International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 11, pp 222-226, November-2025

https://doi.org/10.47001/IRJIET/2025.911027

AI-Driven Threat Detection and Response in Cybersecurity Using Autonomous Adaptive Approach

[1]Ismail Abdulkarim Adamu, [2]Joshua Umaru, [3]Mustapha Umar

[1,2,3]Department of Computer Science, Gombe state Polytechnic, Bajoga, Nigeria

***Abstract* - The exacerbating complexity and frequency of cyber threats present notable obstacles to conventional cybersecurity measures, necessitating the creation of more dynamic and intelligent systems. In this paper we developed a hybrid autonomous adaptive AI threat detection framework using hybrid machine learning algorithms such as unsupervised learning, supervised learning and reinforcement learning. The unsupervised learning is use for anomaly detection, supervised learning for threat classification and reinforcement learning for autonomous decision making. The system was implemented and analyse using NSL-KDD cybersecurity datasets to continuously learn from evolving attack pattern and autonomously respond to mitigate cyber threat risks in real time. The analysis result shows that the hybrid framework achieved 96.8% accuracy, 95.4 % precision, 97.2% recall, 93.6% F1-Score, 2.1% FPR and response time of 25ms. The result indicates that the hybrid framework achieved a strong learning ability in correctly identifying attacks, minimized the number of false threat alert, reduced system workload during analysis and speedily mitigate real-time threats detected in live network.**

Keywords: Cybersecurity, Artificial intelligence, Unsupervised learning, Supervised Learning and Reinforcement learning.

I. INTRODUCTION

Cybersecurity refers to a set of technologies, processes and practices used to protect and defend networks, devices, software and data from attack, damage or illegal access (Kaur *et al.*, 2023). There different cyber-attacks such as malware, phishing, ransomware, denial of service (DOS), distributed denial of service (DDOS), insider threats etc. that use to cause harm in the cyberspace (Shamar *et al.*, 2024). Cybersecurity has emerged as a crucial area of concern in the digital and connected device era, as the frequency and complexity of cyber threats continue to rise (Ali *et al.*, 2025). Conventional cybersecurity strategies, like firewalls, intrusion detection systems (IDS), and antivirus software, often depend on predetermined signatures and protocols, which prove insufficient against emerging and changing cyber threats (Padmaraju, 2023). The emergence of advanced persistent threats (APTs), zero-day vulnerabilities, and sophisticated malware underscores the need for the advancement of more adaptive and intelligent cybersecurity mechanisms (Sfetcu, 2024). Despite advancements in cybersecurity measures, current systems face significant challenges in effectively detecting and mitigating sophisticated and novel cyber threats. Traditional methods often generate high false positive rates and fail to adapt quickly to new threat vectors (Kumar *et al.*, 2023). However, artificial intelligence (AI) approached have been implemented to enhance the traditional cybersecurity techniques. The ability of AI to analyze large dataset to detect patterns and anomalies and make informed decision without any human intervention, makes it a game changer in enhancing cybersecurity. Unlike traditional cybersecurity approach, the AI does not depend on predetermine rules to make informed decisions, it can learn from new data automatically and detects unknown threats (Obafemi, 2024). This gap necessitates the idea of an AI-driven threat detection and response system that can continuously learn and adapt to emerging threats, providing robust, real-time protection. Moreso, Artificial Intelligence (AI) presents a hopeful resolution by bolstering the capacity to recognize, categorize, and counter cyber threats in real-time.

In this paper we implemented a hybrid autonomous AI-driven adaptive threats detection system by integrating some machine learning techniques such as unsupervised learning, supervised learning and reinforcement learning. This is to effectively detects, analyse and responds to cyber threat in real-time. The remaining part of the paper is classified as follows: Section 2 literature review, 3 methodology, 4 system architecture, 5 experimental design and result and 6 conclusions.

II. LITERATURE REVIEW

Kaur *et al.*, (2023), performed an extensive examination of 236 primary studies in order to investigate the utilization of artificial intelligence techniques for enhancing cybersecurity protocols. The results of the investigation underscored the wide-ranging uses of artificial intelligence in cybersecurity, encompassing machine learning, natural language processing, image processing, and other areas. The examination grouped the artificial intelligence applications according to fundamental domains such as reasoning, planning, learning, communication, and perception. There work in general underscores the importance of artificial intelligence in bolstering security protocols and identifies areas for further research and future pathways for exploration in the realm of artificial intelligence for cybersecurity.

