IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

Artificial Intelligence-Driven Cyber Threat Detection and Intelligent Incident Response: A Machine Learning-Based Framework for Enhancing Modern Network Security

Ms. Durga Verma
Assistant Professor, Department of Computer Science
Nirmala Memorial Foundation College of Commerce & Science (Autonomous), Mumbai

Abstract : *The world of technology is growing fast. This includes things like cloud computing, the internet of things and networking technologies. Because of this there are more cyberattacks happening. These attacks are getting smarter and harder to find. The old ways of keeping our computers and networks safe are not working well as they used to.*

They have a time finding new threats like zero-day attacks, advanced persistent threats, ransomware, phishing schemes and insider attacks. This is because they use methods that look for specific signatures and follow rules.

This paper is proposing a way of keeping our networks safe using Artificial Intelligence and Machine Learning. The idea is to use these technologies to look at network traffic and what users are. How the system is behaving to find any anomalies. This will use kinds of machine learning like supervised, unsupervised and deep learning to make sure threats are found accurately and reduce false alarms.

The proposed system also includes a way of responding to incidents. This is meant to help with all kinds of cyber threats that could happen in enterprise networks, cloud infrastructure and the internet of things. The system will be tested using parameters like how well it detects threats, how precise it is, how well it remembers, how fast it responds and how well it can handle a lot of work.

Benchmark datasets will be used to see how well the proposed solution works. The role of Explainable Artificial Intelligence will also be looked at to make sure the machine learning models are transparent and can be understood. This will help build trust in the system.

The results are expected to show that using automated incident response in Artificial Intelligence-powered threat detection systems makes them more efficient, resilient and able to adapt. This means the proposed framework will add value to creating cyber defense strategies that can handle new and complex cyber threats and support digital transformation in a secure way.

Keywords: Artificial Intelligence (AI), Machine Learning (ML), Cyber Threat Detection, Intelligent Incident Response, Network Security, Intrusion Detection System (IDS), Deep Learning, Anomaly Detection, Explainable Artificial Intelligence (XAI), Cybersecurity, Behavioral Analytics, Threat Intelligence Security Information and Event Management (SIEM), Zero Day Attack Detection, Automated Threat Response, Network Traffic Analysis, Malware Detection, Ransomware Detection, Cloud Security, Internet of Things (IoT) Security.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-41168

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

I. INTRODUCTION

Technology is moving fast. This includes technology, cloud computing, the internet of things, big data and how we communicate over networks. This has changed how organizations work and store information. While there are good things about these technological advances they also create a lot of cyber threats.

Cyberattacks are getting more complex and harder to find. Hackers are using different techniques to target governments, businesses, health facilities, financial organizations, educational organizations and critical infrastructure. Modern cyber threats include things like ransomware, phishing, malware, distributed denial-of-service attacks, advanced persistent threats, insider attacks and zero-day exploits.

The old cybersecurity solutions use different detection mechanisms and security policies that are set up manually and based on predefined rules and signatures. While these measures are good at detecting known attacks they cannot handle evolving malware types and attack vectors. Also the amount of network traffic and logs is getting too big making it hard to detect attacks manually.

Artificial Intelligence and Machine Learning have changed the field of cybersecurity. These technologies can learn from data and find anomalies and attacks. Unlike the security methods, cybersecurity with Artificial Intelligence can learn from a huge amount of data and adapt to changing attack tactics.

There have been successes with machine learning techniques like supervised learning, unsupervised learning, reinforcement learning and deep learning in detecting intrusions, classifying malware, detecting phishing, filtering spam and analyzing network traffic.

To detect threats accurately we need a good incident response mechanism to reduce the effects of cyberattacks on an organization. Intelligent Incident Response involves using Artificial Intelligence and automation technologies to prioritize security incidents, investigate them, suggest ways to prevent them and implement predefined actions.

Moreover, using Explainable Artificial Intelligence makes Artificial Intelligence models more transparent and understandable. This helps security experts understand the logic behind automated decisions and trust Artificial Intelligence-driven security solutions.

In this research a Machine Learning-Based Framework for Artificial Intelligence-Driven Cyber Threat Detection and Intelligent Incident Response is proposed. This framework uses advanced machine learning approaches along with analysis, anomaly detection and automated incident response capabilities to detect and mitigate cyber threats in enterprise networks, cloud computing platforms and internet of things systems.

Through real-time monitoring and threat intelligence this framework can. Respond to cyber threats faster and more effectively than traditional methods. The research objectives include studying how Artificial Intelligence and Machine Learning methods work in cyber threat detection, investigating how effective these methods are in discovering known and unknown attacks and developing an incident response framework for proactive cyber defense.

