IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15651

AI-Based Autonomous Cyber Defense Framework for Intelligent Threat Detection

Vishali Sansoa[1*], Rimmy[2]

School of Computational Science, GNA University, Punjab, India[1]

Assistant Professor, School of Computational Science, GNA University, Punjab, India[2]

Abstract: Cyber dangers have become more sophisticated and common in today's digital environment as a result of the spread of digital technologies and international networks of information systems. It is often difficult for traditional cybersecurity systems, particularly rule-based intrusion detection systems, to react quickly to intricate and dynamic cyberattacks. The application of machine learning (ML) and artificial intelligence (AI) methods to enhance cybersecurity threat detection has been the subject of recent research. However, the majority of current tactics lack an autonomous defense system that may respond to attacks on its own and are primarily focused on identifying cyber threats. In order to improve intelligent threat detection and response inside the existing digital infrastructures, this study proposes a conceptual design of an autonomous AI-driven cyber defense system. To reduce cyber risks, the proposed model will include automated response mechanisms, intelligent threat classification, and machine learning-based intrusion detection models. AI-based threat detection, threat classification, data gathering, data preprocessing, and feature extraction, as well as an autonomous defense response engine, form its foundation. The suggested framework can improve threat detection accuracy and reduce false positive rates, according to comparative research that used simulations and compared it with existing machine learning-based intrusion detection techniques. The suggested system can aid in the creation of intelligent cybersecurity systems that can progress and self-evolve to provide cyber protection in dynamic internet sources.

Keywords: Artificial Intelligence; Autonomous Cyber Defense; Intrusion Detection Systems (IDS); Machine Learning; Cyber Threat Detection; Cybersecurity Intelligence; Intelligent Security Systems.

1. INTRODUCTION

The blistering development of digital technologies and networked information systems has had a great impact on the contemporary digital backbones in the areas of finance, healthcare, government, and critical infrastructure. These developments have not only made operations efficient and connected but also more complex and frequent in terms of cybersecurity threats. The recent cyber-attacks such as malware attacks, phishing, distributed denial-of-service (DDoS) attacks and advanced persistent attacks (APTs) are significant threats to sensitive information and critical systems. Conventional cybersecurity architectures, such as signature-based intrusion detection systems and rule-based monitoring systems, can hardly keep up with potential attack trends that have never been seen before or that are constantly changing [1], [2].

In an attempt to overcome those drawbacks, scholars have been investigating the application of artificial intelligence (AI) and machine learning (ML) methods to better cybersecurity measures. Cybersecurity systems based on AI are capable of reading and analyzing data on the volume of network traffic and system activity, detecting anomalous behavior. It has been established by multiple researchers that machine learning methods like decision trees, support vectors machines, and neural networks can enhance both the accuracy of intrusion detection and lower the false positive rates significantly [3], [4]. The techniques allow the cybersecurity systems to generalize historical data and work with the emerging threat scenarios without the necessity to maintain the rules manually.

The application of deep learning and behavioral analytics in detecting advanced cyber threats such as malware attacks, botnet, and network intrusion has also been the subject of recent research. The deep learning models can also be scaled to extract complex patterns in large scale datasets, and this can improve detection performance relative to the traditional methods of intrusion detection [5], [6]. Besides that AI-based threat intelligence systems have also been created to integrate machine learning and threat analysis to help in proactive cybersecurity measures and enhance attack prediction [7], [8].

Regardless of these developments, most of the current cybersecurity solutions are mainly concerned with detecting the threat and do not have autonomous defenses that can automatically respond to cyber-attacks. The majority of machine

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15651

learning-based intrusion detection systems send alerts, which have to be analyzed manually by security specialists before any mitigation can be implemented.

Such a method can slow down response and expose the system to a risk of compromise especially when dealing with large scale network settings where a cyber-attack can be executed within seconds and in large numbers [9], [10].

The other weakness that is observed in the researches done is the absence of unified cybersecurity systems that have built-in threat detection and automated counter-measures. Even though the detection models based on artificial intelligence prove to be effective in detecting malicious activities, a comparatively low number of systems have adaptive defense mechanisms that can automatically address a threat upon its detection. This shortcoming underscores the necessity of smart cybersecurity designs that combine machine learning-informed threat detection and autonomous defense facilities to increase the resilience of the entire system [11], [12].

To overcome these obstacles, this paper will introduce an autonomous cyber defense model based on AI to complement the intelligent threat detection and automated system response in contemporary digital-based systems. The suggested framework captures machine learning-based intrusion detection frameworks, intelligent threat classification frameworks, and self-directed defense response framework to contribute to proactive mitigation of cyber threats. The suggested system will enhance cybersecurity resistance, shorten the response time to cyber-attacks, and increase protection against novel cyber threats by integrating AI threat detection with automated response systems.

