International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

Enhancing Security With AI- Based Intrusion Detection System in Computer Networks

Harini Sri B[1], Hemaraj S[2], Chandru S[3], Jaidi Avinash[4], Dr. R. Yogesh Rajkumar[5]
[1,2,3,4,5]*Department of Information Technology, Bharath Institute of Higher Education and Research*

***Abstract*—The fast evolution of computer networks and internet-based applications have added risk to cyber attack and unauthorized access. Traditional Intrusion Detection Systems (IDS) that are signature-based and rule-based are not typically effective in detecting new and advanced attack. The study will focus on the development of the network security with regards to intrusion detection systems based on artificial intelligence (AI). It uses AI technologies, like machine learning and neural networks, to process network traffic, identify patterns, and detect anomalies in a real-time manner. The proposed system implies the application of data pre-processing, feature selection, and different AI models (Decision Tree, Random Forest, and Neural Networks) to improve the accuracy of detecting and reduce the false alarms. Performance analysis shows that AI-based IDS have a high level of accuracy, flexibility and efficiency in comparison with traditional approach. The article singles out the possibilities of AI in creating smart and resilient cybersecurity solutions towards contemporary network settings.**

***Keywords*— Artificial Intelligence, Intrusion Detection System, Network Security, Machine Learning, Cybersecurity.**

I. INTRODUCTION

In the present digital age, computer networks are significant in communication and data exchange as well as operation of many industries like banking, health, education and e-commerce. As the use and interconnection of the internet has increased by leaps and bounds, it has become a major concern to ensure that computer networks are secure . Computer network is a term used to describe all the policies, practices and technologies meant to secure network infrastructure, devices and data against unauthorized access, abuse or cyberattacks. It is meant to guarantee information confidentiality, integrity and availability in a network.

Intrusion Detection System (IDS) is one of the most important elements of network security. An IDS is a security system that checks the network traffic or system actions to detect suspicious activity or possible security vulnerability. It can be used as a surveillance mechanism that identifies unauthorized access, malicious activities or policy violations . There are two broad categories of IDS: Network-based IDS (NIDS), which uses network traffic as a monitor, and Host-based IDS (HIDS), which uses activities on individual devices as a monitor.

The conventional systems of intrusion detection are mainly signature-based and rule-based methods. Signature-based IDS identifies attacks by comparing network traffic with a list of known attack patterns or signature. Although this method is good in detecting known threats, it does not detect new or unknown attacks otherwise known as zero-day attacks. Conversely, anomaly-based IDS identify the deviations of the normal patterns of behavior. Even though they are able to detect unknown threats, they tend to produce large false positive rates and thus are inefficient in real world applications.

Additionally, the traditional IDS systems have some limitations such as failure to keep up with the changing patterns of attacks, overreliance on inherent rules and lack of ability to scale and process vast amounts of network data . More sophisticated and dynamic security solutions are required as cyber threats, such as advanced persistent threats (APTs), malware and distributed denial-of-service (DDoS) attacks, become increasingly sophisticated.

Artificial Intelligence (AI) has become a potent means to overcome these shortcomings. Machine learning and deep learning are the foundation of intrusion detection systems based on AI that is applied to analyze large volumes of network traffic and identify patterns and detect anomalies in real-time. In contrast to conventional approaches , AI-based IDS are capable of learning, evolving to unknown threats, and enhancing detection accuracy as they learn. Such systems are able to detect known attacks and unknown attack with more precision and at a lower false alarm rate.

Integrating AI into intrusion detection systems has a number of benefits, such as “automated threat detection, enhanced scalability, enhanced accuracy, and the ability to respond in real-time . Decision trees, support vectors machines, neural networks, and deep learning architectures are some of the AI models that can be used to classify network traffic and detect malicious actions.

The primary goals of the research are to examine the application of artificial intelligence to improve intrusion detection systems, review various AI-based models in network security, and determine the benefits and limitations of their application. Another goal of the paper is to give some insights into how to make IDS more efficient and reliable with the help of advanced AI methods.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

II. Literature Review

2.1 Traditional Intrusion Detection Systems

The conventional intrusion detection systems are systems that have been in use over the years to ensure the safety of computer networks. These systems can largely be divided into signature based IDS and anomaly based IDS .