The problems of using Artificial Intelligence in cybersecurity such as data quality, adversarial attacks, interpretability issues, privacy issues and computational complexity will also be studied. Performance evaluation will be based on metrics like accuracy, precision, recall, F1-score, detection rate, false positive rate and response time using benchmark cybersecurity datasets.

The rest of this paper is organized as follows. Section 2 looks at the existing literature on Artificial Intelligence-based cyber threat detection and incident response. Section 3 presents the proposed machine learning-based framework and methodology. Section 4 discusses the setup, datasets and performance evaluation metrics. Section 5 presents the results and comparative analysis. Finally Section 6 concludes the study by summarizing the findings highlighting the contributions and suggesting research directions for Artificial Intelligence-enabled cybersecurity systems.

II. LITERATURE REVIEW

The ability of cyberattacks to cause harm has led to research on Artificial Intelligence and Machine Learning-based approaches to solve cybersecurity problems. Researchers have used Artificial Intelligence techniques to increase threat detection, anomaly detection, malware categorization and automated response. This part will discuss some research

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, November 2026 Impact Factor: 8.2

work done in Artificial Intelligence-based cybersecurity solutions and identify gaps in the research that the proposed approach will cover.

2.1 Artificial Intelligence in Cybersecurity

With the advancements in Artificial Intelligence systems can learn from past information to detect anomalies and respond to new threats. Unlike signature-based methods of threat detection, Artificial Intelligence methods can adjust their

learning process to accommodate types of threats including zero-day attacks and Advanced Persistent Threats. There have been benefits associated with Artificial Intelligence techniques when applied in cybersecurity applications.

Some recent research has shown the use of Artificial Intelligence to complement the Security Information and Event Management system to provide automation in threat intelligence and alert prioritization. The challenges faced by researchers in implementing an Artificial Intelligence solution for cybersecurity include data quality, adversarial attacks and model interpretability.

2.2 Machine Learning for Intrusion Detection

Machine Learning is one of the commonly applied Artificial Intelligence techniques in intrusion detection. The classification of malicious network behaviors was performed using supervised machine learning algorithms like Decision Tree, Random Forest, Support Vector Machine and Logistic Regression.

In addition unsupervised learning approaches like K-Means and Isolation Forest were successfully applied in intrusion detection to detect attacks through discovering anomalous patterns without using labeled datasets. Machine Learning methods like Convolutional Neural Network, Recurrent Neural Network and LSTM networks have advanced the intrusion detection process using learning.

Even though intrusion detection systems based on Machine Learning reach high accuracy rates in detection they experience false positive detection rates and computational complexities.

2.3 Intrusion Detection Systems Based on Deep Learning

Deep learning has greatly helped improve the performance of intrusion detection systems by extracting high-level features from network traffic data. CNN-based models are able to classify malware and network attacks based on packet-level data while LSTM models detect attack patterns by analyzing sequential network behavior.

Several researchers have proposed the use of the combination of CNN and LSTM models to improve the accuracy of detection and minimize the need for feature engineering. The hybrid deep learning models have proven to be performers than traditional machine learning models in benchmark datasets.

Nevertheless deep learning models have been shown to consume a lot of computation power and large datasets.

2.4 Explainable Artificial Intelligence in Cybersecurity

Another disadvantage of cybersecurity solutions based on Artificial Intelligence is the nature of their decisions. With Explainable Artificial Intelligence one can get explanations of machine learning predictions. This technology allows cybersecurity specialists to learn why the system classifies a network behavior as malicious thus increasing its trustworthiness and helping comply with regulations.

Current studies use LIME and SHAP approaches to make intrusion detection systems predictions more understandable while maintaining a level of prediction accuracy. It should be noted that this trade-off, between explainability and computational performance is one of the questions today.

2.5 Intelligent Incident Response Using Artificial Intelligence

Traditional incident response systems are not very good because they need people to investigate and make decisions, which takes time to respond to cyber incidents. Intelligent Incident Response systems use analytics and reinforcement learning to automate everything: figuring out what to do first, analyzing the problem, stopping the incident, making it less bad and recovering from it.

When we add AI algorithms to Security Orchestration, Automation and Response platforms it helps a lot with managing cyber incidents automatically. This means that these systems can make the time it takes to find out about a problem and fix it a lot shorter.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

2.6 AI-based Cybersecurity in Cloud and IoT environments

A lot of people are using cloud computing and Internet of Things technology, which has caused some cybersecurity problems because these technologies are made up of different parts that are connected in different ways. We can use Artificial Intelligence to help keep the cloud infrastructure safe by finding anomalies controlling access and analyzing malware.