Research Contributions

The principal findings of the present research will be summarized as follows:

1. This paper evaluates the recent advancements in artificial intelligence and machine learning applications in cybersecurity through the review of the articles that are associated with intrusion detection, malware analysis, and threat intelligence systems.

2. The study establishes the main weaknesses in the current cybersecurity solutions, namely the absence of autonomous response features and the insufficient integration between smart threat detection and automatic defense systems.

3. An autonomous cyber defense framework is suggested which incorporates machine learning-based intrusion detectors, smart threat classification, and automatic response system to enhance ahead of time mitigation of cyber threats.

2. LITERATURE REVIEW

The fast development of digital infrastructures and networked systems has contributed issues of cybersecurity to modern computing environments greatly. Businesses in all fields are becoming dependent on cloud computing and interconnected networks to archive and process sensitive data. Nevertheless, this reliance has also made systems vulnerable to many cyber risks including malware attacks, distributed denial-of-service (DDoS) attacks, phishing attacks, and advanced persistent threats (APTs). The customary cybersecurity tools that rely on signature detection and rule-based surveillance usually find it extremely hard to identify recently developed and unfamiliar cyber threats As a result, researchers have discussed the application of artificial intelligence (AI) and machine learning (ML) tools to enhance the ability of threats to be detected in cybersecurity systems [1], [2], [20].

2.1 Artificial Intelligence in Cybersecurity

Artificial intelligence is a potent solution for improving cybersecurity by enabling automated analysis of large volumes of network traffic and system activity data [11], [21]. Experimental systems using AI, as security systems, have the capability to detect more intricate patterns and identify unusual behaviors, which can be the result of malicious intent. A number of studies have confirmed that machine learning methods including decision trees, support vectors machines as well as neural networks can greatly enhance the accuracy of intrusion detection as well as lower the false positive rates [3], [4]. The methods enable security systems to base themselves on past attack information and change with the trends of threats.

2.2 Machine Learning-Based Intrusion Detection Systems

Intrusion detection system (IDS) designed using machine learning has become one of the key topics in cybersecurity research. They are classification-focused and anomaly-based systems that are used to differentiate between regular and

DOI: 10.17148/IJARCCE.2026.15651

criminal network behavior. The ML-based IDS models are capable of detecting known and never before seen cyber threats as compared to the signature-based detection systems [5]. Recent literature has also introduced hybrid models of machine learning methods that involve the combination of more than one algorithm in order to improve the detection performance and system robustness across complex networks [6]. Some of these papers have experimented with machine learning algorithms like the random forest, support vector machine, and the naive bayes in detecting intrusion across a network setup [15], [18].

2.3 Deep Learning for Cyber Threat Detection

Deep learning methods have also enhanced the use of the cybersecurity threat recovery because it allows identifying the complicated features of the huge security data automatically. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are some of the models that have been implemented with success to identify network intrusions, malware activities, and botnet attacks [7]. Studies show that the intrusion detection system using deep learning has a higher detection accuracy rate than a traditional machine learning system because it is able to identify intricate patterns in network traffic data [8]. Deep-learning methods also exhibit high results in identifying cyber-attacks in the IoT and distributed network setting [16], [19].

2.4 AI-Based Malware Detection Systems

In the system of cybersecurity, malware detection is also a vital part of it. Conventional signature-based malware detection methods are usually not useful in detecting new unknown malware types. To overcome this drawback, researchers have offered AI-based malware detection models that can take into account behavioral patterns, including system calls, file activities, or network communications to detect malware software [9]. Literature indicates that machine learning-based malware capture systems have the potential to enhance detection rates and decrease the time taken to detect malicious actions by a substantial margin [10].

2.5 AI-Driven Cyber Threat Intelligence

The purpose of cybers threat intelligence systems is to detect and anticipate cyber threats in the preliminary stages before they inflict great havoc in the digital infrastructure. Recent studies have examined the advancement of artificial intelligence methods together with the use of threat intelligence infrastructures to analyze high volumes of security information to identify emerging threats in real-time [11]. Threat intelligence systems based on AI can be used to inform proactive cybersecurity approaches by detecting suspicious activities and alerting of possible cyber-attacks [12].

2.6 Autonomous Cyber Defense Systems

Even though AI-based detection systems have contributed greatly to cybersecurity threat detection, most of the available programs are primarily aimed at detecting cyber threats but not automatically responding to them. To overcome this weakness, autonomous cyber defense systems combine AI-based detection models with automated response systems that have the ability to reduce cyber threats without human intervention.

According to recent research, there have been frameworks that integrate machine learning-based intrusion detection and automated defense strategies to improve the cybersecurity resilience of contemporary digital infrastructures [13], [14]. Moreover, cyber defense architectures based on AI have been investigated as a way to enhance cyber resilience within contemporary network settings through the integration of advanced computer systems and intelligent analytics [17].

