Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2528

AI in enhancing cybersecurity incident response

Pooja Bagane *
Sonali Kothari †
Ankur Goyal §
Prisha Patel ‡
Sakshi Chauhan @
Shaurya Gupta #
Tawishi Gupta $
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Symbiosis International (Deemed University)
Lavale
Pune 412115
Maharashtra
India

Abstract

With new threats emerging all over the place, the capability to assess and address an advanced threat has become paramount to the health and longevity of organizations. AI provides a potent capacity in augmenting the procedures concerned with cybersecurity incidents response. In this paper, the writer looks at how AI and its applications such as Machine learning algorithms and Automation is being adopted in Cybersecurity to improve on the detection of threats, analysis, and mitigations. AI can quickly analyze attack patterns, assess the likelihood of risks, and eradicate threats mathematically and without delay compared to human protection. Moreover, this paper outlines the concerns and risks when implementing an AI solution for cybersecurity, as well as the right ways to ensure that the AI system is secure and reliable. The evidence presented in the paper supports the AI's

* *E-mail:* **pooja.bagane@sitpune.edu.in (Corresponding Author)**
† *E-mail:* **sonali.kothari@sitpune.edu.in**
§ *E-mail:* **ankur.goyal@sitpune.edu.in**
‡ *E-mail:* **prisha.patel.btech2021@sitpune.edu.in**
@ *E-mail:* **sakshi.chauhan.btech2021@sitpune.edu.in**
# *E-mail:* **shaurya.gupta.btech2021@sitpune.edu.in**
$ *E-mail:* **tawishi.gupta.btech2021@sitpune.edu.in**

application in defining the cybersecurity of the future and establishing its relevance as an essential tool against cyber threats.

Subject Classification: *Primary 68T01, Secondary 94A60.*

Keywords: *Artificial intelligence, Cybersecurity, Incident response, Automation, Threat detection, Machine learning.*

1. Introduction

The threat of cyber incidents has become very large. In order to cope with these threats and return to normal, necessary changes are being made in the response situation. The use of "Artificial Intelligence (AI)" in cyber incident management has facilitated this change [1]. AI can quickly detect, identify and mitigate cyber threats, making it a powerful tool for improving cybersecurity. To better enhance our digital defenses and recover faster from an incident, this article identifies areas of intelligence-enhanced cyber incident response and recovery. Organizations are leveraging the power of AI to prevent cyber threats and mitigate threats from criminals.

2. Literature Review

Jada and Mayayise [1] discussed how AI enhances cybersecurity by automating threat detection and vulnerability management, while also generating new risks and regulatory requirements. Lysenko et al. [2] stressed AI's efficacy in sniffing out phishing and zero-day threats, warning of divergence and calling for governance. Chahal [3] mentioned recovery in cyber as an application for AI due to infrastructure, cost, and ethical limitations. Fysarakis et al. [4] presented PHOENI2X, an AI-driven system for rapid response gaining advantages in recovery but issues with data privacy. 5 Rafy suggested future work for AI-enabled cybersecurity is to be extended with ML, and neural networks [5]. Farzaan et al. [6] proposed a cloud security system based on Random Forest, which achieved the classification accuracy of 90% and 96% for malware detection. Chandran, Panda, and Sreenivas [7] proposed secure authentication scheme for personalized healthcare system. Binhammad et al. [8] investigated the use of AI for digital identity security with expressed concerns about bias and privacy. Goyal et al. [9] proposed mathematical model for phishing detection. AI was used by Manjunatha and Kempanna

[10] for discovering the web app vulnerabilities. Kaushik, Singh, and Kumari [11] improved the intrusion detection by using SVM.

3. Methodology

In this work, we utilized an AI-based technique using a Long Short-Term Memory (LSTM) neural network to streamline incident response in cybersecurity for identifying deviations from the expected behavior of network traffic. First, we used normal distribution to create synthetic network traffic data for each period of time mimicking a regular activity. This data was then normalized (using Min-Max scaling) to scale it for the LSTM model.

