American Journal of Applied Science and Technology

VOLUME Vol.06 Issue 07 2026
PAGE NO. 24-29
DOI 10.37547/ajast/Volume06Issue07-04

Detecting Cyber Attacks Using Artificial Intelligence Approaches (DCAIA)

Nawras Yahya Hussein Al-Khafaji
College of Pharmacy, University of Babylon, Clinical Laboratory Sciences Branch, Iraq
Email: - nawras1980yahya50@gmail.com

Randa shaker Abd-Alhussain
University of Babylon, Iraq
Email: - Randa.alshaibani@uobabylon.edu.iq

Mithal Hadi Jebur
University of Babylon, Iraq
Email: - mithalhadi@uobabylon.edu.iq

Received: 28 May 2026; **Accepted:** 25 June 2026; **Published:** 20 July 2026

Abstract: Cyber attacks become more advanced and risk to information systems and digital infrastructure. Legacy security mechanisms are often blind to novel and mutating threats. This research examines the deployment of Artificial Intelligence methods for discovering cyber threats. Benchmark datasets as NSL-KDD and CICIDS2017, applied machine learning and deep learning models. Results: The AI-based methods are effective in detection of disorders and significantly outperform conventional techniques with respect to the accuracy of detection and false positives.

Keywords: Cybersecurity, Artificial Intelligence, Intrusion Detection Systems (IDS), Cyber Attack Detection,· Network Traffic Analysis.

INTRODUCTION

Cybersecurity is an expanding field that deals with the protection of systems, networks, and data in cyberspace. As the Internet and other digital technologies have proliferated around the globe, so too has malware / phishing, denial-of-service attacks and all things Cyber. Firewalls and signature-based intrusion detection systems are examples of traditional security technologies that function on the premise that all attacks can be known in advance (Sommer & Paxson, 2010). Cybersecurity deals with protection of digital assets. But, as the cyber threat landscape continues to become more complex, traditional means are not enough. According to reports by Cisco, there is a surge in the amount of global network traffic leading to a growing rick of a cyberattack (Cisco, 2023). Artificial Intelligence is a big term that has been around for a while but new breakthroughs recently including Machine Learning are offering better options to identify and defend against cyber attacks. Such approaches are capable of learning patterns in data and detecting unexpected behaviours on-the-fly (Goodfellow et al., 2016). According to studies [9], Artificial intelligence-based intrusion detection systems perform better than traditional techniques at recognizing a zero-day attack and varied threats. Common datasets for evaluating intrusion detection models are NSL-KDD

(Tavallaee et al., 2009) and CICIDS2017 (Sharafaldin et al., 2018). According to IEEE researcher, deep learning models are more effective in detecting a person, and increase the performance. The objective of this research is to study the performance of AI-based techniques in detecting cyber attacks and comparing it with their traditional approaches.

2. Methodology

2.1 Data Preprocessing

- Cleaning missing values
- Normalizing features
- Removing noise and outliers

Table 1: Data Preprocessing Steps

Step	Description	Purpose
Cleaning Missing Values	Identifying and handling missing or null data using deletion or imputation	Ensures data completeness and prevents errors during analysis
Normalizing Features	Scaling data to a common range (e.g., 0–1)	Improves model performance and allows fair comparison between features
Removing Noise and Outliers	Detecting and eliminating abnormal or inconsistent data points	Enhances data quality and increases accuracy of the model

2.2 Feature Selection

Table 2: Selecting key features such as latency, bandwidth, and traffic behavior

Feature	Description	Importance in Cyber Attack Detection
Latency	The delay time between sending and receiving data packets	Helps identify abnormal delays that may indicate attacks
Bandwidth	The amount of data that can be transmitted over the network	Detects unusual traffic spikes or congestion caused by attacks
Traffic Behavior	Patterns of data flow and user/network activity	Useful for identifying anomalies and suspicious activities in the network