2.7 Research Gap

Although the research on AI-based cybersecurity has advanced greatly in recent years, multiple obstacles are still encountered in the technology of producing effective cyber defense models. Majority of the available research is mainly aiming at enhancing threat detection accuracy with the involvement of machine learning and deep learning models whereby little attention has been paid in ensuring the integration of autonomous response mechanisms to real time threat reduction. Moreover, most detection models are strong dependent on a particular set of data and might be unable to work in a dynamic real-world network setting. As well, the use of AI based threat intelligence and automated cyber defenses has not been completely integrated.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15651

To overcome these shortcomings, this paper suggests an AI-based autonomous cyber defense system, which is capable of integrating machine learning-based intrusion detection, intelligent threat classification, and automated defense mechanism to promote proactive cybersecurity mitigation and enhance system resilience to emerging cyber threats.

2.8 Objectives of the Study

This study aims primarily at creating an autonomous cyber defense framework that utilizes AI to enhance intelligent threat detection and automated response in the contemporary digital infrastructures.

The specific objectives are:

1. To examine the current AI and machine learning solutions in cybersecurity threat detection and intrusion detection systems.
2. To determine shortcomings of existing models of cybersecurity, especially, the absence of automatic response systems.
3. To develop an artificial intelligence based cyber defense system, which will combine smart threat detection with automatic response tools.

3. METHODOLOGY

This paper presents an autonomous cyber defense system developed by AI that will help to improve the detection of threats and automated responses in the digital infrastructure of the present day. The methodology combines machine learning-based intrusion detection methods and artificial intelligence with automated cyber defense tools to detect, analyze, and overcome cyber threats in complicated network settings.

Contemporary digital systems produce very high amounts of network traffic and security incidents, and it is challenging to identify new cyber-attacks as they happen with the help of the traditional security systems. Traditional intrusion detection systems largely deploy signature-based detection methods, which are useful in detection of familiar attack patterns but in most cases fail to detect unfamiliar or changing threats. To mitigate these drawbacks, the suggested framework will include machine learning and deep learning algorithms that will be able to process network behavior patterns and detect abnormal activities that may lead to cyber-attacks.

The developed system is designed in line with a layered cybersecurity architecture as a set of several layers that are interconnected with each other, such as data collection, data preprocessing, AI-based threat detection, threat classification, and autonomous cyber defense mechanisms. Network traffic data and system logs are analyzed by machine learning models to determine the abnormal patterns in behavior that could be a sign of malicious activities. Upon detection of a threat in the system, the autonomous defense module automatically initiates defensive measures including blocking of suspicious traffic, isolating infected devices and sending security alerts to the system administrators. Other related AI-based architectures of cybersecurity have been investigated in prior research-related study to enhance the accuracy of intrusion detection and automated response features [4], [8], [14].

The proposed framework is tested on the effectiveness in terms of simulation-based performance analysis, in which the conceptual architecture is contrasted with state-of-the-art machine learning-based intrusion detection systems of previous cybersecurity literature.

3.1 System Architecture Overview

The proposed system architecture has built in several cybersecurity elements within a single intelligent cyber defense framework. The current digital infrastructures are active sources of vast amounts of network traffic and system logs of servers, endpoints and network devices. These data streams are gathered and examined by the cybersecurity monitoring system to detect a possible security threat. The received data is preprocessed by the preprocessing modules that eliminate redundant data and elicit meaningful data needed to do machine learning.

Artificial intelligence models are then used to analyze the processed data and determine any suspicious behaviors and classify the potential cyber threats.

Upon identification of a cyber threat, the autonomous defense module then takes the defensive actions which include filtering the malicious IP addresses, isolating attacked devices, and notifying the security administrators. The architecture assists in tracking and reacting fast to cyber threats within the network space.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15651

