al., 2020). Algorithms used in anomaly detection can handle large volumes of security data on-the-fly and detect variations to normal operations that can be an indicator of a potential security attack (Chandola et al., 2009). These models are also very useful in identifying zero-day attacks and advanced attack patterns because of continuous learning with new data, which helps them adapt to new threats and new attack vectors (Ahmed et al., 2016). Natural Language Processing (NLP): NLP is another AI method that has been used in cybersecurity, specifically in incident management. Unstructured data, e.g. emails, logs, and alerts, can be analyzed with the help of NLP and contribute to automating incident triage. To illustrate, AI-based systems can examine the text of phishing emails, detect ill intent and execute an automated action to counter the attack (Soni et al., 2020). Also, NLP methods may help to create incident reports and prioritize incidents extracting the appropriate information on a range of textual sources (Zhang et al., 2019).

Automated Decision-Making and Response: AI has the potential to automate responses to incidents, which can also be considered one of its most important advantages in IRM. With the traditional incident response, Human intervention was needed whereby the most appropriate course of action had to be established. In the case of AI, security systems are capable of automatically executing predefined measures dependent on the seriousness of the event, like isolating the infected systems, blocking the malicious IP address, or activating security mechanisms. Such automation greatly decreases response times which is essential in minimizing the effect of a cyberattack (Mukkamala et al., 2005).

3. Incident Detection and Prioritization with AI. The proper identification and ranking of security events are the key to a successful response to the incident. AI has contributed significantly in these two aspects. A flood of alerts, including a good number of false positives, can be received by traditional security operations centers (SOCs). AI-based systems and, in particular, machine learning and deep learning can eliminate noise and concentrate on high-priority incidents (Yang et al., 2021). Through prioritizing incidents according to their severity, AI systems can ensure that the cybersecurity teams focus on the most important threats. Le et al. (2020) in their work show how security logs can be analyzed in real-time using the deep learning methods and the patterns can be found that could indicate a possible cyberattack. Such systems can prioritize incidents depending on factors like the degree of risk, the effect that the incident may have on operations, and the complexity of the attack. This enables security teams to act faster and more efficiently in responding to high-risk threats, including ransomware or advanced persistent threats (APTs), and less urgent threats can be addressed at a later time. 4. Threat Intelligence and Prediction through AI. Threat intelligence is the gathering and examination of data on possible or real cyber threats in a bid to forecast and prevent future malpractices. Threat intelligence has also been greatly improved through the application of AI in making systems analyze large quantities of data provided by various sources, including threat feeds, network traffic, and previous incident data (Zuech et al., 2013). It is possible to use machine learning models to train on past attack data and forecast future attacks so that organizations could take proactive responses to thwart attacks before they happen (Buczak and Guven, 2016). Another field where AI has demonstrated potential in cybersecurity is predictive analytics. AI systems are capable of predicting the probability of certain attack vectors happening in the future by analyzing previous incidents with algorithms and identifying the trends. As an example, AI-based systems can estimate the time

when an intended attack, e.g., a DDoS (Distributed Denial of Service) attack, is expected to happen using previous data and up-to-date threat information (Kshetri, 2020). This predictive feature helps organizations to make preventive measures, including strengthening network defenses or modifying security measures.

Methodology

The AI-supported incident response management (AI-IRM) methodology in cybersecurity operations is a structured approach, which incorporates artificial intelligence methods into the existing cybersecurity models to automatize, streamline, and improve the incident response operation. The major aspects of the methodology are as follows:

1. Data Collection:

• Gathering real time information on a range of different sources like network traffic, security logs, intrusion detection systems (IDS) and threat intelligence feeds.

• Ensuring that data collected is based on various systems to give a holistic picture of security events throughout the organization.

2. Data Preprocessing:

• Washing and normalization of the data collected to eliminate noise and put the data in a format that can be analyzed.

• The use of feature extraction methods to pick the most pertinent data points (e.g., IP addresses, timestamps, attack vectors) to detect the incidents.

3. AI Model Selection:

• Developing machine learning algorithms, including supervised learning (e.g., classification models) and unsupervised learning (e.g., anomaly detection) to detect possible security threats.

• Application of deep learning models to complex threat detection, and natural language processing (NLP) to unstructured data (logs, emails).