Padmaraju (2023), carried out an investigation into the role of Artificial Intelligence (AI) in augmenting cybersecurity mechanisms. The methodology in the research comprises an extensive examination of current literature on AI and cybersecurity, with a focus on machine learning algorithms that preserve privacy and the utilization of AI for identifying and preventing cyber threats. He deliberates on the criteria for assessing the efficiency of AI-driven cybersecurity systems, including detection rate, false positive rate, false negative rate, response time, scalability, and adaptability. The results of the study underscore the transformative influence of AI on cybersecurity, underscoring its capacity to scrutinize vast datasets, identify patterns and anomalies, and make decisions based on data autonomously. AI-driven solutions have demonstrated their effectiveness in improving threat detection and response times, decreasing the occurrence of false positives and negatives, and enhancing scalability and automation in cybersecurity operations. Through the synergistic deployment of AI and human expertise, organizations can devise more resilient cybersecurity strategies to effectively counter evolving cyber threats.

Adi *et al.*, (2022), delineate the transition in the progression of artificial intelligence methodologies, showcasing the efficacy of contemporary AI strategies in facilitating an adversary to achieve their goals related to cyberattacks.

Abraham *et al.*, (2023), elucidate the limitations of conventional security protection mechanisms and deliberate on the advancements achieved through the integration of artificial intelligence to address contemporary cybersecurity challenges. This endeavor may enhance the capabilities of detection technologies and algorithms for safeguarding computer networks.

Sarker *et al.*, (2021), There research offers a thorough examination of AI-driven Cybersecurity, showcasing its significance in the realm of intelligent cybersecurity services and management. Moreso, it exposes various avenues for research within the parameters of the investigation, thereby facilitating prospective research endeavors AI-driven cybersecurity domain.

III. RESULTS AND DISCUSSIONS

To achieve the autonomous adaptive cybersecurity framework in this paper, we integrate both supervised, unsupervised and reinforcement learning. This is to ensure that the framework continuously evolve with the emergent cyber threat landscape. The processes of the framework development include:

3.1 Data collection

The data used in this work are collected from network traffic, system logs, firewall log and user behaviour using wireshark. The input data stream is the raw data the system monitors continuously represented as:

$$X = \{x_1, x_2, \dots, x_n\}, \quad x_i \in \mathbb{R}^d$$

Where X represent the set of incoming network data samples such as logs, packets and user activities and x_i represent each data point with features d which represent the Source IP, Packet sizes, destination port, and protocol types used.

3.2 Anomaly Detection

Unsupervised learning is adopted using Autoencoder algorithm for anomaly detection in the system. Autoencoder is used to reconstruct the input as follows:

$$\hat{x} = f_{dec}\left(f_{enc}(x)\right)$$

Where: $\boldsymbol{f_{enc}}$ represents the Encoder that compresses the input into a lower-dimensional representation and $\boldsymbol{f_{dec}}$ represents the Decoder that tries to reconstruct the original input from the compressed version.

An anomaly score is used to reconstruct the error and shows the difference between the actual input from the reconstructed input represented as:

$$A(x) = \| x - \hat{x} \|^2$$

And a threshold $\boldsymbol{\theta}$ is used to determines the anomaly:

$$label(x) = \begin{cases} 1 & \textbf{if } A(x) > \theta \\ 0 & \textbf{otherwise} \end{cases}$$

If the anomaly score is greater than the threshold θ, the sample is flagged as a threat. Otherwise, it is considered normal.

3.3 Threat Classification

We used supervised learning algorithm such as Random Forest algorithm for threats classification. The threats classification is represented as:

$$\min_{h} \mathcal{L}(y, h(x))$$

Where $\boldsymbol{h(x)}$ represents the classifier that predicts whether the class of the input detected is benign or anomalous. it is train to minimize loss functions, $\boldsymbol{y}$ is the true label of the data from labeled training datasets and $\boldsymbol{\mathcal{L}}$ is the loss function that measures the difference between predicted and actual labels.

3.4 Reinforcement learning

Reinforcement learning enables the system to respond in a suitable manner as soon as a threat is detected or classified. The environment is defined by states S, actions A, transition probabilities P, and reward function R. The agent learns an optima policy through Deep Q-learning as follows:

$$Q(s,a) \leftarrow Q(s,a) + \alpha\left(r + \gamma \max_{a} Q(s',a') - Q(s,a)\right)$$

Here:

$\boldsymbol{s}$**:** Represent the current state of the system e.g., attack ongoing, normal traffic etc.

$\boldsymbol{a}$**:** Represents actions to be taken e.g., block IP, isolate device, send alert, etc.

$\boldsymbol{Q(s,a)}$**:** Is the value of taking an action a in state s.

$\boldsymbol{\alpha}$**:** Represents the learning rate showing how much new knowledge updates old knowledge).

$\boldsymbol{r}$**:** Is the reward signal indicating positive if the response mitigates attack and negative if it fails.