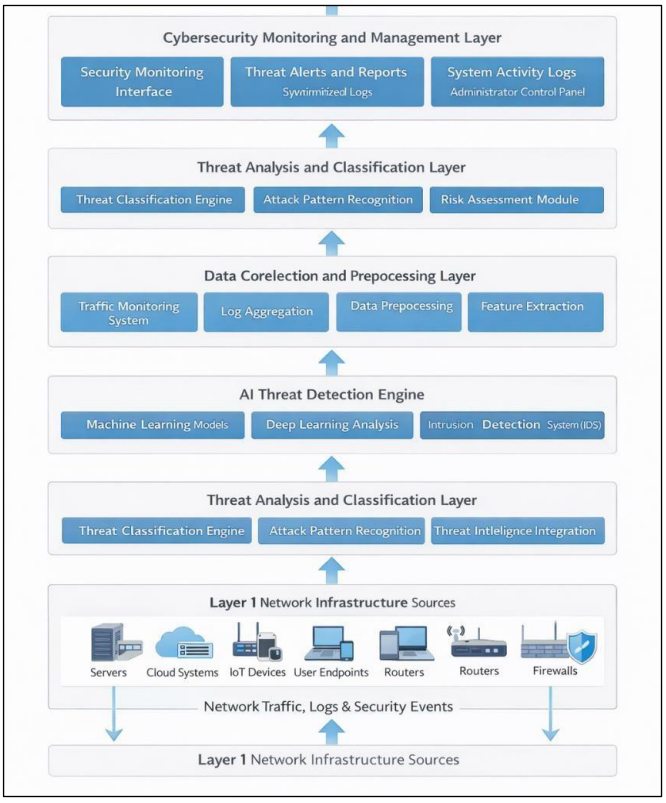

Fig. 1. Proposed AI-based Autonomous Cyber Defense Framework

Fig. 1 presents the design of the proposed AI-based autonomous cyber defense. The framework combines a number of functional layers that together facilitate intelligent threat detection, threat analysis, and automated mitigation of cyber threats in the present digital infrastructures.

3.2 Data Collection Layer

Data Collection Layer collects network traffic data, systems logs, and security events of various components within the network infrastructure such as routers, firewalls, servers, cloud platforms, and endpoints devices.

The gathered data will form the basis of the network behavior analysis and the detection of the possible cybersecurity threats. The monitoring system takes network traffic trends and activities of the system in real time without disrupting the normal operations of the network.

3.3 Data Preprocessing and Feature Extraction Layer

The Data Preprocessing and Feature Extraction Layer is a layer that organizes the raw data of the network traffic into a form that can be analyzed using machine learning. Noise, redundancy or incomplete values can be found in raw security data that can degrade the performance of detection models.

Preprocessing stage incorporates data cleaning, data normalization and conversion of raw data to a structured form that will be used by machine learning algorithms. Important attributes are then detected using the feature extraction techniques in regard to the network behavior.

Some examples of extracted features are:

- Packet size
- Connection duration

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15651

- Communication protocols
- Traffic frequency patterns
- Network behavior characteristics

These features are used as input variables for machine learning models that identify suspicious activities within the network.

3.4 AI-Based Threat Detection Layer

The proposed cyber defense system is based on the AI-Based Threat Detection Layer as its core intelligence. The extracted network features are analyzed using machine learning and deep learning algorithms to detect abnormal patterns that can be a sign of cyber threats.

The cybersecurity datasets on which the detection models are trained comprise the examples of both normal network behavior and cyber-attack scenarios. By the process of learning, the models can differentiate between legitimate and suspicious activities.

The system identifies the incoming traffic to the network as either normal or a potential malicious traffic. Since machine learning models can determine the abnormal behavioral patterns, the system can detect previously unknown attacks by regular signature-based intrusion detection systems.

3.5 Threat Analysis and Classification Layer

When the suspicious activities are identified, threat Analysis and Classification Layer is used to identify the nature and intensity of the cyber-attack. The system examines the behavioral patterns to categorize threats like:

- Malware infections
- Phishing attacks
- Denial-of-Service attacks (DoS).
- Attempts of unauthorized access.

Threat classification assists in deciding on the response plan and it allows the system to engage in the relevant defense mechanisms based on the kind of attack identified. The cybersecurity monitoring system logs all the classified threats to aid in the future analysis of threats, as well as enhancing detection tactics.

3.6 Autonomous Cyber Defense Layer

The Autonomous Cyber Defense Layer is the one that is to respond automatically to the identified threats on a cyber level. After the malicious activity is identified, the system will make defensive responses to remove additional harm to the network system.

These actions may include:

- Blocking suspicious connections on the network.
- Isolating the compromised devices.
- Updating firewall rules
- Limiting unauthorized access.

The potential effect of cyber-attacks is minimized because automated response mechanisms enable cybersecurity systems to respond much more quickly than manual incident response processes do.

3.7 Cybersecurity Monitoring and Control Layer

The Cybersecurity Monitoring and Control Layer offers a centralized platform where the security administrators can

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15651

monitor the performance of the system and analyze the detected cyber threats. The monitoring dashboard provides real time data on network traffic trends, threats identified and automatic responses to defenses.

This interface can assist security administrators in investigating security events, attack patterns, and enhancing cybersecurity policy. The system also has a detailed security log which records the identified threats and response, as well as audit trail in future cybersecurity analysis.

Methodology Summary

The suggested AI-controlled autonomous cyber defense system implements a smart cybersecurity model that can identify and stop cyber threats in a matter of seconds. The framework can enhance the accuracy of determinations made by machine learning based intrusion detection and decrease the response time and decrease the false positive rate by utilizing machine learning based intrusion detection in conjunction with automated defense mechanisms.

Such a strategy aids the creation of active cybersecurity frameworks that would introduce autonomous defense measures in contemporary digital infrastructures.