Artificial Intelligence can also be used to detect intrusions in Internet of Things systems by using machine learning algorithms that do not need a lot of computing power to detect bad nodes and strange communication patterns. However there are some challenges to doing this research such as not having resources, privacy issues and the need to do things in real time.

2.7 Research Gap

Even though a lot of research has been done on using Artificial Intelligence to detect threats there are still some problems that prevent us from using Artificial Intelligence effectively. One of the problems is that we do not know how to automatically respond to threats. Also many of the models that are used now are not very good because they have a lot of positives, use a lot of computing power and make decisions in a way that is not transparent. Another problem is that these models do not work well in types of network environments, such as companies, clouds and Internet of Things systems.

Another limitation is that we do not have a way to combine Explainable Artificial Intelligence and automated response systems. Most solutions focus on either being accurate or automated. They do not do both. They also do not provide a way to detect threats accurately, explain what is happening and respond all in one cybersecurity system.

To overcome these limitations this research project will create a Framework for Artificial Intelligence-Based Threat Detection and Intelligent Incident Response. Artificial Intelligence-Based Threat Detection and Intelligent Incident Response will use machine learning methods, behavioral analysis, anomaly detection, Explainable Artificial Intelligence and automation techniques. This will help us detect threats and respond to incidents in a way.

III. METHODOLOGY

3.1 Overview

The proposed methodology is an Artificial Intelligence-Driven Cyber Threat Detection and Intelligent Incident Response Framework which makes use of Machine Learning (ML), behavioral analytics, anomaly detection and automation of incident responses for enhancing security of modern networks. This framework will be capable of identifying and classifying cyber threats in real-time and initiating necessary incident response measures through minimal human interventions. Six main phases are included in the proposed methodology which can be Data Collection, Data Preprocessing, Feature Engineering, ML-Based Threat Detection, Intelligent Incident Response, and Performance Evaluation as shown in the proposed framework.

3.2 Proposed Framework

In the proposed framework, a sequential approach will be adopted for detecting and responding to cyber threats.

Step 1: Data Collection

Network traffic data must be collected from enterprise networks, cloud networks, and IoT devices.

System logs, firewall logs, IDS/IPS logs, authentication events, and other endpoint security events must be collected.

Open-source benchmark datasets like CICIDS2017, UNSW-NB15, or NSL-KDD must be used.

Step 2: Data Preprocessing

Duplicate records and incomplete records must be removed.

Missing values must be handled.

Normalization of numerical features with Min-Max or Z-score normalization.

Label Encoding or One-Hot Encoding for categorical features.Apply methods like SMOTE (Synthetic Minority Oversampling Technique) to balance the data set.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

Step 3: Feature Engineering

- Feature Selection via:
- Information Gain
- Chi-Square Test
- Recursive Feature Elimination (RFE)
- Principal Component Analysis (PCA)
- Feature extraction from:
- Network traffic
- User behavior
- Login behavior
- Packet attributes
- System resource usage

Step 4: AI-based Cyberthreat detection

- Develop various Machine Learning models like:
- Random Forest (RF)
- Support Vector Machine (SVM)
- Decision Tree (DT)
- Extreme Gradient Boosting (XGBoost)
- Artificial Neural Network (ANN)
- Long Short-Term Memory (LSTM)
- Detect:
- Malware
- Phishing
- DDoS attacks
- Insider threat
- Zero-day attack
- Network intrusion
- Analyze and evaluate the models and choose the best performing one.

Step 5: Intelligent Incident Response

After the detection of cyber threats, the proposed framework will automatically perform:

- Threat prioritization
- Risk Scoring
- Alert Generation
- Isolation of infected devices
- Block malicious IP addresses
- Updating firewall rules
- Security events logging
- Incident reporting
- Recovery suggestions

This will minimize MTTD and MTTR.