$\boldsymbol{\gamma}$**:** Represents the discount factor signifying the importance of future rewards vs. immediate rewards.

$\boldsymbol{s'}$**:** Represents the next state after action a has been executed.

The Q-values in the equation is updated over time to allow the system learns best response to anomaly autonomously using Deep Q-learning.

IV. SYSTEM ARCHITECTURE

The architecture of the hybrid autonomous framework function by first accepting stream of data from different sources which include system logs, network traffic firewall logs, user behaviour etc. for anomaly detection using unsupervised learning algorithm. If there exist any detected anomaly on the stream data by anomaly detector engine it is flagged and classified using supervised learning. Reinforcement learning is triggered to act on the classified attacks to determine the optimal system response. The adaptive decision function integrates output from the three techniques to ensure final action on the input which include to block the input data if anomalous or allow input data to process if benign.

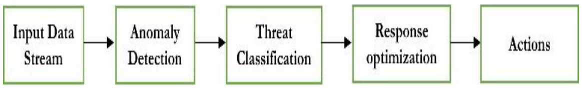

Figure 1: Architecture of the hybrid framework

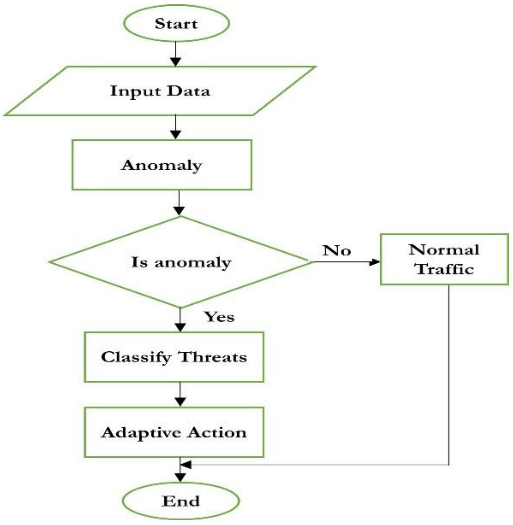

Figure 2: Flowchart of the hybrid framework

4.1 Algorithm of the system

```
Algorithm for AI-Adaptive Threat Detection and Response
Input: Incoming data stream X
Output: autonomous decision action D
1. For each data sample x in X:
2.      Compute reconstruction error A(x)
3.      If A(x) > θ then
4.          Label x as anomaly
5.          Trigger RL-based response Q(s,a)
6.      Else
7.          Use classifier h(x) to classify x
8.          If classified as attack then
9.              Trigger RL-based response Q(s,a)
10.         Else
11.             Mark as benign
12.     End If
13. Return decision D(x)
```

V. EXPERIMENTAL DESIGN AND RESULT

5.1 Anomaly Detection

5.1.1 Dataset

The dataset used in the design of the hybrid framework is NSL-KDD.

ISSN (online): 2581-3048
Volume 9, Issue 11, pp 222-226, November-2025
https://doi.org/10.47001/IRJIET/2025.911027

5.1.2 Simulation Environment

The experiment was conducted on virtual environment using docker container to simulate different attacks and defenses and OpenAI Gym platform was used for reinforcement learning.

5.1.3 Software/Hardware Tool

Python (TensorFlow, PyTorch, and scikit-learn) was used to run the experiment code, suricata and wireshark for data collection and GPU enabled servers for data training.

5.2 Experimental Result

The system was experimented using NSL-KDD cybersecurity dataset to obtain the performance result of the hybrid model. The hybrid frame was evaluated using Accuracy, Precision, Recall, F1-score, False positive rate (FPR), and Response time metrics to analyze the performance of system.

The hybrid frameworks well on NSL-KDD datasets because they contain different known attack types. The hybrid method adopted generalizes well to structures signature and anomaly patterns. The result analysis from table1 above shows that:

Table 1: Result Analysis using NSL-KDD Datasets

Datasets	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)	Avg. Response time (%)
NSL-KDD	96.8	95.4	97.2	96.3	2.1	25

Accuracy achieved 96.8% which indicates the system correctly identified almost all normal and attack traffic showing a strong learning ability from structured attack patterns. Precision achieved 95.4% indicating that form all threat alerts raised 95.4% were truly an attack reducing the number of false alarms. Recall achieved 97.2% which shows that the system was able to detect almost all threat attacks allowing only few which is very crucial for minimizing undetected attacks or intrusion. F1-Score achieves 96.3% which shows a balance performance combining precision and recall. False positive Rate (FPR) achieved 2.1% showing a very low false positive rate, indicating a reduced analysis in the system workload. Response Time were achieved in 25ms indicating that the system is fast enough to mitigate real time threats detected in live networks.