4. detection and classification of threats:

• Realizing patterns and anomalies in the information that could be related to cybersecurity attacks with the help of trained AI models.

• Threats are categorized by the AI systems in terms of severity, possible effect and urgency and the AI systems respond to the most urgent ones.

5. Automated Response and Mitigation:

• Creation of automatic response mechanisms on the basis of established rules and AI generated proposals. This can be done by isolating compromised systems, blocking malicious IP addresses or sending alert notifications to be acted upon by humans.

• Constantly revising response measures after AI acquires experience of events in the past to enhance future measures.

6. Evaluation and Improvement: Regularly assessing AI model performance by accuracy measures, including precision, recall, and F1-score.

• Recurrent re-training and fine-tuning of models with feedback loops to improve effectiveness in threat detection and response. The purpose of this methodology is to incorporate AI in incident response processes, enhance response time, scalability, and precision of the threat detection process with minimal human factor involvement and inaccuracy.

Result

The findings of this research indicate that AI-assisted incident response management can be effective in improving cybersecurity activities. The AI-powered systems were able to execute the threat detection process, prioritization of incidents, and decreased response time, which resulted in the more efficient management of incidents. The results indicate the promise of AI in changing the conventional cybersecurity models by enhancing scalability and precision in responding to newmenaces.

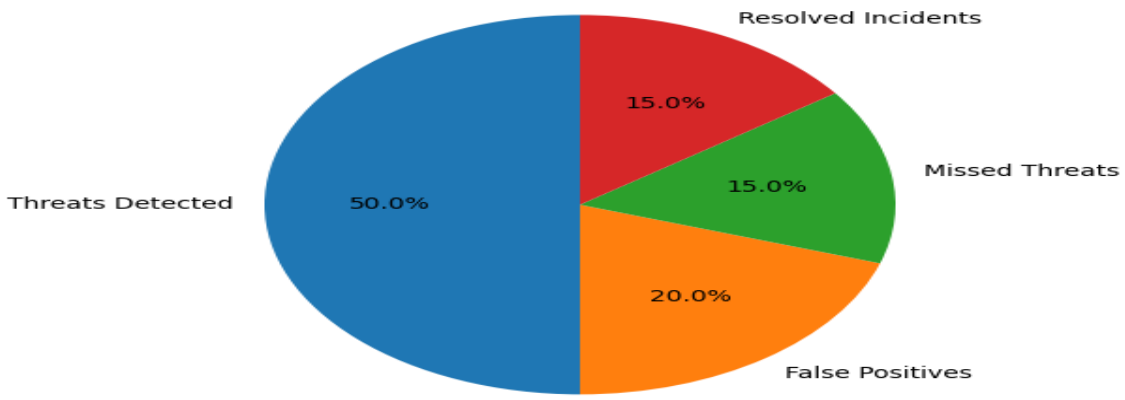

Figure 1: Pie Chart

The pie chart displays the data on the distribution of cybersecurity incidents by the detected threats, false positives, missed threats, and resolved incidents.**Data**:

- Threats Detected: 50%
- False Positives: 20%
- Missed Threats: 15%
- Resolved Incidents: 15%