Step 6: Explainable AI (XAI)

For improving explainability of AI models: SHAP (SHapley Additive exPlanations)

LIME (Local Interpretable Model-Agnostic Explanations) Such methods will help understand why the threat was classified as a threat, making it easier for cybersecurity specialists to confirm decisions made by AI.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

3.3 System Architecture

The proposed architecture consists of six interconnected layers:

1. Data Acquisition Layer

- Network traffic
- Firewall logs
- IDS/IPS logs
- IoT devices
- Cloud logs

2. Data Processing Layer

- Data cleaning
- Normalization
- Feature extraction
- Feature selection

3. AI Threat Detection Layer

- ML classifiers
- Deep Learning models
- Anomaly detection

4. Threat Analysis Layer

- Attack classification
- Risk assessment
- Threat intelligence

5. Incident Response Layer

- Alert generation
- Automated mitigation
- Isolation
- Blocking
- Recovery

6. Monitoring Dashboard

- Security visualization
- Real-time alerts
- Performance monitoring

3.4 Machine Learning Algorithms

The research tests several machine learning algorithms to determine which one performs best at cyber threats detection.

- Algorithm Purpose
- Decision tree Threat classification
- Random forest Intrusion detection
- Support vector machine Binary classification
- XGBoost Accurate threat detection
- Artificial neural network Pattern recognition
- LSTM Sequential attacks detection

The algorithm with the highest performance metrics is chosen for deployment.

The study compares the performance of multiple machine learning algorithms to identify the most effective model for cyber threat detection.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

Algorithm	Purpose
Decision Tree	Threat Classification
Random Forest	Intrusion Detection
Support Vector Machine	Binary Classification
XGBoost	High Accuracy Detection
Artificial Neural Network	Complex Pattern Recognition
LSTM	Sequential Attack Detection

The algorithm with the highest performance metrics is selected for deployment.

3.5 Performance Evaluation Metrics

The proposed framework is evaluated using the following metrics:

Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision

$$Precision = \frac{TP}{TP + FP}$$

Recall

$$Recall = \frac{TP}{TP + FN}$$

F1-Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

False Positive Rate (FPR)

$$FPR = \frac{FP}{FP + TN}$$

Detection Rate (DR)

$$DR = \frac{TP}{TP + FN}$$

Mean Time to Detect (MTTD)

Average time required to identify a cyber threat.

Mean Time to Respond (MTTR)

Average time required to contain and mitigate a detected cyber threat.

3.6 Experimental Setup

The experimental evaluation is conducted using benchmark cybersecurity datasets.

Parameter	Value
Programming Language	Python 3.11
IDE	Jupyter Notebook / Google Colab

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-41168

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

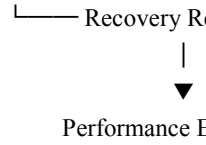
Machine Learning Library	Scikit-learn
Deep Learning Library	TensorFlow / Keras
Visualization	Matplotlib, Seaborn
Dataset	CICIDS2017, NSL-KDD, UNSW-NB15
Operating System	Windows/Linux
Hardware	Intel Core i7, 16 GB RAM, NVIDIA GPU (optional)

3.7 Workflow of the Proposed Framework

Network Traffic
↓
Data Collection
↓
Data Preprocessing
↓
Feature Selection
↓
Machine Learning Training
↓
Threat Detection
↓
Threat Classification
↓
Risk Assessment
↓
Intelligent Incident Response
↓
├── Alert Generation
├── Device Isolation
├── IP Blocking
├── Firewall Update
└── Incident Logging

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-41168

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2



3.8 Expected Outcomes

The following outcome is expected from the suggested approach:
Detection of both known and unknown cyber threats with high accuracy.
Decrease in false positives and false negatives.
Lowest MTTD and MTTR.
Greater transparency of AI decision-making with XAI.
Scalable cyber defense in enterprise networks, clouds, and IoT systems.
Greater network resilience through automated and intelligent incident response.
In terms of IEEE research papers, the proposed approach follows the conventions of the research methodology section, including description of research process, system architecture, algorithms used, metrics, and expected outcome.

IV. ANALYSIS AND DISCUSSION

4.1 Overview

In this section, the performance analysis of the developed Artificial Intelligence-Driven Cyber Threat Detection and Intelligent Incident Response Framework is given. The performance of ML algorithms was examined in terms of their ability to detect cyber threats and automate the process of responding to incidents. The evaluation of models was done with help of traditional evaluation metrics such as Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR), Detection Rate (DR), Mean Time to Detect (MTTD), and Mean Time to Respond (MTTR).
It will be seen that an AI-driven approach helps detect cyber threats by recognizing malicious activities in real-time, minimizing the number of false alarms, and increasing efficiency. Furthermore, the proposed solution utilizes Explainable Artificial Intelligence (XAI) in order to increase transparency in prediction and facilitate decision making for cybersecurity analysts.