Signature based IDS are based on the predefined patterns or signature of known attacks. These signatures are put in a database and traffic in a network is compared to these signatures to identify any malicious activities occurring. This methodology is very precise in detecting threats that are known and produces fewer false positives.

Nevertheless, its biggest weakness is that it cannot identify new or unknown attacks since it is purely reliant on the previously determined attack patterns. Also, the signature database is costly to maintain and update and must be monitored at all times.

On the contrary, anomaly-based IDS identify intrusions by detecting abnormalities of the normal network behavior. Such systems create a benchmark of normality and indicate any abnormal patterns as threats . Zero-day attacks and new threats can be detected by anomaly-based systems, which are more adaptable than signature-based systems. Numerously, however, they have high false positive rates because normal fluctuations in network behavior can be falsely identified as malicious activities. This may result in unnecessary notifications and the security administrators working harder.

Each method has its merits and demerits, which are not sufficient to address the growing dynamism of the cyber threats in the current world. This has led researchers to think of more sophisticated ways of enhancing intrusion detection techniques, such as artificial intelligence.

2.2 AI in Cybersecurity

AI has had a significant influence in the cybersecurity sector in terms of offering intelligent and reactive security solutions. In intrusion detection systems, AI methods, especially machine learning and deep learning are popular in enhancing detection accuracy and efficiency.

Machine learning (ML) enables systems to acquire knowledge out of data and to make decisions without being explicitly programmed. The intrusion detection involves the use of ML algorithms to analyze network traffic data and identify patterns that are associated with normal and malicious actions. The common or used ML techniques that are used in IDS are decision trees, random forests, support vector machines (SVM) and K-nearest neighbors (KNN) techniques. The models used in protecting the network traffic can also be used to classify traffic and detect anomalies with high accuracy .

Deep learning (DL) is a subdivision of machine learning and is a process that entails the use of multi-layered neural networks to process complex data. The two deep learning models that are most successful at high scale network data and identifying high level attack patterns are convolutional neural networks (CNN) and recurrent neural networks (RNN). Such models have the capability of deriving features automatically on raw data, eliminating the manual feature engineering.

AI-driven IDS have a number of benefits as compared to conventional techniques. They are capable of processing vast amounts of data, changing with threats, and offer real-time detection. Moreover, AI models have the ability to continuously improve their performance by learning new information, and are thus highly suitable in dynamical network settings .

Nevertheless, AI application in cybersecurity also has its issues, including the requirement of large-scale data, a high level of complexity, and possible bias in the training data. Nonetheless, AI has a chance to become an effective network security improvement strategy even under such conditions.

2.3 Existing AI-Based IDS Models

A number of studies have researched on the use of AI methods in intrusion detection systems. Such studies have proven machine learning and deep learning models to be effective in identifying cyber threats.

The KDD Cup 1999 dataset is one of the most commonly utilized data sets in the study of IDS and it comprises a substantial amount of network traffic data that has been labeled as either normal or malicious. Nevertheless, this data is limited by factors, including redundancy and obsolete attack patterns. In order to overcome these problems, a better variant of the NSL-KDD dataset was offered, which provides a better balanced and more realistic dataset to test the IDS models.

Based on these datasets, researchers have created different AI-based IDS models . As an example, decision tree and random forest models have been employed to obtain high accuracy in classification at a comparatively low cost in terms of computation.

It is also due to the high-dimensionality of data that support vectors machines have become very popular. CNN and RNN are the deep learning models that gained popularity over recent years because of their ability to identify advanced and dynamic patterns of attacks.

Numerous investigations have shown that AI-based IDS have better performance than conventional techniques. Such systems prove to have better detection rates, false positives and flexibility to emerging threats. Nevertheless, research gaps are still numerous and need to be filled.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

One of the challenges is that it is not implemented in practice yet, in real-time, with the help of AI-based IDS. Offline analysis is studied by most studies through benchmark datasets, which might not be representative of real network conditions. Moreover, one needs large labelled datasets and this can be a challenge because they can be cumbersome and time consuming.

The other gap in research is the interpretability of models of AI. The majority of deep learning models are black boxes and there is little information on how they arrive at decisions . This is a weakness of its transparency, which can restrict its application to essential security applications.