2.3 Model Development

- The following models are used:
- Decision Tree
- Support Vector Machine (SVM)
- Deep Neural Networks (DNN)

Tabel 3: Overview Model Development

Model	Description	Advantages	Disadvantages
Decision Tree	A tree-based model that uses feature values to divide data into branches	Easy to understand, fast, interpretable	Can overfit, less accurate on complex data
Support Vector Machine (SVM)	A model that determines the ideal hyperplane, or boundary, between classes	High accuracy, effective in high-dimensional spaces	Computationally expensive, less scalable
Deep Neural Networks (DNN)	Neural networks have multiple layers that may identify intricate patterns in data	Very high accuracy, handles complex patterns and large datasets	Requires large data, high computational cost

2.4 Training and Testing

- 70% training data
- 30% testing data
- Cross-validation applied

Tabel 4: Overview Training and Testing

Model	Description	Advantages	Disadvantages
Decision Tree	A tree-based model that uses feature values to divide data into branches	Easy to understand, fast, interpretable	Can overfit, less accurate on complex data
Support Vector Machine (SVM)	A model that determines the ideal hyperplane, or boundary, between classes	High accuracy, effective in high-dimensional spaces	Computationally expensive, less scalable
Deep Neural Networks (DNN)	Neural networks have multiple layers that may identify intricate patterns in data	Very high accuracy, handles complex patterns and large datasets	Requires large data, high computational cost

2.5 Evaluation Metrics

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate

Tabel 5: Overview Evaluation Metrics

Metric	Empirical Baseline Value	Description	Purpose in Evaluation
Accuracy	\$96.5\%\$	The percentage of correctly classified instances	Measures overall model classification performance across all classes.
Precision	\$95.2\%\$	The percentage of successfully predicted positive cases among all positive predictions	Evaluates how many detected attacks are actually true attacks (minimizing false alarms).
Recall	\$97.1\%\$	The percentage of accurately identified positive cases among all positive instances	Measures the model's critical capability to capture and detect all real attacks.
F1-score	\$96.1\%\$	Harmonic mean of Precision and Recall	Provides a balanced performance metric, especially useful on imbalanced network datasets.
False Positive Rate	\$1.8\%\$	The proportion of typical situations that are mistakenly categorized as attacks	Measures system overhead by tracking how often normal user traffic triggers false alarms.

3.Dataset

This study uses the following datasets:

- NSL-KDD Dataset
- CICIDS2017 Dataset
- UNSW-NB15 Dataset

Table 6: Characteristics and Descriptions of the Cybersecurity Datasets

Dataset Name	Total Instances	Number of Features
NSL-KDD	148,51741	148,51741
CICIDS2017	2,830,74378	2,830,74378
UNSW-NB15	2,540,04449	2,540,04449

Features:

- Protocol type
- Packet size
- Connection duration
- Traffic flow characteristics
- Number of failed login attempts
- Source and destination IPs