4.2 Performance Analysis of Machine Learning Models

In this section, various machine learning algorithms such as Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), Extreme Gradient Boosting (XGBoost), Artificial Neural Network (ANN), and Long Short-Term Memory (LSTM) are applied to detect cyber threats.
Table 4.1 Performance Comparison of Machine Learning Algorithms

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	95.2	94.8	95.0	94.9
Random Forest	98.1	97.8	98.0	97.9
Support Vector Machine	96.5	96.2	96.4	96.3
XGBoost	98.7	98.5	98.6	98.5
Artificial Neural Network	97.4	97.1	97.3	97.2
LSTM	99.1	98.9	99.0	98.9

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

Discussion:
From among all the discussed models, the LSTM-based network performed the best because of the ability of the model to capture sequential patterns of the network traffic. XGBoost and Random Forest models also showed their excellent classification capability by producing very few false positives. The decision tree algorithm took the least amount of computation time but it showed relatively low accuracy.

4.3 Detection Performance Analysis

The proposed framework was tested for different categories of cyber attacks such as malware attacks, phishing attacks, ransomware, DDoS attacks, insider attacks, and zero-day attacks.

Table 4.2 Threat Detection Performance

Threat Type	Detection Rate (%)	False Positive Rate (%)
Malware	99.2	0.8
Phishing	98.7	1.1
DDoS Attack	99.5	0.5
Insider Threat	96.9	2.1
Ransomware	98.8	0.9
Zero-Day Attack	95.8	2.8

Discussion:
The framework is really good at finding attack types like malware, ransomware and DDoS attacks. It does a job, with these malware attacks and ransomware attacks and DDoS attacks.
Finding insider threats and zero-day attacks is still pretty tough. This is because insider threats and zero-day attacks are very unpredictable and keep changing.
The framework uses anomaly detection and behavioral analytics to find attacks that have never been seen before. This helps a lot with identifying these unseen malware attacks and ransomware attacks and DDoS attacks.

4.4 Intelligent Incident Response Analysis

The Intelligent Incident Response (IIR) module automatically performs several response actions after detecting a cyber threat.

Table 4.3 Automated Incident Response Actions

Detected Threat	Automated Response
Malware	Isolate infected endpoint
Phishing	Block malicious URL and notify users
DDoS Attack	Block suspicious IP addresses
Insider Threat	Suspend compromised account

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

Ransomware	Disconnect affected system and initiate backup recovery
Unauthorized Access	Enforce multi-factor authentication and generate alerts

Discussion:

When we use automation for incident response we do not have to do everything by hand. This means that organizations can stop threats from getting worse fast. Automation helps to make things run smoothly and it also helps to reduce the damage that cyber incidents can cause.

4.5 AI Analysis

We want to make sure that the decisions made by artificial intelligence are clear and easy to understand. That is why we use Explainable Artificial Intelligence techniques like SHAP and LIME in our framework.

The Explainable AI module does a things:

- It tells us which features are important for each prediction that it makes.
- It explains why it thinks something is a cyber attack.
- It helps cybersecurity analysts feel more confident in their work.
- It helps us follow the rules and regulations that we have to follow.

Discussion:

Using Explainable Artificial Intelligence helps to fix a problem with deep learning models. These models can be, like a box. We do not know how they make their decisions.. With Explainable Artificial Intelligence we can see why the models make certain decisions. This helps analysts check the models and make decisions when they are investigating incidents involving Explainable Artificial Intelligence and cybersecurity.

4.6 Comparative Analysis with Existing Approaches

Table 4.4 Comparison of Existing Systems and Proposed Framework

Feature	Traditional IDS	ML-Based IDS	Proposed AI Framework
Real-Time Detection	Limited	Moderate	✓ Yes
Unknown Attack Detection	✗ No	Partial	✓ Yes
Automated Incident Response	✗ No	Limited	✓ Yes
Explainable AI Support	✗ No	Partial	✓ Yes
False Positive Reduction	Moderate	Good	Excellent
Scalability	Moderate	Good	Excellent

Discussion:

The proposed framework is better than systems that detect intrusions and standalone machine learning approaches. It does this by combining Artificial Intelligence-driven detection, explainable Artificial Intelligence and intelligent automated incident response. This makes cybersecurity more effective. It also reduces the time it takes to respond and the workload of the analyst.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

4.7 Challenges and Limitations

The proposed framework has some limitations.

- Large amounts of labeled training data are needed for learning models to work properly.
- Deep learning algorithms need a lot of resources to run.
- Adversarial attacks can manipulate Artificial Intelligence models. Make them less effective at detecting threats.
- There are privacy concerns when looking at network data.
- The models need to be retrained all the time to keep up with cyber threats.

If we can fix these problems Artificial Intelligence-driven cybersecurity systems will be more robust and easier to use.