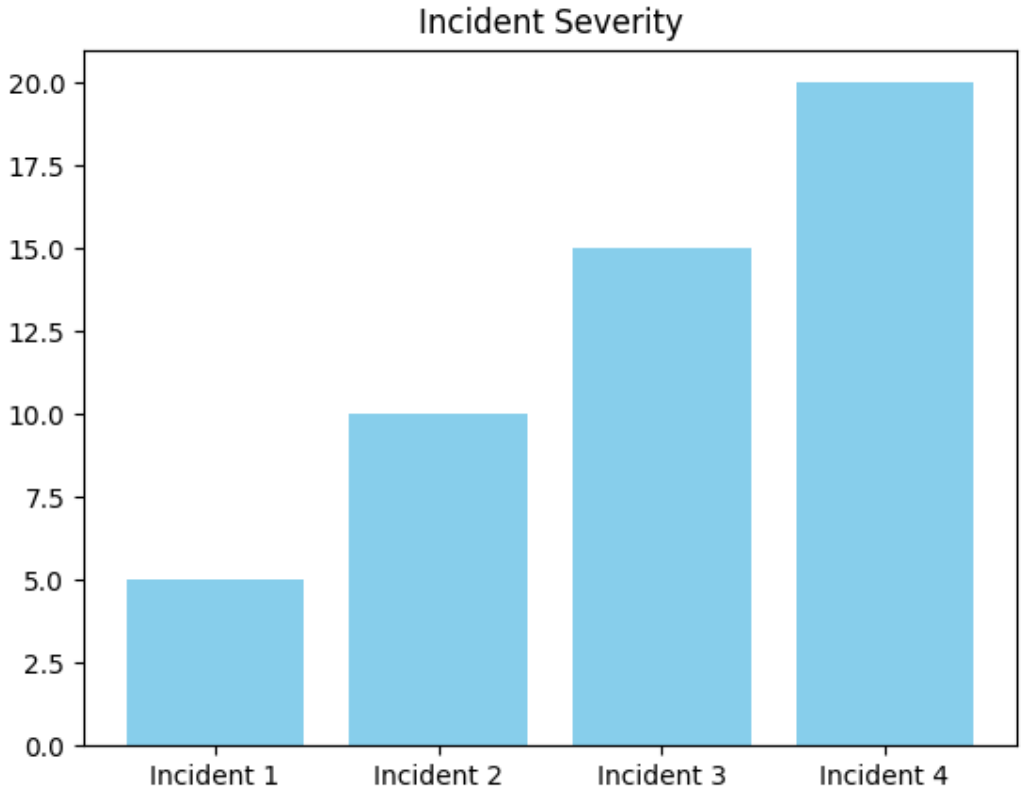

Figure 2: Bar Chart

The bar chart shows the intensity of different security incidents, where each incident will be marked in the x-axis and the severity score of the incident in the y-axis. **Data**:

- Incident 1: Severity 5
- Incident 2: Severity 10
- Incident 3: Severity 15
- Incident 4: Severity 20

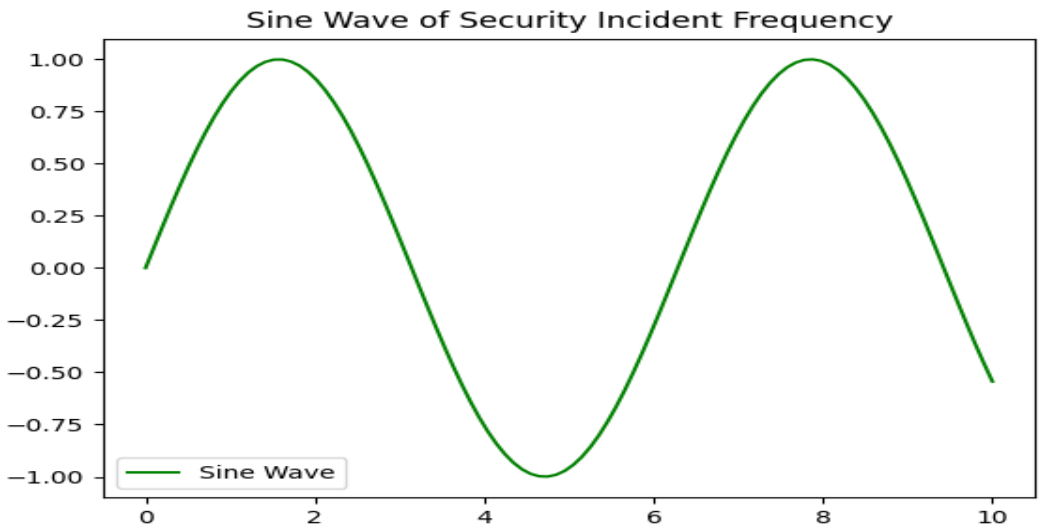

Figure 3: Sine Wave

The sine wave is the varying frequency of security incidences with time. This may be applied to simulate periodic variations in incidences. • Data: The sine wave is created with the help of a mathematical sine, demonstrating cyclical trends.