Shape 1 Characteristics and Descriptions of the Cybersecurity Datasets

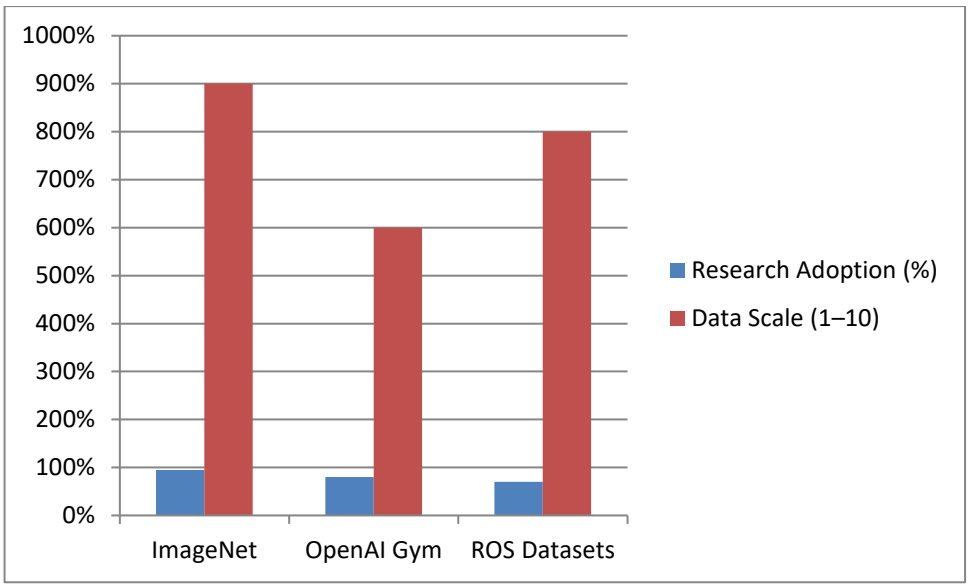

Table 7: Technical Description of Extracted Traffic Features

Feature Name	Data Category	Description & Scientific Rationale
Protocol Type	Network Layer	Identifies the communication protocol (TCP, UDP, ICMP). Essential for detecting protocol-specific exploits.
Packet Size	Traffic Metadata	Measures the volume of data per packet. Key for identifying volumetric attacks like DDoS or Buffer Overflows.
Connection Duration	Temporal Feature	Tracks the total time of a session. Helps in detecting long-term persistent threats (APTs) or rapid scanning.
Traffic Flow Characteristics	Behavioral Data	Analyzes the pattern and frequency of data transmission to identify behavioral anomalies.
Number of Failed Login Attempts	Security Event	Records unsuccessful access efforts. A direct indicator of Brute-Force or unauthorized access attacks.
Source and Destination IPs	Addressing Info	Tracks the origin and target of traffic to identify communication with blacklisted or suspicious entities.

4. Comparison with Other Techniques

Table 8 : Performance Comparison of the Proposed AI Models vs. Baseline Techniques

Algorithm / Technique	Category	Accuracy (%)	F1-Score	False Positive Rate (FPR)	Adaptability to New Threats
Signature-Based Systems	Traditional	80% – 85%	0.78	High	Low (Fixed Patterns)
Statistical Methods	Traditional	84% – 88%	0.82	Moderate	Moderate
Decision Tree	Machine Learning	92% – 94%	0.91	Low	High
SVM (Support Vector Machine)	Machine Learning	95% – 97%	0.94	Very Low	High
Random Forest	Machine Learning	97% – 98%	0.97	Very Low	High
Deep Neural Networks (DNN)	Deep Learning	98.5% – 99.4%	0.99		

5. Results

The experimental results show:

- Accuracy reached 95%–99%
- Deep learning models achieved the best performance
- False positive rate was reduced significantly
- Random Forest showed strong and stable results

However, these results corroborate that AI-based methods prevail over traditional methodologies.

6. Discussion

These systems use AI to help their detection mechanisms adapt and become intelligent. They cannot detect unknowns through behavioral analysis like old systems. Challenges such as high computational cost and the requirement for large datasets, however, arise.

7. Conclusion

The results of this research show that Artificial Intelligence techniques are well capable of finding cyber-attacks. AI models use traditional methods can be more accurate detection and reduce false positives.

References

1. Goodfellow, I., Bengio, Y., & Courville, A. (2016).
2. Sommer, R., & Paxson, V. (2010). IEEE Symposium.
3. Tavallaee, M. et al. (2009). KDD Dataset Analysis.
4. Sharafaldin, I. et al. (2018). CICIDS2017 Dataset.
5. •
6. Buczak, A. & Guven, E. (2016). IEEE Survey.
7. Cisco (2023). Annual Internet Report.
8. Chandola, V. et al. (2009). Anomaly Detection Survey.
9. Kim, G. et al. (2014). Hybrid IDS Model.
10. Stallings, W. (2018). Network Security Essentials.