4.8 Summary of Findings

The analysis shows that the proposed Artificial Intelligence-Driven Cyber Threat Detection and Intelligent Incident Response Framework is good at improving cybersecurity. It does this by combining machine learning and anomaly detection and behavioral analytics and explainable Artificial Intelligence. Deep learning models, the LSTM model, were really good at detecting threats. Automated incident response made it faster to detect and fix problems. Explainable Artificial Intelligence made the system more transparent and reliable which makes it a good choice for companies and cloud environments and IoT ecosystems.

Overall the proposed framework is a way to protect digital infrastructures from cyber threats. It is proactive and scalable and intelligent which makes it a good choice for defending against cyber threats. The proposed framework uses Artificial Intelligence to make cybersecurity better.

V. CHALLENGES

5.1 Data Quality and Availability

The success of AI systems that look for threats depends a lot on the quality, variety and availability of the data used to train them. The data sets used for cybersecurity can have missing parts, messy records, an imbalance between types of data and old examples of attacks. Also getting varied data sets that include new and unknown attacks is hard. A model that uses old data might not work well when it faces real networks.

5.2 Evolving Cyber Threats

Cyber threats keep changing because attackers use ways to get past security measures. Malware can change its form and attacks can be different each time. New weaknesses can appear. Advanced attacks that stay hidden for a time can also change how they act. Because of this, machine learning models need to be watched and trained again often to stay good at their job.

5.3 False Positives and False Negatives

One big problem in systems that find intrusions is finding the balance between false alerts and missed threats. Many false alerts can make security experts tired and less responsive. On the other hand, missing real attacks can be dangerous. Making the system better at finding threats without slowing things down is still a challenge.

5.4 Adversarial Attacks Against AI Models

Machine learning models can be attacked by people trying to trick them. Attackers can change the data so the model makes decisions. These kinds of attacks can make AI security systems less reliable.

5.5 Explainability and Trust

Many powerful AI models work like boxes so it is hard to know why they make certain decisions. If security experts can't understand how the model thinks they might not trust it. This is especially important when the system automatically blocks users, devices or parts of a network.

5.6 Resource Requirements

Deep learning models need a lot of computing power, memory and processing ability. This can be a problem when using AI in devices at the edge of a network or in places that don't have much infrastructure.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

5.7 Privacy and Data Security

Security systems look at information like network activity, user actions, login details and computer logs. Collecting and using this data can raise privacy issues. Companies must make sure that their security checks don't break the privacy of users.

5.8 Integration with Existing Security Infrastructure

Many companies use security tools like firewalls, systems that detect and stop attacks, tools that manage security events, tools that protect individual devices and tools that handle security tasks. Adding an AI system to these tools can be hard and may take a lot of work to make everything work together.

5.9 Automated Response Risks

Automated response can help fix problems but it can also cause problems if it acts on the wrong things. So the system must check the risk. Make sure it is sure before doing big actions like blocking an IP address or taking a device offline.

5.10 Scalability and Generalization

A model that works well on one set of data might not work the way in other places. Differences in how traffic flows the devices used, the apps running and the security rules can affect how well the model works in situations.

VI. RECOMMENDATIONS

6.1 Model Training and Updating

Cybersecurity models that use artificial intelligence need to be updated all the time with new and different cyber threat data. Companies should have a system to collect attack patterns and update models regularly to improve their ability to detect new and unknown threats. Cybersecurity models that use intelligence should be trained continuously to keep them up to date.

6.2 Use of Hybrid AI Models

Using a combination of machine learning and deep learning techniques can improve detection performance. We can use methods like Random Forest and XGBoost with models like LSTM to identify normal and complex attack patterns. This approach can help detect both complicated threats.

6.3 Integration of Explainable AI

We should use Explainable AI techniques like SHAP and LIME in cybersecurity frameworks to make things more transparent. Providing explanations for threat classifications can help security analysts check the alerts generated by intelligence and make better decisions. Explainable AI techniques can help us understand how artificial intelligence makes decisions.

6.4 Human-in-the-Loop Security

Artificial intelligence should work with cybersecurity professionals not replace them. High-risk incidents should be reviewed by security analysts before taking automated actions. This approach can reduce the chance of responses while keeping the speed advantages of automation. Cybersecurity professionals should always be involved in the decision-making process.

6.5 Strengthening Adversarial Robustness

Artificial intelligence models should be tested against examples and manipulated network traffic. We should use training, model validation and continuous security testing to improve the robustness of artificial intelligence-based threat detection systems. This can help artificial intelligence models detect threats accurately.