The primary objective of this LSTM model was to forecast network traffic patterns using historical data. It was configured to learn normal behavior and identify anomalies that were recorded as security incidents. Predicted values were compared with actual network traffic to assess the quality of predictions. The difference between predicted and actual traffic was calculated to identify anomalies which in turn were processed with a threshold-based mechanism, if significant deviations are seen incidents will be flagged as result.

We simulated an incident response workflow structure for further analysis by independently giving every detected anomaly a severity level according to its score. The anomaly score placed each incident into "Critical", "High" or "Low" severity, and led to a distinct response action. In a granular level, we measured response time and compared it with respect to a baseline — i.e. quantified the time AI model saved in detecting & responding incidents. At the end, some visualizations show how well our model performs so that it effectively detects anomalies over time (In and out heatmap), Heatmap of incident severity and then stats on detection times/durations for incidents. The findings illustrated how AI had the potential to both automate and expedite all aspects of incident response, in many cases reducing time-to-response exponentially compared with traditional methods.

Figure 1 shows a block diagram of the enhanced methodology, which has been conducted, showcasing the steps and sequence in which the implementation was projected.

4. Implementation Details

We came up with a model that would ideally be able to detect anomalies in network traffic data, considered one of the most representative cybersecurity incidents as shown in Figure 2.

Data Preparation: A generated set of network traffic data was done with regular and abnormal transactions. Records of the level of traffic over time were present in the data set along with standardized MinMaxScaler on scale values for improved modeling performance.

Sequence Creation: The given time series data set was divided into sequences with fixed lengths in order to effectively time out relationship patterns. It allows the model to learn relationships between the current levels of traffic and preceding data points.

LSTM Model: We designed the Long Short-Term Memory (LSTM) neural network architecture in order to process such sequences. LSTMs are suitable for sequential dependencies, hence very aptly utilized to detect anomalies in time series data. We therefore trained the model on past history to predict future network traffic behavior.

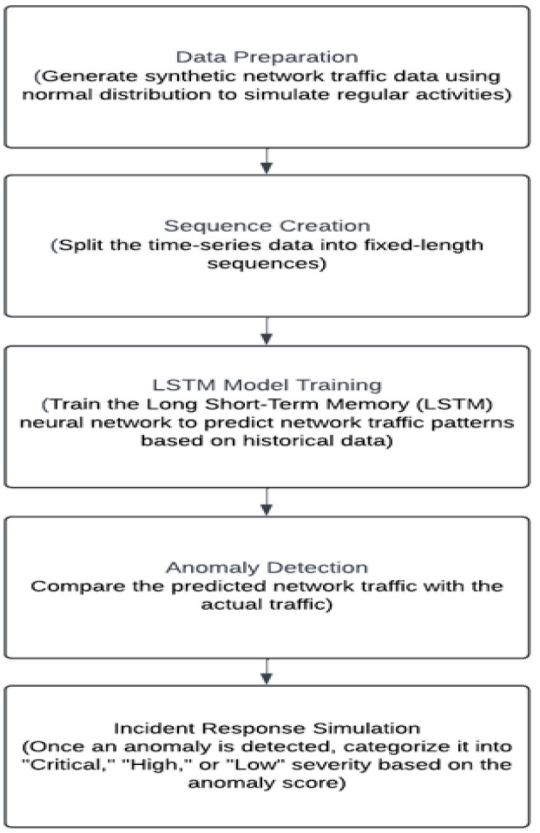

Figure 1

Block diagram of enhanced methodology

Anomaly Detection: Comparison of model predictions versus actual traffic data was conducted when the model had been successfully trained. The anomaly score was based on how much the deviation between a predicted and an observed value. A threshold was established to flag anomalies that could represent a potential cybersecurity incident.

Incident Response Simulation: At every anomaly detected, an incident response flow was triggered. Responses depended upon the categorization of the anomaly-from being critical to high or low severity based on the magnitude of deviation. Activities such as shutdown systems and activation of the alert for SOC teams along with logging of the incident were part of the simulation.

Visualization and Reporting: Multiple graphs show the results of anomalies over time, severity heatmaps, as well as the duration of incidents, categorized by severity, therefore giving deeper insights on incidents that occurred and the response action.