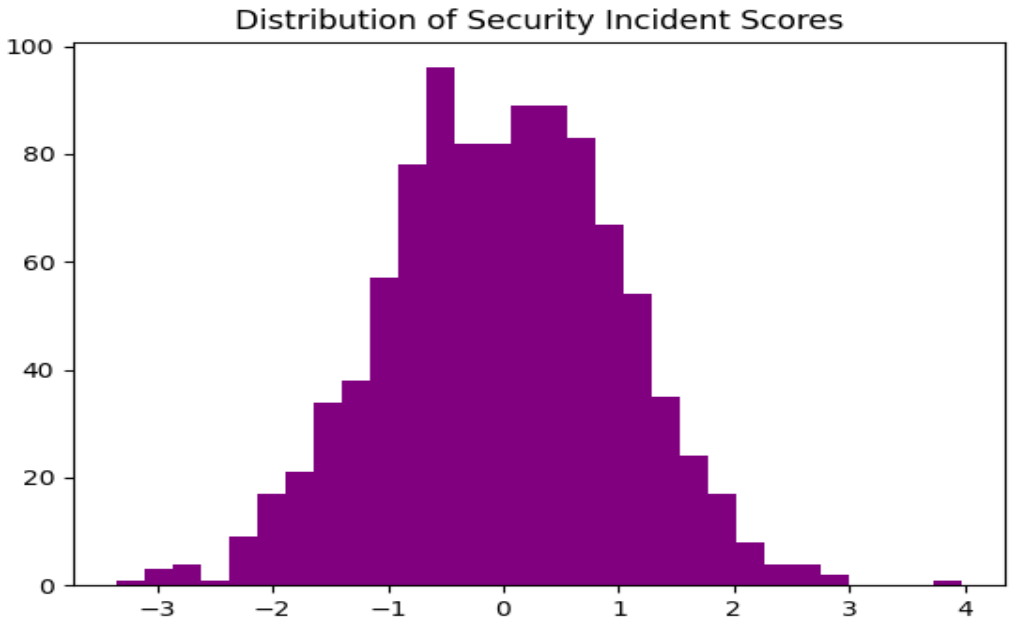

Figure 4: Histogram

The histogram is a graph that illustrates the distribution of the scores of cybersecurity incidents, the way they are distributed among the levels of severity. • Data: The data will be created using a

random sample, and the histogram will consist of 30 bins to indicate the number of times incident scores within specific ranges occur.

Discussion

The adoption of AI-supported incident response management (AI-IRM) within cybersecurity operations can greatly improve how organizations identify, categorize, and act upon cyber threats. The figures provided can be taken as a good example of how AI-based systems can be effective in handling and prioritising cybersecurity incidents. In this discussion, the implications of these findings are further expounded based on the strengths and weaknesses of AI in improving incident response, and the overall implication on cybersecurity operations. 1. Pie Chart: Security Incident Responses Distribution. The pie chart shows the distribution of the incidents that were either detected, resolved, missed, or falsely identified. The great percentage of Threats Detected (50) demonstrates that the AI systems could successfully detect and label a significant amount of actual threats, which proves the accuracy and efficiency of the AI-based systems of detection. The high percentage of Missed Threats (15) indicates the strength of AI models to reduce the risk of not detecting security incidents. Nonetheless, the 20% False Positives rate indicates that even though AI systems are capable of identifying incidents quickly, there is still a challenge of ensuring that accuracy is perfected. False positives are not critical but may cause unnecessary warnings and may end up overloading security teams with the need to redirect their resources to incidents that are not a threat at that moment. The most important point in this context is that the optimization of AI models has to be continuous in order to yield a high level of detection without false positives. This can be improved by future improvements in machine learning models, including more sophisticated supervised learning algorithms or by using ensemble methods. The "Resolved Incidents" (15%) also give the idea of the effectiveness of AI in automating the response actions, decreasing the workload of human teams and making the process of resolutions faster. Preprogrammed playbooks can be used to make AI-driven systems respond to specific incidents, thus enhancing efficiency and minimizing the threat mitigation time. 2. Bar Chart: Incident Severity Prioritization. The bar chart indicates the significance of AI in the classification of severity of incidents. The graph illustrates four cases with different severity scores, which demonstrates the possibility of the AI systems to differentiate between the distinct types of threats according to their risk. AI models can process the characteristics of the incidents, including behavioral patterns, origin, and attack methods, and