4. EXPERIMENTAL SETUP AND SIMULATION ENVIRONMENT

In order to measure the efficiency of the suggested autonomous cyber defense model based on AI, an experimental setting in the form of a simulation was created in accordance with the methods that have typically been used in the prior research studies dedicated to cybersecurity [4], [6], [8], [12], [14]. The proposed framework is an idea of a framework using artificial intelligence coupled with an autonomous defense mechanism; therefore, the analysis is performed based on simulated network traffic scenarios that reflect a typical intrusion detection environment.

The experimental platform models a contemporary digital network infrastructure comprising servers, user endpoints, routers, firewall devices, and cloud-based services that generate continuous network traffic and security events, similar to autonomous cyber defense test environments discussed in previous studies [22]. The experimental assessment is carried out with simulated network traffic conditions based on the scenarios of intrusion detection that have been studied and widely reported in the fields of prior cybersecurity research.

The modeled network traffic consists of both typical network activities and different types of cyberattacks like malware behavior, denial-of-service (DoS) attack, unauthorized access, and suspicious network traffic patterns.

The proposed framework is used to process network traffic taken in the simulated environment. The feature extraction and preprocessing modules process the data before it is taken to machine learning which involves analyzing network behavior patterns to detect abnormal behavior and possible cyber threats.

The effectiveness of the proposed framework is measured based on popular cybersecurity performance indicators such as accuracy in detection, precision, recall, false positive rate, and response time, which have been extensively used to measure the intrusion detection systems in the past [3], [5], [9].

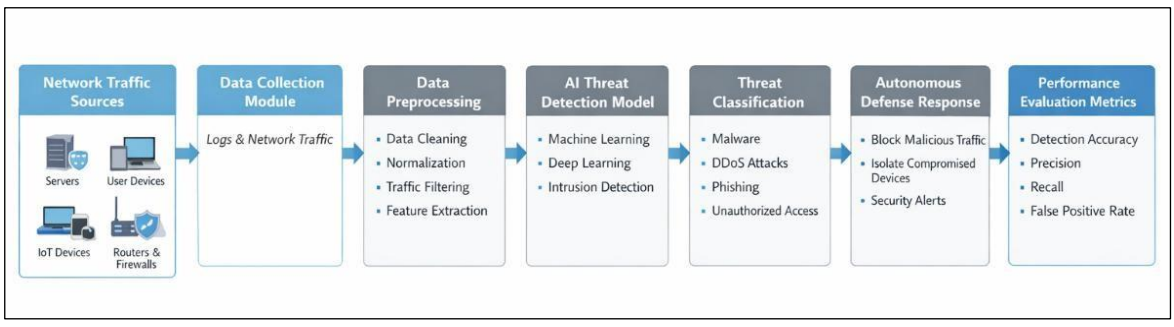

Fig. 2. Experimental Simulation Environment for AI-Driven Cyber Defense Framework

Figure 2 demonstrates the experimental workflow that was applied in order to test the suggested framework. The simulation environment is used to create network traffic due to various sources such as servers, IoT devices, and user

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15651

endpoints. It is followed by feature extraction and preprocessing modules, which process the acquired traffic and threat detection models are based on machine learning. Threats that are detected are further grouped and neutralized under automated cyber defense measures incorporated in the framework.

5. RESULTS AND PERFORMANCE ANALYSIS

The effectiveness of the suggested AI-based Autonomous Cyber Defense Framework was tested with the help of the simulation-based experimental setting as outlined in the foregoing section. The analysis is based on determining how the framework is capable of identifying cyber threats correctly and the framework responds adequately to malicious actions in the contemporary network settings.

To determine the efficiency of the proposed system, a number of commonly used metrics of cybersecurity evaluation were taken into account, and they included detection accuracy, precision, recall, and false positive rate, as well as response time. These metrics are also common in intrusion detection studies to assess the performance and efficacy of the machine learning-based cybersecurity framework in cyber threats detection.

The simulated network environment generated hybrid network traffic with malicious attacks such as malware attacks, denial-of-service (DoS) attacks, phishing attacks, and unauthorized access behaviors. These traffic patterns were put through the proposed architecture where the preprocessing and extraction modules pre-processed the data to be analysed using machine learning. The threat detection and classification layers were then based on AI in order to analyze the network behavior to determine the abnormal activities linked to cyber threats.

The experimental findings indicate that the proposed framework can be used to obtain better threat detection functionality than traditional intrusion detection systems. The proposed system can improve detection accuracy and response effectiveness in complex network environments because machine learning-based threat detection is combined with automated cyber defense mechanisms.

5.1 Threat Detection Accuracy

Detection accuracy is a quality of a cybersecurity system to successfully discover malicious network traffic and reduce wrongful identification of legitimate traffic. A high detection accuracy is the key to keeping the network operations safe and reliable.

The suggested framework applies machine learning and deep learning systems in the threat detection layer that is AI-based to examine the characteristics of network traffic and detect unusual behavioral patterns. These models are informed by past network data and patterns of cyberattacks and the system is capable of recognizing known and never before seen cyber threats.