Moreover, it is also necessary to create light and powerful AI models that can be used in resource-limited contexts, including IoT networks. To improve the feasibility and usefulness of AI-based intrusion detection systems, future studies should aim to tackle these issues.

III. Methodology

The research methodology in this paper is aimed at developing and testing an Intrusion Detection System (IDS) based on Artificial Intelligence (AI) to improve network security. The suggested system has a systematic process that involves the collection of data, preprocessing, feature selection, model training, and evaluation.

3.1 Data Collection

The initial one is to gather network traffic data comprising of both normal and malicious traffic. The datasets that are publicly available like KDD Cup 1999 and NSL-KDD have been widely used because of their extensive coverage of network traffic patterns. These datasets encompass different forms of cyberattacks including denial-of-service (DoS), probing, user-to-root (U2R) and remote-to-local (R2L) attacks. The data sets are composed of various attributes such as protocol type, service, flag, source bytes and destination bytes, which are critical in detecting abnormalities in the network behavior.

3.2 Preprocessing Techniques

Raw network data is usually filled with noise, missing values and redundant data, which adversely impacts the performance of AI models. Thus, a preprocessing is an important step. It includes the cleaning, normalization and transformation of data. Imputation is used to fill in gaps in the data and encoding is used to transform categorical variables into numerical ones (e.g., one-hot encoding).

Normalization methods such as Min-Max scaling are used to put all the features in a similar range, which enhances the effectiveness of training the model.

3.3 Feature Selection

The feature selection is carried out to determine the most useful features that help in intrusion detection. Minimizing computational complexity and enhancing the performance of models can be achieved by reducing the number of features. Techniques such as correlation analysis, information gain, and recursive feature elimination are used to select significant features. This action is taken to make sure that only informative data is utilized to train AI models.

3.4 AI Models Used

The research uses various AI models to measure their capability to detect intrusions:

• *Decision Tree:* This is a simple and understandable model, which represents a tree-like structure used to make decisions based on the features value. It is quick and simple to apply and can be overfitted.

• *Random Forest:* This is an ensemble learning method which consists of multiple decision trees to enhance accuracy and minimize overfitting. It offers enhanced generalization and is extensively applied in classification issues.

• *Neural Networks:* These are models that are made up of interrelated layers of neurons and are able to learn intricate patterns in data. Deep learning models and neural networks, in particular, are extremely useful in identifying advanced cyberattacks.

All the models are trained with the help of the chosen dataset and are measured by the performance metrics.

3.5 System Architecture (IDS Workflow)

The suggested AI-based IDS is based on a systematic workflow:

Input: Data is a real-time or from datasets collection of network traffic data.

• *Preprocessing:* Data is normalized and cleaned.

• *Feature Selection:* Noteworthy features are selected.

• *AI Model:* The analyzed data is inputted into trained models.

• *Detection:* The system identifies traffic as normal or malicious.

• *Alert:* In case an intrusion is detected, then an alert is sent to take action.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

This architecture is efficient in detecting intrusions and real-time monitoring.

IV. Performance Analysis

The effectiveness of the AI-based intrusion detection system is measured based on the conventional metrics to assess its ability to identify cyber threats.

Evaluation Metrics

The metrics used are:

• *Accuracy:* Determines the accuracy of the model. It represents the percentage of rightly predicted instances, to the total instances.

• *Exactly:* Refers to the percentage of correctly identified positive cases among all the predicted positives. It is an indication of the capability of the model to prevent false alarms.

• *Recall (Detection Rate):* The detection rate is a measure that shows how the model can detect real attacks. With high recall, it means an improved detection.

• *F1-Score:* The harmonic mean of precision and recall, which gives a balanced approach to the evaluation of a model performance.

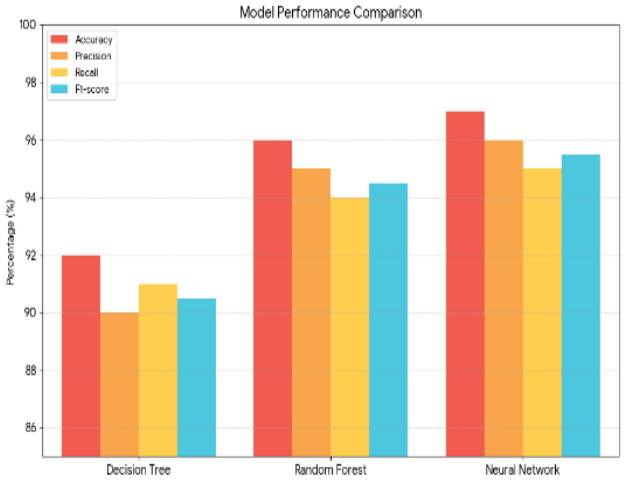
Comparison of AI Models.