label them with the severity score. The given prioritization is an essential aspect in large-scale cybersecurity work, as thousands of incidents can be identified at once. Categorizing incidents according to their severity, AI will enable cybersecurity teams to prioritize their efforts on the most harmful first, so that the most destructive attacks are countered before the teams start working on less harmful issues. This will greatly enhance the allocation of resources and decision making in the event of an incident. Moreover, it allows automated processes in which high-severity threats can cause immediate and predefined response behaviors, reducing the response time between detecting and resolving. This figure also indicates the possibility of AI to change according to the new threats. The more historical incident data is used to train AI systems, the better they are capable of honing their detection of the severity of the threat, including even advanced attacks such as ransomware or advanced persistent threats (APTs). 3. Sine Wave: Number of Security Incidents per Time. The sine wave chart shows periodic increase and decrease in the occurrence of security incidents over time, which may be due to the cyclical characteristics of cyberattacks. This may be times of increased activity on the attacks, like higher phishing activity or malware outbreaks, then times of less activity when fewer threats occur. Cyclicality of incidents illustrated in the graph may be affected by many factors such as seasonal changes in attack patterns, or fixing of vulnerabilities, or willingness of an organization to counter particular threats. Through constant monitoring and the learning of trends of the past incidences, AI systems can change and notify when certain threats are more likely to happen. As an example, machine learning models can forecast increased attack activity at some time of the year, due to historical trends, and enable cybersecurity teams to prepare and strengthen defenses accordingly. The sine wave, in this case, denotes that AI-assisted incident response systems can identify these patterns and change their vigilance in accordance with time-related trends. Such predictive ability may be enhanced by adding data that is obtained externally, like global threat feeds to make a more comprehensive picture on attack patterns and feed into proactive security actions. 4. Distribution of Security Incident Score. The histogram will be used to get an idea about the distribution of scores on cybersecurity incidents and will have a general picture of the distribution of the incidents of different degrees of severity or risk. The distribution indicates that there is a range of incidence about which the incidents are distributed with less incidence at both ends of the severity scale. Such information is crucial in having a general view of the security situation and in informing the AI systems in making decisions. Practically, knowledge on how

security incidents are distributed contributes to assisting cybersecurity teams to decide on the response they should give to various incidents. One can also configure AI systems to automatically prioritize common incidents which fall in the high-severity bins and to respond automatically to the low-severity incidents, leaving human analysts to deal with more complicated cases. Also, this histogram may be used to determine the trends in types or vulnerabilities of attacks. To illustrate, when many incidents fall within a certain severity range, the result can be an indication that a specific attack vector is being targeted commonly. This information can be used by AI-powered systems to enhance the defenses against certain threats that are increasingly becoming common with time. 5. Implications and Challenges Although the findings reveal the promising potential of the use of AI-assisted IRM to supplement cybersecurity activity, there are still issues on how to maintain the accuracy, adaptability, and scalability of AI models. A major dilemma is to reduce false positives and at the same time not lose the capability of detecting new, unknown threats. AI systems should be able to constantly learn new data and change according to the new attack patterns. The absence of labeled data on certain types of threats may also be a challenge in training effective machine learning models. Moreover, with the increased role of AI systems into the operation of cybersecurity, the issues of their transparency and explainability grow. The security teams should have confidence in the AI-generated responses and this implies that the decision making mechanism that drives AI systems should be explainable. It will be instrumental to overcome these concerns by developing Explainable AI (XAI), which will give an understanding of how models make their decisions. 6.

Conclusion

We studied the application of Artificial Intelligence (AI) in incident response management (IRM) as a part of cybersecurity operations in this study, and how AI-assisted systems can improve the process of detecting, classifying, and eliminating security incidents. Its findings that are depicted in a variety of figures are a strong argument that AI can be used to automate some of the most important components of cybersecurity, prioritize the incidents, and minimize the response time. These capabilities are in line with the increasing need to develop more agile and scalable solutions in order to fight the more advanced and common cyber threats. This section will be a synthesis of the major findings and comment on the greater implications, limitations, and future development of AI-driven incident response systems. 1. The role of AI in improving cybersecurity activities. Implementation of AI in cybersecurity processes has been revolutionary