Through the above performance analysis, it was shown how AI improves the detection time of the AI model compared to a baseline response time and how AI-based monitoring reduces detection and response times, thus offering potential for overall improvement in incident cybersecurity management.

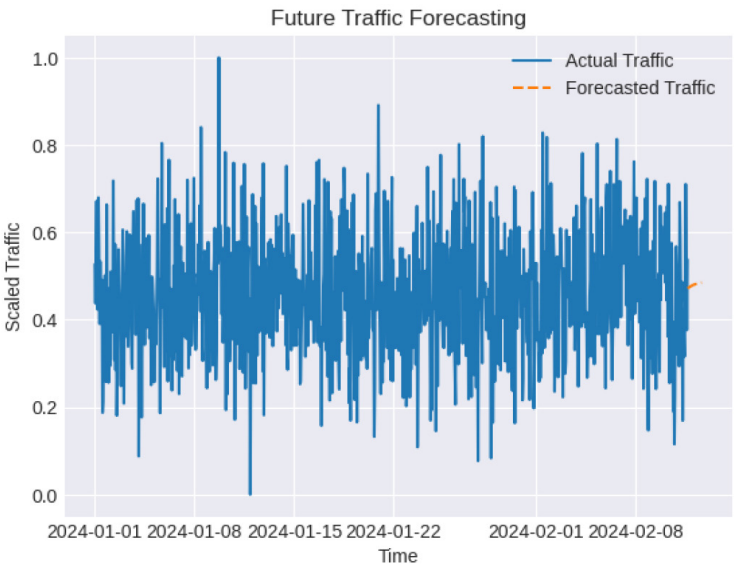

Figure 2

Future Traffic forecasting

5. Results and Discussion

Anomaly Detection Performance: The LSTM model successfully detected anomalies in the network traffic data, defined as potential intrusions or abnormal executions, by comparing predicted and real traffic. Anomalies detected over time are presented.

Figure 3 shows that the model is successful at identifying anomalies in traffic. With one exception, all the anomalies were flagged at locations where the monitored traffic was far from what the model predicted.

Incident Severity and Response: Once an anomaly is detected, we calculate the severity of that incident based on the anomaly score and simulate what alerts or investigations would have been triggered in our actions to that incident. We categorize severity into three buckets: critical, high, or low. The distribution of severity for detected incidents throughout the six-month period.

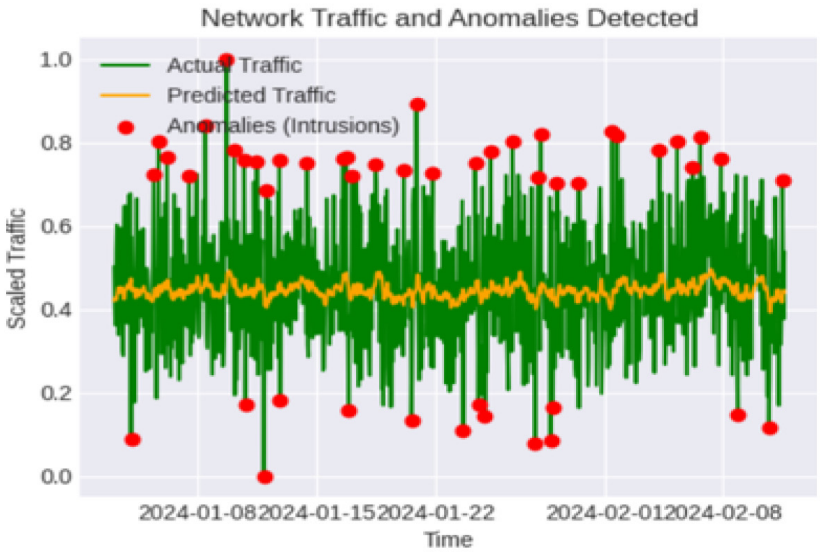

Figure 3

Visualization of anomalies detected over time

A new heatmap shown in Figure 4 was requested to visualize how the severity of incidents changed over time. We needed a way to quickly show how many incidents were low, medium, high or critical severity. The more high and critical severity incidents detected, the more we need to act now.