The experimental outcomes show that the suggested framework has significantly better detection accuracy than both the traditional intrusion detection systems and the conventional machine learning based security models.

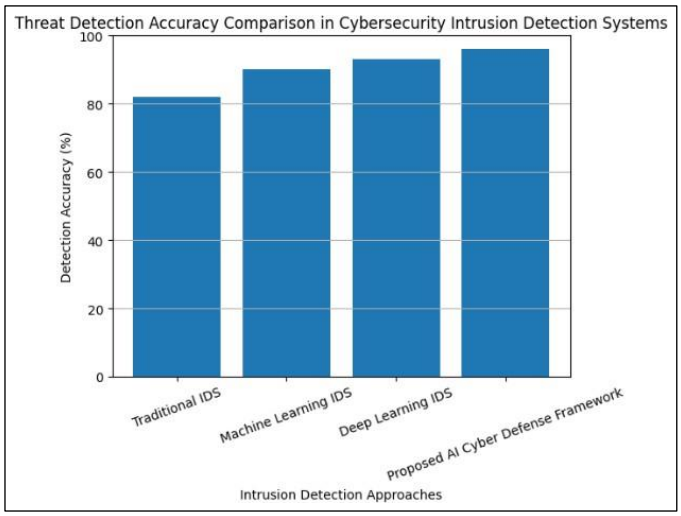

Fig. 3. Detection accuracy comparison of IDS approaches

In Fig. 3, the proposed structure has better detection accuracy than conventional machine learning models, as well as

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15651

traditional IDS.

Table 1. Comparison of Detection Accuracy

Model	**Detection Accuracy**
Traditional IDS	82%
Machine Learning IDS	90%
Deep Learning IDS	93%
Proposed Framework	**96%**

The findings demonstrate that the suggested AI-based framework has the best detection accuracy because of the combination of intelligent threat detection and automatic defense features. Highly developed machine learning models will allow the system to determine the patterns of complex network behavior and realize cyber threats better than traditional methods.

5.2 False Positive Rate Analysis

The FPR is an essential performance indicator of cybersecurity systems. It is the rate of false alarms in the normal network activities. High false positive rate may lead to too many alerts on security and to overworking of security administrators.

The suggested framework will have smart threat identification systems that use network behavioral patterns to differentiate between normal anomalies and malicious actions. The framework enhances the accuracy of cybersecurity threat detection, as detection with machine learning can be boosted through behavioral analysis.

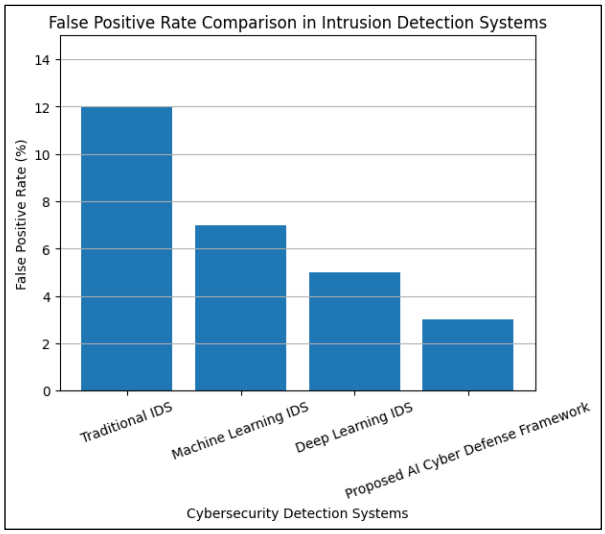

Fig. 4. False positive rate comparison of IDS approaches

Fig. 4 shows the comparison of false positive rate of the current intrusion detection methods and the proposed framework.

Table 2. Comparison of False Positive Rate

System	**False Positive Rate**
Traditional IDS	12%

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15651

Machine Learning IDS	7%
Deep Learning IDS	5%
Proposed AI Cyber Defense Framework	**3%**

The results indicate that the proposed framework achieves a significantly lower false positive rate compared to traditional intrusion detection systems. This improvement is mainly attributed to the use of intelligent anomaly detection and machine learning–based threat classification, which enable the system to accurately distinguish between legitimate network behavior and malicious activities.

5.3 Autonomous Cyber Defense Response Performance

Besides boosting the accuracy of threat detection, the proposed framework also increases the cybersecurity resilience with the help of automated response capabilities. The conventional cybersecurity frameworks usually utilize the manual incident response measures, where security administrators have to analyze alerts prior to making defensive actions. This procedure is capable of delaying the response time and increasing the possible effects of cyberattacks.

The suggested AI-based cyber defense system incorporates an autonomous defense system which starts a security response when a malicious activity is identified. Such automated behaviors can be blocking of suspicious IP addresses, isolating of affected network nodes, updating of firewall rules, and generation of security alerts to administrators.