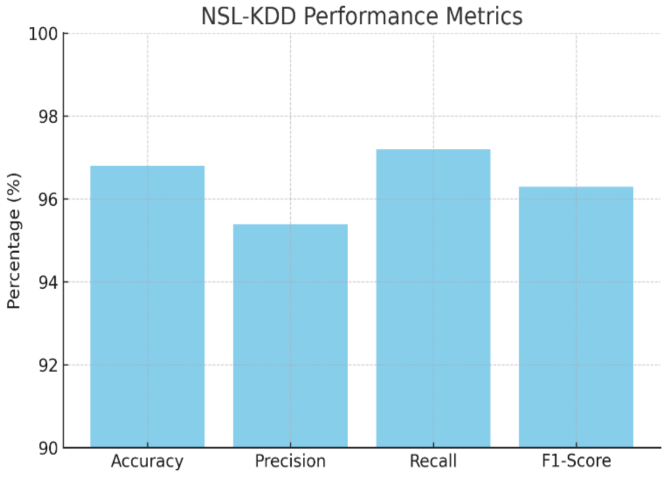

Figure 3: Image of the analysis result

VI. CONCLUSION

In this paper we developed a hybrid AI-driven autonomous and adaptive framework for cyber threats detection by integrating unsupervised learning, supervised learning and reinforcement learning. The result obtained shows an improved accuracy, reduced false positive rate and a reasonable real-time autonomous response making it suitable for emergent threat detection and prevention. The hybrid framework was implemented using NSL-KDD cybersecurity datasets and in the future, we aimed to explore other datasets and make comparable performance analysis to test the effectiveness of the system.

ACKNOWLEDGEMENT

I want to extend my profound gratitude to the Tertiary education Trust Fund (Tetfund) for sponsoring and making this research a reality.

REFERENCES

[1] Abrham, T., Kaddoura, S., & Al Breiki, H. (2023). Artificial intelligence applications in cybersecurity. *In Handbook of Research on AI Methods and Applications in Computer Engineering* (pp. 179-205). *IGI Global*.

[2] Adi, E., Baig, Z., & Zeadally, S. (2022). Artificial Intelligence for Cybersecurity: Offensive Tactics, Mitigation Techniques and Future Directions. *Applied Cybersecurity & Internet Governance*, 1(1), 1-23.

[3] Ali, S., Wang, J., & Leung, V. C. M. (2025). AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy

ISSN (online): 2581-3048
Volume 9, Issue 11, pp 222-226, November-2025
https://doi.org/10.47001/IRJIET/2025.911027

implications for evolving paradigms: A comprehensive review. *Information Fusion*, 102922.

[4] Binhammad, M., Alqaydi, S., Othman, A., &Abuljadayel, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. *Journal of Information Security*, 15(02), 245-278.

[5] Barik, K., Misra, S., & Fernandez-Sanz, L. (2024). Adversarial attack detection framework based on optimized weighted conditional stepwise adversarial network. *International Journal of Information Security*, 1-24.

[6] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 101804.

[7] Kumar, N., Sen, A., Hordiichuk, V., Jaramillo, M., Molodetskyi, B., & Kasture, A. (2023). AI in cybersecurity: threat detection and response with machine learning. *Tuijin Jishu/Journal of Propulsion Technology*, 44(3), 38-46.

[8] Obafemi, O. A. (2024). AI-Driven Threat Detection and Response Systems: Advancing Cybersecurity.

[9] Padmaraju, A. K. (2023). Cybersecurity in the AI Era: Ensuring Your Data Stays Protected. *Journal of Computer Architecture*, 10(1), 9-14.

[10] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, 2(3), 173.

[11] Sfetcu, N. (2024). Advanced persistent threats in cybersecurity–Cyber warfare. *MultiMedia Publishing*.

[12] Sharma, R., Vashistha, S., & Sharma, S. Artificial Intelligence: A Game Changer in Cyber Security.

AUTHORS BIOGRAPHY

Mr. Ismail Abdulmarim Adamu, Lecturer I in the department of computer science Gombe state polytechnic, Bajoga, Nigeria.

Mr. Joshua Umaru, Principal Technologist in the department of computer science, Gombe state polytechnic, Bajoga, Nigeria.

Mr. Mustapha Umar, Lecturer II in the department of computer science, Gombe state polytechnic, Bajoga, Nigeria.

Citation of this Article:

Ismail Abdulkarim Adamu, Joshua Umaru, & Mustapha Umar. (2025). AI-Driven Threat Detection and Response in Cybersecurity Using Autonomous Adaptive Approach. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(11), 222-226. Article DOI https://doi.org/10.47001/IRJIET/2025.911027

****