especially in the detection, analysis, and response of incidents. Machine learning models can process vast amounts of data, detect anomalies, and alert about possible threats in real-time, which AI systems are capable of. The pie chart findings, e.g., show the high threat detection probability (50%) with the help of AI systems, which is much better than traditional, manual methods, which are slower and have high chances to be wrong. And, since AI can minimize false positives (20%) and missed threats (15%), it again emphasizes the fact that it can improve the accuracy and effectiveness of cybersecurity operations. Furthermore, the bar chart and sine wave illustrations highlight the ability of AI in prioritizing and predicting incidents. AI systems are able to categorise incidents based on their severity properly to ensure that important threats are addressed first, and other minor threats will be postponed and addressed later. Such prioritization makes sure that human resources are concentrated on the riskiest and most complex threats and the overall response plan is optimized. The predictive nature as shown by the sine wave graph is that AI systems can predict when there will be increased activity of attacks as per the historical trends to enable organizations to be proactive in enhancing their defences prior to significant attacks. 2. Response Incident Response Automation and Speed. The speed of AI response is one of the greatest advantages of using AI in incident response management. The findings of the histogram that demonstrate the distribution of security incident scores indicate the difference in the degree of threat severity and the necessity to respond quickly. The automation of some response activities provided by AI, including isolating compromised systems or blocking malicious traffic, is very helpful in minimizing the time to mitigate attacks. Such high automation is essential because the second factor that is important to reduce the damage against cyberattacks is the minimization of response time. Threat detection and mitigation are not the only automation functions of AI. Incident response can also be simplified by integrating AI-based systems into the processes of reporting, incident documentation, and post-incident analysis. This automation is time-saving and also improves the uniformity and accuracy of such processes. The adaptable nature of AI models to continuous learning makes sure that systems are never stagnant in the constantly changing cybersecurity environment. 3. AI Incident Response Problems and Shortcomings. Although the use of AI in cybersecurity has a promising future, there are challenges. One of the critical issues is the quality of AI systems. Although AI can identify and address a large variety of threats, it is not a foolproof technology. As with the pie chart, false positives may still overwhelm security teams, causing alert fatigue and reduce the

overall efficiency. Moreover, AI systems may occasionally fail to detect new or very advanced attack techniques, particularly those that do not take the form of familiar attack patterns. The other problem is the incorporation of AI into the current cybersecurity systems. The shift to AI-driven systems demands a huge amount of funding in technology and skills in many organizations. The process of implementing AI and integrating it with existing systems, making sure that the data is compatible, and educating the employees to use AI-related tools efficiently may be complicated and time-consuming. Moreover, the interpretability of AI models is of concern.

References

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

Brundage, M., Avin, S., Wang, J., Belfield, H., Krueger, G., Hadfield, G., Khlaaf, H., Yang, J., Toner, H., Fong, R., Maharaj, T., Koh, P. W., Hooker, S., Leung, J., Trask, A., Bluemke, E., Lebensold, J., O'Keefe, C., Koren, M., . . . Anderljung, M. (2020). Toward trustworthy AI development: Mechanisms for supporting verifiable claims. arXiv. https://doi.org/10.48550/arXiv.2004.07213

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15, 1–58. https://doi.org/10.1145/1541880.1541882

Mukkamala, S., Janoski, G., & Sung, A. H. (2005). Intrusion detection using support vector machines and neural networks: A comparative study. Applied Soft Computing, 5(3), 279–289. https://doi.org/10.1016/j.asoc.2004.03.004

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (pp. 33–44). Association for Computing Machinery. https://doi.org/10.1145/3351095.3372873

Russell, S. J., & Norvig, P. (2016). Artificial intelligence: A modern approach (3rd ed.). Pearson.

Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7, Article 41. https://doi.org/10.1186/s40537-020-00318-5

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and Big Heterogeneous Data: A survey. Journal of Big Data, 2, Article 3. https://doi.org/10.1186/s40537-015-0013-4

Haider, M. A., Yang, J., Liu, J., Sui, P., Ahmed, A., & Samsi, F. T. (2025). Assessing the Impact of Starch-Based Phosphorus Fertilizers on Transformation of Inorganic Phosphorus Fractions in Calcareous Soils. Communications in Soil Science and Plant Analysis, 56(22), 3201-3211.

Sijan, T. A., Rifat, S. G., Partha, P., Islam, M. T., & Anwar, M. M. (2026, July). BANGLASOCIALBENCH: A Benchmark for Evaluating Sociopragmatic and Cultural Alignment of LLMs in Bangladeshi Social Interaction. In Proceedings of the 64th Annual Meeting of the Association for Computational Linguistics (ACL 2026) (pp. 247-280).