Incident Duration by Severity Level: The categorization of incident severity by our model provided us with more detailed information about the resolution time of incidents.

In Figure 5, incidents that belong to the highest severity category tend to have larger durations than low-severity incidents. It shows clear the relationship between how severe a threat is and how long it takes to resolve, which really reinforces that we need to be good at telling what's really going on so we can apply the appropriate level of response.

Time Saved by AI-Driven Incident Detection: A key performance metric for the AI model is reduction in response time demonstrated in Figure 6. Model detection time is compared to a baseline human-driven response time. On average, the reduction in AI detection times was significant as seen from the Table 1. The AI model provides an improvement over manual incident detection since it potentially reduces the manuscript detection time by minutes on average.

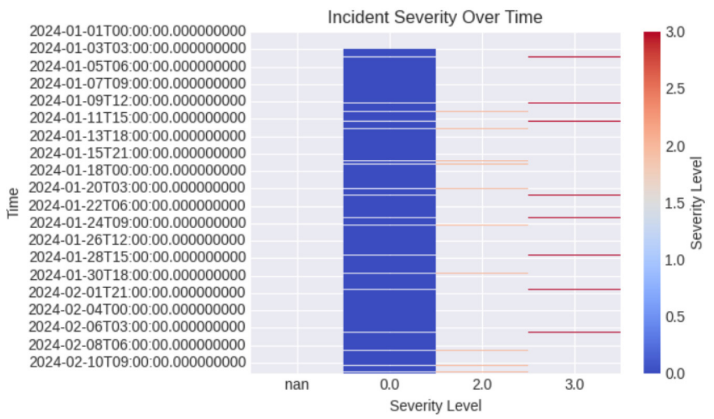

Figure 4

Heatmap showing severity of incidents over time

Table 1

Metrics showing anomaly detection and time saved by AI

Metric	Value
Total Anomalies detected	48
Average Detection Time	1369.83 minutes
Average Incident Duration	0.15 hours (9 minutes)
Baseline Response Time	2000 minutes
Time Saved by AI	630.17 minutes