The different AI models show varying levels of performance according to the complexity and learning capacities. Decision Trees are easy and quick, but might not work with complicated information. Random Forest provides a better predictor since it operates with multiple trees as opposed to Neural Networks which provides the best predictor since it can predict complicated trends in the information.

Table 1:
Performance of AI Models

Model	Accuracy	Precision	Recall	F1-score
Decision Tree	92%	90%	91%	90.5%
Random Forest	96%	95%	94%	94.5%
Neural Network	97%	96%	95%	95.5%

The findings show that Neural Networks are better than the other models and then comes the Random Forest. Decision Trees have a relatively lower accuracy.



Detection Rate vs False Alarm Rate

The results are that Neural Networks are better than other models, and, finally, there is the Random Forest. Decision Trees are less accurate.

False Alarm rate vs Detection rate.

A good IDS needs to have a high detection rate and low false alarm rate. Fake positives are also greatly minimized by the use of AI-based models as opposed to conventional IDS. Random Forest and Neural Networks have a higher balance of detection and false alarm, thus they are more applicable to real-world scenarios.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

V. Security Analysis

Intrusion detection systems that are based on AI systems will go a long way in improving the security of a network by offering smart and dynamic threat detection systems.

One of the benefits is the detection of unknown or zero-day attacks. Conventional IDS are based on predefined signatures and are unable to detect new threats [12].

On the other hand, AI models learn trends using the information and can learn and detect abnormal behavior, which can be utilized to know new attacks that have never been detected previously.

The other significant aspect of AI-based IDS is real-time monitoring. These systems are continually checking network traffic and provide immediate alert in case of suspicious activity. This assists organizations to react swiftly to any threats that may arise and reduce damages.

AI also prevents the false positives which is a common issue of traditional IDS [13]. Using historical data, the AI models will be able to be more effective in distinguishing between normal and malicious behavior, which reduces unnecessary alerts.

Adaptive learning capability is another important characteristic. The AI systems are constantly enhanced with new capabilities through the use of new information. This ensures that they are very effective in a dynamic environment where attack patterns change all the time.

Table 2:
Security Techniques in AI-based IDS

Technique	Purpose
Machine Learning	Pattern detection
Deep Learning	Complex attack identification
Encryption	Data protection
Authentication	Access control

Altogether, AI-based IDS can be a powerful and effective tool to improve network security.

VI. Challenges

Although AI-based intrusion detection systems have their benefits, there are a number of challenges associated with them.

The high computational cost is one of the main problems. The training of AI models, in particular deep learning models, is computationally intensive and consumes a lot of memory. Limited resources of organizations can be a limitation of this.

The need to have large datasets is another challenge. The training of AI models requires large datasets that are labeled, which are not necessarily available. Such data is time-consuming and costly to gather and label.

There are also concerns on false positives and false negatives. Even though AI can decrease false alarms, it is not able to eliminate them entirely. The wrong identification of attacks or normal traffic may influence system reliability.

Another critical issue is data privacy. The network data can be a source of sensitive information, and training AI models with this data can pose a question of data security and confidentiality.

Lastly, overfitting of the model is a typical machine learning issue. When a model is overfitted to a dataset, it might not generalize well to other unseen data. To overcome this problem, proper validation techniques are needed.

VII. Future Work

The current studies of AI-based intrusion detection systems can be developed in the future in the following areas to enhance performance and applicability.

The detection accuracy can be further improved by using more sophisticated deep learning models like Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN). Such models can analyze complex patterns and temporal data in network traffic.

Integration with cloud computing and Internet of Things (IoT) environments is another important area. With the growth in the number of IoT devices, it is important to secure these networks. Such systems can be monitored and secured by AI-based IDS.