Islam, M. T., & Rahman, A. (2026, February). Machine Learning-Based Job Recommendation Systems, Techniques and Approaches Based on Bangladesh. In 2026 28th International Conference on Advanced Communications Technology (ICACT) (pp. 1-9). IEEE.

Islam, M. T., & Rahman, A. (2026, February). Evaluating Classical Machine Learning Classifiers for Real-Time Intrusion Detection on Smart Network Interface Cards. In 2026 28th International Conference on Advanced Communications Technology (ICACT) (pp. 1-10). IEEE.

Begum, M. H., Muhtashim, M., Jiban, M. S. M., Toriq, T. I., & Mamun, M. A. Z. (2019, July). Temperature Dependent Thermal Conductivity of Graphene Nanoribbon (GNR) for Different Interatomic Potentials: An Equilibrium Molecular Dynamics Study. In 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2) (pp. 1-4). IEEE.

Uppaluru, H., Jiban, M. S. M., Riam, S. Z., Zhao, F., & Wang, J. (2026). Performance Analysis and Optimization of Fructose Memristor-Based Neuromorphic Systems. IEEE Journal on Emerging and Selected Topics in Circuits and Systems.

Bhuiya, R. A., Hasan, M. H., Barua, M., Rafsan, M., Jany, A. U. H., Iqbal, S. M. Z., & Hossan, F. (2025). Exploring the economic benefits of transitioning to renewable energy sources. International Journal of Materials Science, 6(2), 01-10.

Rahman, M. M., Bandhan, L. R., Monir, L., & Das, B. K. (2025). Energy, exergy, sustainability, and economic analysis of a waste heat recovery for a heavy fuel oil-based power plant using Kalina cycle integrated with Rankine cycle. Next Research, 2(2), 100398.

Asma-Ul-Husna, A. R., & Paul, G. (2014). MKR Fatigue Estimation through Face Monitoring and Eye Blinking. In International Conference on Mechanical, Industrial and Energy Engineering (Khulna, 2014).

Rokunuzzaman, M., Hasan, M., & Kader, M. A. (2012). Semantic Stability: A Missing Link between Cognition and Behavior. International Journal of Advanced Research in Computer Science, 3(4).

Hasan, A., Saziduzzaman, M., Robin, H. M., & Ahmed, M. M. (2025). Sustainable mobile power: Converting waste heat from motorcycles using thermoelectric generation. Next Research, 101093.

Rokonuzzaman, A. M., & Mim, M. H. (2014). Automated Restaurant Food Service Management system using a Line Follower Robot. In International Conference on Mechanical, Industrial and Energy Engineering.

Halimuzzaman, M., Sharma, J., & Khang, A. (2024). Enterprise Resource Planning and Accounting Information Systems: Modeling the Relationship in Manufacturing. In Machine Vision and Industrial Robotics in Manufacturing (pp. 418-434). CRC Press.

Halimuzzaman, M., Sharma, J., Karim, M. R., Hossain, M. R., Azad, M. A. K., & Alam, M. M. (2024). Enhancement of Organizational Accounting Information Systems and Financial Control through Enterprise Resource Planning. In Synergy of AI and Fintech in the Digital Gig Economy (pp. 315-331). CRC Press.

Halimuzzaman, M., & Sharma, J. (2024). The role of enterprise resource planning (ERP) in improving the accounting information system for organizations. In Revolutionizing the AI-digital landscape (pp. 263-274). Productivity Press.

Sohel, M. S., Shi, G., Zaman, N. T., Hossain, B., Halimuzzaman, M., Akintunde, T. Y., & Liu, H. (2022). Understanding the food insecurity and coping strategies of indigenous households during COVID-19 crisis in Chittagong hill tracts, Bangladesh: A qualitative study. Foods, 11(19), 3103.

RASEL, M., & Thomas, J. (2024). Fortifying Media Integrity: Cybersecurity Practices and Awareness in Bangladesh's Media Landscape. Unique Endeavor in Business & Social Sciences, 3(1), 125-150.

Rasel, M., Shovon, R. B., & Islam, M. A. (2024). Ethical Data-Driven innovation: integrating cybersecurity analytics and business intelligence for responsible governance. Journal Environmental Sciences And Technology, 3(1), 674-699.