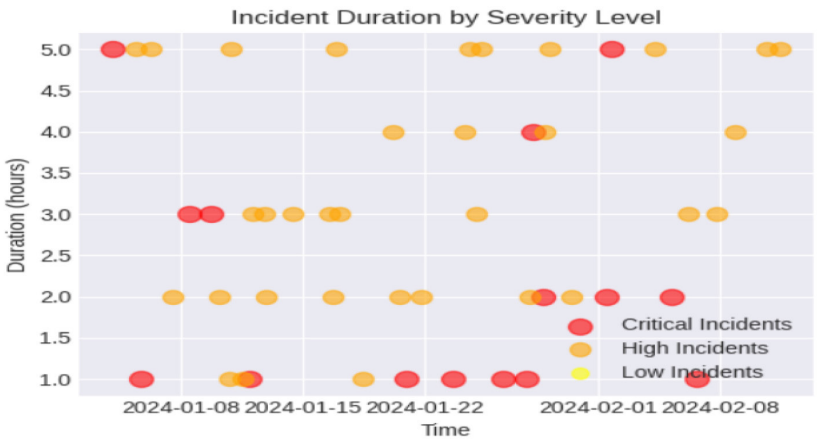

Figure 5

Incident duration by severity level

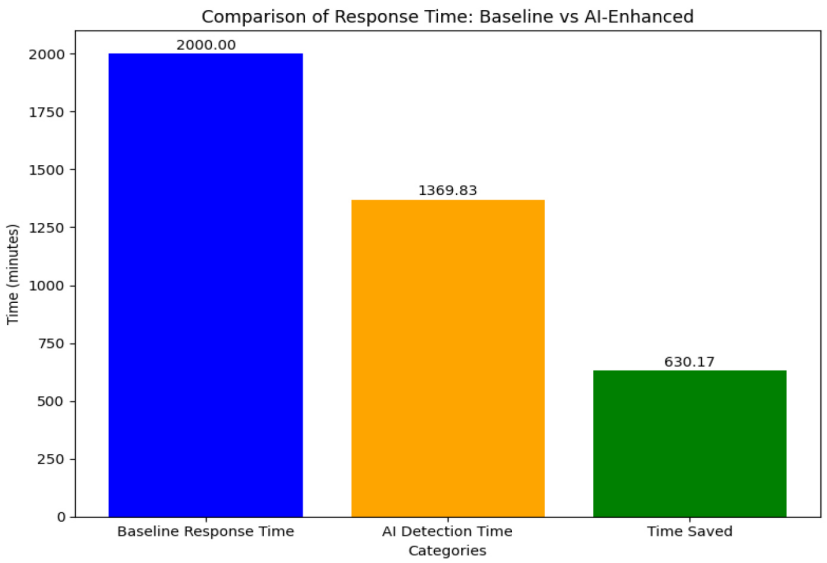

Figure 6

Time saved by AI-driven detection compared to human baseline

6. Conclusion

This study demonstrates the potential of AI in enhancing cybersecurity incident response through the continuous monitoring of network traffic

for anomaly detection in real time. The AI model detected network anomalies and reduced the time for detection and response as compared to conventional approaches. With automated detection and faster incident response, AI can significantly increase cyber-operations capability. Overall, this study suggests that AI can contribute to organizational security readiness to better respond and predict with minimal damage.

References

[1] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data and Information Management*, vol. 8, no. 2, pp. 100063 (Jun. 2024).

[2] S. Lysenko, N. Bobro, K. Korsunova, O. Vasylchyshyn, and Y. Tatarchenko, "The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats," *Economic Affairs*, vol. 69, no. 1, pp. 45–52 (Feb. 2024).

[3] S. Chahal, "AI-enhanced cyber incident response and recovery," *International Journal of Science and Research (IJSR)*, vol. 12, no. 3, pp. 1795–1801 (Mar. 2023).

[4] K. Fysarakis, A. Lekidis, V. Mavroeidis, K. Lampropoulos, G. Lyberopoulos, I. Garcia-Milà Vidal, J. C. Terés i Casals, E. Rodriguez Luna, A. A. Moreno Sancho, A. Mavrelos, M. Tsantekidis, S. Pape, A. Chatzopoulou, C. Nanou, G. Drivas, V. Photiou, G. Spanoudakis, and O. Koufopavlou, "PHOENI2X: A European cyber resilience framework with artificial-intelligence-assisted orchestration, automation and response capabilities for business continuity and recovery, incident response, and information exchange," in 2023 IEEE Int. Conf. Cyber Security and Resilience (CSR) (Jul. 2023).

[5] M. F. Rafy, "Artificial intelligence in cyber security," *SSRN Electron. J.* (Jan. 2024).

[6] M. A. M. Farzaan, M. C. Ghanem, A. El-Hajjar, and D. N. Ratnayake, "AI-enabled system for efficient and effective cyber incident detection and response in cloud environments," arXiv preprint arXiv:2404.05602 (Apr. 2024).

[7] K. Chandran, S. Panda, and B. Sreenivas, "An efficient secure authentication scheme for personalized healthcare system," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 1, pp. 215–227 (2020).

[8] M. Binhammad, S. Alqaydi, A. Othman, and L. H. Abuljadayel, "The role of AI in cyber security: Safeguarding digital identity," *Journal of Information Security,* vol. 15, no. 2, pp. 245–278 (2024), doi: 10.4236/jis.2024.152015.

[9] D. Goyal, F. Sheth, P. Mathur, and A. K. Gupta, "Discrete mathematical models for enhancing cybersecurity: A mathematical and statistical analysis of machine learning approaches in phishing attack detection," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 569–599 (2024).

[10] K. M. Manjunatha and M. Kempanna, "Count vectorizer model based web application vulnerability detection using artificial intelligence approach," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 7, pp. 2039–2048 (2022).

[11] R. Kaushik, V. Singh, and R. Kumari, "Multi-class SVM based network intrusion detection with attribute selection using infinite feature selection technique," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 8, pp. 2137–2153 (2021).

Received April, 2025