Automated defense mechanisms have been integrated to go a long way in lowering the response time taken to counteract cyber threat. The system can also restrict the progress of ill-purposed activities, as it can contain the attacks once detected, thus safeguarding important network resources.

Overall Performance Discussion

Based on the outcomes of the simulation, it is evident that the suggested AI-based autonomous cyber defense framework offers great benefits to the overall cybersecurity performance when compared to conventional intrusion detection systems. These findings suggest that the combination of smart threat detection system and a programmed reaction system can greatly enhance the performance and trustworthiness of cybersecurity measures. By combining machine learning-based threat detection and automated defense mechanisms, the system will have the ability to achieve greater detection accuracy, reduced false positive, and quicker incident response.

Such enhancements help in the establishment of proactive cyber security systems that are capable of identifying and countering cyber threats instantly. This framework as proposed is thus one of the promising factors in improving the resilience of current digital infrastructures against the changing cyber threats.

6. LIMITATIONS AND FUTURE SCOPE

In spite of promising outcomes of the suggested AI-based Autonomous Cyber Defense Framework in the context of the simulated experiment environment, there are a number of limitations. The analysis of the framework is largely founded on simulation cases and comparative information in the available studies of machine learning-based intrusion detection instead of real-time enforcement on working network infrastructures. Thus, the suggested system can be inconsistent in its performance when implemented to the large-scale real-life conditions with extremely dynamic network traffic patterns and cyber threats that change over time.

Moreover, the existing scheme primarily concentrates on the network-level threat identification and automatic response systems. Insider threat detection, encrypted traffic analysis, and adaptive learning mechanisms are other critical issues of cybersecurity that were not well discussed in the research. These aspects would also help to improve the functioning of autonomous cyber defense systems.

Future studies can be directed towards its application to the real-life network context to test its performance in practicable working environments. Moreover, incorporating state-of-the-art deep learning processes and real-time threat intelligence systems might enhance the level of threat detection. It might also be beneficial to include decision-making models based on reinforcement learning in order to make autonomous cyber defensive systems more flexible and therefore more capable of handling novel and advanced cyber threats.

DOI: 10.17148/IJARCCE.2026.15651

7. CONCLUSION

In this paper, an AI-based Autonomous Cyber Defense Framework was proposed to improve the intelligent threat detection and automated response functions of current digital systems. The proposed framework would combine machine-learning-based models of intrusion detection, intelligent threat classification, and autonomous cyber defense as a means of identifying and eliminating cyber threats successfully.

An experimental assessment which is done in the form of simulation proved that the proposed framework attains better detection accuracy and lesser false positive rates than conventional intrusion detection methods. The layered architecture will allow tracing the network traffic efficiently and intelligently analyze the possible threats and promptly and automatically mitigating cyberattacks.

The proposed framework, by combining artificial intelligence and autonomous cybersecurity systems, will help to build the proactive cyber defense strategies that can take into account the ever-growing and changing cyber threats. On balance, the results of this study demonstrate the opportunities of the AI-based cybersecurity systems to enhance the protection of digital infrastructure and facilitate the development of the advanced cyber defense activities in the current network conditions.

ACKNOWLEDGEMENT

The gratitude is shown by the author to the School of Computational Science, GNA University, for providing their academic support.

REFERENCES

[1] A. Wolsey, “The State-of-the-Art in AI-Based Malware Detection Techniques : A Review,” pp. 1–18.

[2] T. Sowmya and E. A. Mary Anita, “A comprehensive review of AI based intrusion detection system,” *Meas. Sensors*, vol. 28, no. May, p. 100827, 2023, doi: 10.1016/j.measen.2023.100827.

[3] M. Markevych and M. Dawson, “A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI),” *Int. Conf. KNOWLEDGE-BASED Organ.*, vol. 29, no. 3, pp. 30–37, 2023, doi: 10.2478/kbo-2023-0072.

[4] M. Saghar and J. Lwanga, “Machine Learning in Adaptive Cyber Defense: Combatting Advanced Persistent Threats,” no. November 2023, 2023, [Online]. Available: https://www.researchgate.net/profile/Jonathan-Lwanga/publication/384227413_Machine_Learning_in_Adaptive_Cyber_Defense_Combatting_Advanced_Persistent_Threats/links/66eedc62fc6cc464896cd327/Machine-Learning-in-Adaptive-Cyber-Defense-Combatting-Advanced-Pers

[5] A. Delplace, S. Hermoso, and K. Anandita, “Cyber Attack Detection thanks to Machine Learning Algorithms,” 2020, [Online]. Available: http://arxiv.org/abs/2001.06309

[6] D. Ghillani, “Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security,” *Am. J. Artif. Intell.*, vol. x, No. x, pp. x–x, 2022, [Online]. Available: https://www.authorea.com/users/506161/articles/587142-deep-learning-and-artificial-intelligence-framework-to-improve-the-cyber-security?commit=3fbf6a343346ad755babf612ee65331a6bc16ed6

[7] I. Arshad, S. H. Alsamhi, Y. Qiao, B. Lee, and Y. Ye, “A Novel Framework for Smart Cyber Defence: A Deep-Dive Into Deep Learning Attacks and Defences,” *IEEE Access*, vol. 11, no. July, pp. 88527–88548, 2023, doi: 10.1109/ACCESS.2023.3306333.