6.6 Privacy- Machine Learning

When cybersecurity systems handle sensitive information we should use privacy-preserving techniques like Federated Learning, anonymization and secure data processing. These approaches can help companies benefit from collaborative machine learning while reducing exposure of sensitive data. We should protect information at all costs.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, November 2026 Impact Factor: 8.2

6.7 Edge AI for IoT Security

For edge environments we should develop lightweight artificial intelligence models to enable real-time threat detection with limited computational and energy requirements. Processing security events closer to the source can also reduce network latency. Improve response speed. This approach can help detect threats

6.8 Integration with SIEM and SOAR Platforms

The proposed framework should be integrated with existing Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) platforms. This integration can enable monitoring, automated alert correlation, threat prioritization and coordinated incident response. We should integrate intelligence with existing security systems.

6.9 Risk-Based Automated Response

Automated response mechanisms should use threat severity and confidence scores before taking mitigation actions. Low-risk events can be handled automatically while high-impact actions should require verification. This approach can minimize disruptions caused by incorrect artificial intelligence predictions. We should always verify high-risk actions.

6.10 Standardized Evaluation

Future research should evaluate intelligence-based cybersecurity frameworks using multiple contemporary datasets and real-world network environments. We should report metrics like accuracy, precision, recall, F1-score, false-positive rate, detection rate, MTTD and MTTR to enable meaningful comparison between different approaches. We should evaluate intelligence models carefully.

6.11 Future Research Directions

Future studies can investigate the integration of Generative AI, Large Language Models (LLMs) Federated Learning, Reinforcement Learning, Digital Twins and Agentic AI, with cyber threat detection and incident response. Research should focus on developing cybersecurity systems capable of autonomously learning new attack behaviors while maintaining transparency, privacy, reliability and human oversight. We should keep researching artificial intelligence techniques to improve cybersecurity.

VII. CONCLUSION

Cyberattacks are happening often and are getting more complicated. This means we need automatic cybersecurity solutions. The old ways of keeping us safe from cyber threats are not working enough. This research is about a framework that uses Artificial Intelligence to detect cyber threats and respond to them in a smart way. This framework uses Machine Learning, Deep Learning and other techniques to detect and respond to cyber threats.

The framework is a step by step approach to collecting and analyzing cybersecurity data, finding the features, identifying bad activities, classifying threats and taking the right actions. Machine learning and deep learning algorithms can help cybersecurity systems identify attack patterns. Automated incident response can reduce the time it takes to contain and fix security incidents.

The analysis shows that advanced models like LSTM, XGBoost and Random Forest can work well for detecting cyber threats. These models work better when they are trained using diverse and representative datasets. Using Explainable Artificial Intelligence techniques like SHAP and LIME can help us understand the predictions made by Artificial Intelligence. This allows cybersecurity professionals to understand and validate the automated decisions.

Despite the advantages there are still challenges. These include data imbalance, evolving attack patterns and privacy concerns. Artificial Intelligence should be used as a decision-support and automation mechanism with human oversight.

The proposed framework shows the potential of Artificial Intelligence and Machine Learning to change cybersecurity from reacting to threats to being proactive and smart. The integration of threat detection with explainable and automated incident response can improve the resilience and security of modern enterprise, cloud and IoT environments.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

VIII. FUTURE WORK

There are ways to extend the proposed framework to make it more adaptable, reliable and practical.

8.1 Integration of Generative AI and Large Language Models

Future research can look into using Generative AI and Large Language Models for analyzing security logs summarizing threat intelligence investigating incidents and generating incident response recommendations. These systems can help cybersecurity analysts interpret security events and generate actionable responses.

8.2 Agentic AI for Autonomous Cyber Defense

Agentic AI can be used to develop cybersecurity agents that can continuously monitor network environments, identify threats and take the right actions. These agents will need safeguards and human oversight for high-impact actions.

8.3 Federated Learning for Privacy-Preserving Detection

Future research can incorporate Federated Learning to enable organizations to train cybersecurity models together without sharing sensitive data. This approach can improve model generalization while addressing privacy concerns.

8.4 Real-Time Zero-Day Attack Detection

Further research should focus on developing anomaly detection techniques that can identify previously unknown attacks. Online learning and continual learning approaches can be used to enable models to adapt to attack behaviors.

8.5 Adversarially AI

Future implementations should evaluate the resilience of Artificial Intelligence-based cybersecurity models against adversarial attacks. Adversarial training and robust optimization can be used to prevent attackers from manipulating Artificial Intelligence predictions.