It is also promising to develop real time adaptive IDS systems. Such systems have the ability to automatically adapt to the evolving network conditions and new threats without human intervention.

Another recent area is explainable AI (XAI), which aims at enhancing the understandability of AI models. Explicit explanations of the decisions made by the detection system could enhance the use and acceptance of AI-based security systems.

VIII. Conclusion

Finally, the sophistication of cyber threats has rendered conventional intrusion detection systems inadequate in the provision of network security. The solution is Artificial Intelligence, which provides effective intrusion detection that is intelligent, adaptive, and efficient.

This paper outlines the usefulness of AI-based IDS in identifying known and unknown attacks to a high degree of accuracy. The models like Neural Networks and Random Forest show high performance than conventional methods.

AI-based systems have a number of benefits, such as real-time monitoring, minimized false positives, and continuous learning. But issues like high computational cost, data needs and privacy issues need to be considered.

All in all, AI has greatly enhanced intrusion detection systems in terms of efficiency and reliability. The cybersecurity solutions will be enhanced by further developments of deep learning, cloud integration, and explainable AI in the future. AI-based IDS will play a crucial role in building secure and resilient network infrastructures in the future.

REFERENCES

[1] Ahmad R, Salahuddin H, Rehman AU, Rehman A, Shafiq MU, Tahir MA, Afzal MS. Enhancing database security through AI-based intrusion detection system. Journal of Computing & Biomedical Informatics. 2024 Sep 1;7(02).

[2] Nay T. Enhancing iot security with ai-driven hybrid machine learning and neural network-based intrusion detection system. Babylonian Journal of Artificial Intelligence. 2024 Dec 5;2024:158-67.

[3] Park C, Lee J, Kim Y, Park JG, Kim H, Hong D. An enhanced AI-based network intrusion detection system using generative adversarial networks. IEEE Internet of Things Journal. 2022 Oct 3;10(3):2330-45.

[4] Saini J, Kumari A, Kumar S, Yadav A. Enhancing Network Security With Ai-Driven Intrusion Detection. In2025 International Conference on Innovations and Emerging Technologies In AI & Communication Systems (IETACS) 2025 Nov 6 (pp. 482-486). IEEE.

[5] Abuali KM, Nissirat L, Al-Samawi A. Advancing network security with AI: SVM-based deep learning for intrusion detection. Sensors. 2023 Nov 3;23(21):8959.

[6] Kathirvel A, Maheswaran CP. Enhanced AI-Based intrusion detection and response system for WSN. InArtificial intelligence for intrusion detection systems 2023 Oct 16 (pp. 155-177). Chapman and Hall/CRC.

[7] Markevych M, Dawson M. A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai)". InInternational conference knowledge-based organization 2023 Jun (Vol. 29, No. 3, pp. 30-37).

[8] Gujar SS. AI-enhanced intrusion detection systems for strengthening critical infrastructure security. In2024 Global Conference on Communications and Information Technologies (GCCIT) 2024 Oct 25 (pp. 1-7). IEEE.

[9] Yadulla AR, Kasula VK, Yenugula M, Konda B. Enhancing cybersecurity with AI: implementing a deep learning-based intrusion detection system using convolutional neural networks. European Journal of Advances in Engineering and Technology. 2023;10(12):89-98.

[10] Dash B, Ansari MF, Sharma P, Ali A. Threats and opportunities with AI-based cyber security intrusion detection: a review. International Journal of Software Engineering & Applications (IJSEA). 2022 Sep;13(5).

[11] Sivakumar J, Salman NR, Salman FR, Salimova HR, Ghimire E. AI-driven cyber threat detection: enhancing security through intelligent engineering systems. Journal of Information Systems Engineering and Management. 2025 Mar 14;10(19):790-8.

[12] Vikram A, Shnain AH, Jeet R, Vennila C, Sahu P, Krishnakumar K. Ai-powered network intrusion detection systems. In2024 IEEE international conference on communication, computing and signal processing (IICCCS) 2024 Sep 19 (pp. 1-6). IEEE.

[13] Chauhan GS, Mekala R. AI-driven intrusion detection systems: Enhancing cybersecurity with machine learning algorithms. International Journal of Multidisciplinary and Current Research. 2019 Apr 25;7(2):131-9.