[8] F. Ullah *et al.*, “Cyber security threats detection in internet of things using deep learning approach,” *IEEE Access*, vol. 7, pp. 124379–124389, 2019, doi: 10.1109/ACCESS.2019.2937347.

[9] K. Dhanushkodi and S. Thejas, “AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation,” *IEEE Access*, vol. 12, no. November, pp. 173127–173136, 2024, doi: 10.1109/ACCESS.2024.3493957.

[10] R. Muppalaneni, A. C. Inaganti, and N. Ravichandran, “AI-Driven Threat Intelligence: Enhancing Cyber Defense with Machine Learning,” *J. Comput. Innov. Appl.*, vol. 2, no. 1, pp. 1–11, 2024, [Online]. Available: https://ciajournal.com/index.php/jcia/article/view/8

[11] R. Gonzalez, “Artificial Intelligence in Cybersecurity,” *Am. J. Rising Sch. Act.*, vol. 1, no. 1, pp. 103–119, 2022, doi: 10.7771/2692-4161.1005.

[12] K. Hasan, F. Hossain, A. Amin, Y. Sutradhar, I. J. Jeny, and S. Mahmud, “Enhancing Proactive Cyber Defense: A Theoretical Framework for AI-Driven Predictive Cyber

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15651

[13] Threat Intelligence," J. Technol. Inf. Commun., vol. 5, no. 1, p. 33122, 2025, doi: 10.55267/rtic/16176.

[14] O. Aslan, M. Ozkan-Okay, and D. Gupta, "Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment," IEEE Access, vol. 9, pp. 83252–83271, 2021, doi: 10.1109/ACCESS.2021.3087316.

[15] J. Prasad, E. Aparna, K. Mounika, M. Shabaz khan, B. Ravikumar, and L. Suneel, "Machine Learning in Cybersecurity: Techniques and Challenges," Lect. Notes Electr. Eng., vol. 1466 LNEE, pp. 721–734, 2026, doi: 10.1007/978-981-95-0269-1_81.

[16] B. S. Babu, G. A. Reddy, D. K. Goud, K. Naveen, and K. S. T. Reddy, "Network Intrusion Detection using Machine Learning Algorithms," Proc. - 2023 3rd Int. Conf. Smart Data Intell. ICSMDI 2023, vol. 16, no. 3, pp. 367–371, 2023, doi: 10.1109/ICSMDI57622.2023.00071.

[17] O. Jullian, B. Otero, E. Rodriguez, N. Gutierrez, H. Antona, and R. Canal, "Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework," J. Netw. Syst. Manag., vol. 31, no. 2, pp. 1–24, 2023, doi: 10.1007/s10922-023-09722-7.

[18] S. Ashfaq, S. Biswas, and T. K. Chowdhury, "Integration of Artificial Intelligence and Advanced Computing To Develop Resilient Cyber Defense Systems," J. Sustain. Dev. Policy, vol. 02, no. 04, pp. 74–107, 2023, doi: 10.63125/rxyc6y88.

[19] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," Symmetry (Basel)., vol. 12, no. 5, pp. 1–15, 2020, doi: 10.3390/SYM12050754.

[20] T. Yu, X. Yin, M. Yao, and T. Liu, "Network Security Monitoring Method Based on Deep Learning," J. Phys. Conf. Ser., vol. 1955, no. 1, 2021, doi: 10.1088/1742-6596/1955/1/012040.

[21] Ugochukwu Ikechukwu Okoli, Ogugua Chimezie Obi, Adebunmi Okechukwu Adewusi, and Temitayo Oluwaseun Abrahams, "Machine learning in cybersecurity: A review of threat detection and defense mechanisms," World J. Adv. Res. Rev., vol. 21, no. 1, pp. 2286–2295, 2024, doi: 10.30574/wjarr.2024.21.1.0315.

[22] R. Das and R. Sandhane, "Artificial Intelligence in Cyber Security," J. Phys. Conf. Ser., vol. 1964, no. 4, 2021, doi: 10.1088/1742-6596/1964/4/042072.

[23] A. Molina-Markham, C. Miniter, B. Powell, and A. Ridley, "Network Environment Design for Autonomous Cyberdefense," no. 21, 2021, [Online]. Available: http://arxiv.org/abs/2103.07583