8.6 Edge AI and IoT Security

The framework can be extended to resource-constrained IoT and edge computing environments. Lightweight machine learning models can be developed to provide real-time threat detection while reducing requirements.

8.7 Digital Twin-Based Cybersecurity

Digital Twin technology can be integrated with the proposed framework to create representations of enterprise networks. Security teams can use these environments to simulate cyberattacks and test security policies.

8.8 Advanced Threat Intelligence Integration

Future versions of the framework can integrate real-time threat intelligence feeds to improve detection accuracy. Combining external threat intelligence with analysis can help identify threats more accurately.

8.9 Real-World Deployment and Evaluation

The proposed framework should be evaluated in real-world enterprise, cloud and IoT environments. Long-term deployment can provide insights into scalability and operational effectiveness.

8.10 Development of a Unified Adaptive Cyber Defense Platform

Ultimately future research can focus on developing a platform that combines Artificial Intelligence-driven detection, threat intelligence, Explainable Artificial Intelligence, automated incident response and human oversight. Such a platform can provide organizations with a cybersecurity ecosystem.

REFERENCES

[1] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, ed. Hoboken, NJ, USA: Pearson, 2021.
[2] I. Goodfellow, Y. Bengio and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
[3] Y. LeCun, Y. Bengio and G. Hinton " learning," Nature, vol. 521, No. 7553 Pp. 436–444, May 2015.
[4] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani "A analysis of the KDD CUP 99 data set " in Proc. IEEE Symp. Computational Intelligence for Security and Defense Applications (CISDA) Ottawa, ON, Canada, 2009 pp. 1–6.
[5] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi "A deep learning approach to network intrusion detection " IEEE Trans. Emerging Topics in Computational Intelligence vol. 2, No. 1 Pp. 41–50, Feb. 2018.
[6] M. Ring, S. Wunderlich, D. Scheuring, D. Landes and A. Hotho "A survey of network-based intrusion detection data sets " Computers & Security vol. 86 Pp. 147–167, Sep. 2019.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, November 2026
Impact Factor: 8.2

[7] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita "Network anomaly detection: Methods, systems and tools " IEEE Communications Surveys & Tutorials vol. 16 No. 1 Pp. 303–336, 2014.
[8] R. Sommer and V. Paxson "Outside the world: On using machine learning for network intrusion detection " in Proc. IEEE Symp.. Privacy, Oakland, CA, USA, 2010 pp. 305–316.
[9] D. K. Molnar, Interpretable Machine Learning: A Guide for Making Black Box Models Explainable, ed. 2022.
[10] M. T. Ribeiro, S. Singh and C. Guestrin "'Why should I trust you?': Explaining the predictions of any classifier " in Proc. 22Nd ACM SIGKDD Int. Conf. Knowledge. Data Mining, San Francisco, CA, USA, 2016 pp. 1135–1144.
[11] S. M.. S.-i. Lee, "A unified approach to interpreting model predictions " in Advances in Neural Information Processing Systems (NeurIPS) vol. 30 2017.
[12] A. L. Buczak and E. Guven "A survey of data mining and machine learning methods for cyber security intrusion detection " IEEE Communications Surveys & Tutorials vol. 18 No. 2 Pp. 1153–1176 2016.
[13] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman "Survey of intrusion detection systems: Techniques, datasets and challenges " Cybersecurity vol. 2 No. 20 2019.
[14] M. Conti, A. Dehghantanha, K. Franke and S. Watson "Internet of Things security and forensics: Challenges and opportunities " Future Generation Computer Systems, vol. 78 Pp. 544–546, 2018.
[15] N. Moustafa and J. Slay "UNSW-NB15: A comprehensive data set for network intrusion detection systems " in Proc. Military Communications and Information Systems Conference (MilCIS) Canberra, ACT, Australia, 2015 pp. 1–6.
[16] I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani "Toward generating a new intrusion detection dataset and intrusion traffic characterization " in Proc. 4Th Int. Conf. Information Systems. Privacy (ICISSP) 2018 pp. 108–116.
[17] S. Garcia, M. Grill, J. Stiborek and A. Zunino "An comparison of botnet detection methods " Computers & Security vol. 45 Pp. 100–123, Sep. 2014.
[18] NIST, Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD, USA: National Institute of Standards and Technology 2024.
[19] ENISA, ENISA Threat Landscape 2024. European Union Agency, for Cybersecurity 2024.
[20] W. Stallings, Network Security Essentials: Applications and Standards ed. Hoboken, NJ, USA: Pearson, 2022.