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 5, May 2026

DOI: 10.17148/IJARCCE.2026.15564

AI Driven IDS System in Network Security

Kartik P Shetty[1], Prof. Theerthashree G S[2]

PG Student, Dept. of MCA, Bangalore Institute of Technology, Bengaluru-560 004, Karnataka, India[1]

Professor, Dept. of MCA, Bangalore Institute of Technology, Bengaluru-560 004, Karnataka, India[2]

Abstract: The increasing use of internet technologies, cloud computing, and smart devices has significantly increased cyber threats in modern networks. Traditional Intrusion Detection Systems (IDS) are unable to effectively detect advanced and unknown attacks because they rely mainly on predefined signatures and static security rules. Artificial Intelligence (AI) based IDS provides an intelligent and adaptive approach for improving network security. This paper presents a seminar-based study on AI Driven IDS Systems in Network Security using Machine Learning and Deep Learning techniques. The proposed system analyzes network traffic patterns, identifies abnormal behavior, and detects cyberattacks with improved accuracy and reduced false alarm rates. Various AI algorithms such as Random Forest, Support Vector Machine, Convolutional Neural Network, and Long Short-Term Memory are discussed in this paper. The study highlights the importance of AI-driven security systems in detecting both known and unknown threats efficiently. The proposed approach enhances overall network protection and provides better adaptability against evolving cyberattacks.

Keywords: Artificial Intelligence, Intrusion Detection System, Machine Learning, Deep Learning, Network Security, Cybersecurity

I. INTRODUCTION

In the modern digital era, computer networks are widely used in banking, education, healthcare, business, cloud computing, and communication systems. The continuous growth of internet services and connected devices has increased the risk of cyberattacks and unauthorized access to sensitive information. Attackers use advanced techniques such as malware, phishing, ransomware, denial-of-service attacks, and data theft to compromise network security. Therefore, protecting network infrastructure has become an essential requirement for organizations and individuals.

Traditional security systems such as firewalls and antivirus software provide only limited protection against modern cyber threats. Signature-based Intrusion Detection Systems (IDS) are effective for detecting known attacks, but they fail to identify unknown or zero-day attacks because they depend on predefined attack signatures. Due to the rapid evolution of cyber threats, there is a need for intelligent and adaptive security mechanisms.

Artificial Intelligence (AI) plays an important role in improving the performance of Intrusion Detection Systems. AI-based IDS can automatically learn network traffic behavior, analyze large volumes of data, and detect abnormal activities in real time. Machine Learning (ML) and Deep Learning (DL) algorithms help in identifying attack patterns with high accuracy and lower false positive rates. These technologies enable IDS systems to adapt to changing attack patterns and improve overall network security.

This seminar paper focuses on the study of AI Driven IDS Systems in Network Security and discusses various AI techniques used for intrusion detection. The paper also explains the advantages, challenges, and applications of machine learning and deep learning approaches in protecting modern computer networks against cyber threats.

II. LITERATURE SURVEY

Several researchers have proposed Artificial Intelligence and Machine Learning based Intrusion Detection Systems to improve network security and overcome the limitations of traditional IDS models.

Mahdi Zamani and Mahnush Movahedi discussed different machine learning techniques used in intrusion detection systems. Their study explained how AI-based IDS improves detection accuracy and reduces false alarm rates compared to traditional methods. The paper highlighted the importance of adaptive learning techniques in identifying dynamic cyber threats.

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15564

Richard Kimanzi et al. reviewed various deep learning algorithms such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Deep Neural Networks (DNN), and Long Short-Term Memory (LSTM) models for intrusion detection systems. Their research showed that deep learning techniques provide better performance in analyzing large-scale network traffic and detecting complex attacks.

Ziadoon K. Maseer and other researchers presented a systematic review of anomaly-based Network Intrusion Detection Systems using Machine Learning and Deep Learning approaches. Their study focused on datasets, attack detection methods, and performance evaluation techniques. The authors concluded that AI-based IDS offers better adaptability for detecting unknown attacks in modern networks.

Adel Alabbadi and Fuad Bajaber proposed an explainable AI-based intrusion detection system for IoT environments. Their research used deep learning models including CNN and DNN along with Explainable Artificial Intelligence (XAI) techniques to improve transparency and understanding of attack predictions.

Soham Chatterjee and team conducted an experimental study using deep learning models such as Artificial Neural Networks (ANN), CNN, and LSTM for network intrusion detection. Their research demonstrated that deep learning techniques significantly improve attack classification accuracy and response efficiency in IDS systems.

MohammadNoor Injadat and other researchers proposed a multi-stage optimized machine learning framework for network intrusion detection. Their work focused on feature selection, hyperparameter optimization, and reducing computational complexity while maintaining high detection performance.

From the literature survey, it is observed that AI, Machine Learning, and Deep Learning technologies greatly improve the performance of intrusion detection systems by increasing detection accuracy, reducing false positives, and enabling real-time detection of sophisticated cyberattacks.

III. EXISTING SYSTEM

Traditional Intrusion Detection Systems mainly use signature-based and rule-based techniques to identify malicious activities in computer networks. These systems compare network traffic with predefined attack signatures stored in databases. If a match is found, the system generates an alert for the detected attack.

Existing IDS models are capable of detecting known cyber threats effectively, but they face several limitations when dealing with modern and sophisticated attacks. Since traditional systems depend heavily on predefined rules and signatures, they are unable to identify new or zero-day attacks that do not already exist in the database. In addition, these systems often generate high false positive and false negative rates, which reduces their overall efficiency.

Conventional IDS also struggle to process large volumes of network traffic generated in modern environments such as cloud computing, IoT networks, and enterprise systems. Manual updating of attack signatures is time-consuming and requires continuous monitoring by security experts. As cyberattacks evolve rapidly, traditional IDS approaches become less effective in providing real-time and adaptive security solutions.

Some existing systems use machine learning techniques to improve intrusion detection performance. However, many of these models suffer from issues such as high computational complexity, insufficient training datasets, overfitting problems, and limited adaptability against evolving attack patterns.

Therefore, there is a need for an intelligent and AI-driven Intrusion Detection System that can automatically learn network behavior, analyze traffic patterns efficiently, and detect both known and unknown attacks with higher accuracy and lower false alarm rates.

IV. PROPOSED SYSTEM

The proposed system presents an AI Driven Intrusion Detection System for improving network security using Machine Learning and Deep Learning techniques. The system is designed to monitor network traffic continuously, analyze communication patterns, and detect malicious activities in real time.

 This work is licensed under a Creative Commons Attribution 4.0 International License

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 5, May 2026

DOI: 10.17148/IJARCCE.2026.15564

In the proposed approach, network traffic data is collected from different sources such as routers, servers, and network devices. The collected data is preprocessed to remove duplicate and irrelevant information. Feature extraction techniques are then applied to identify important attributes related to network behavior.

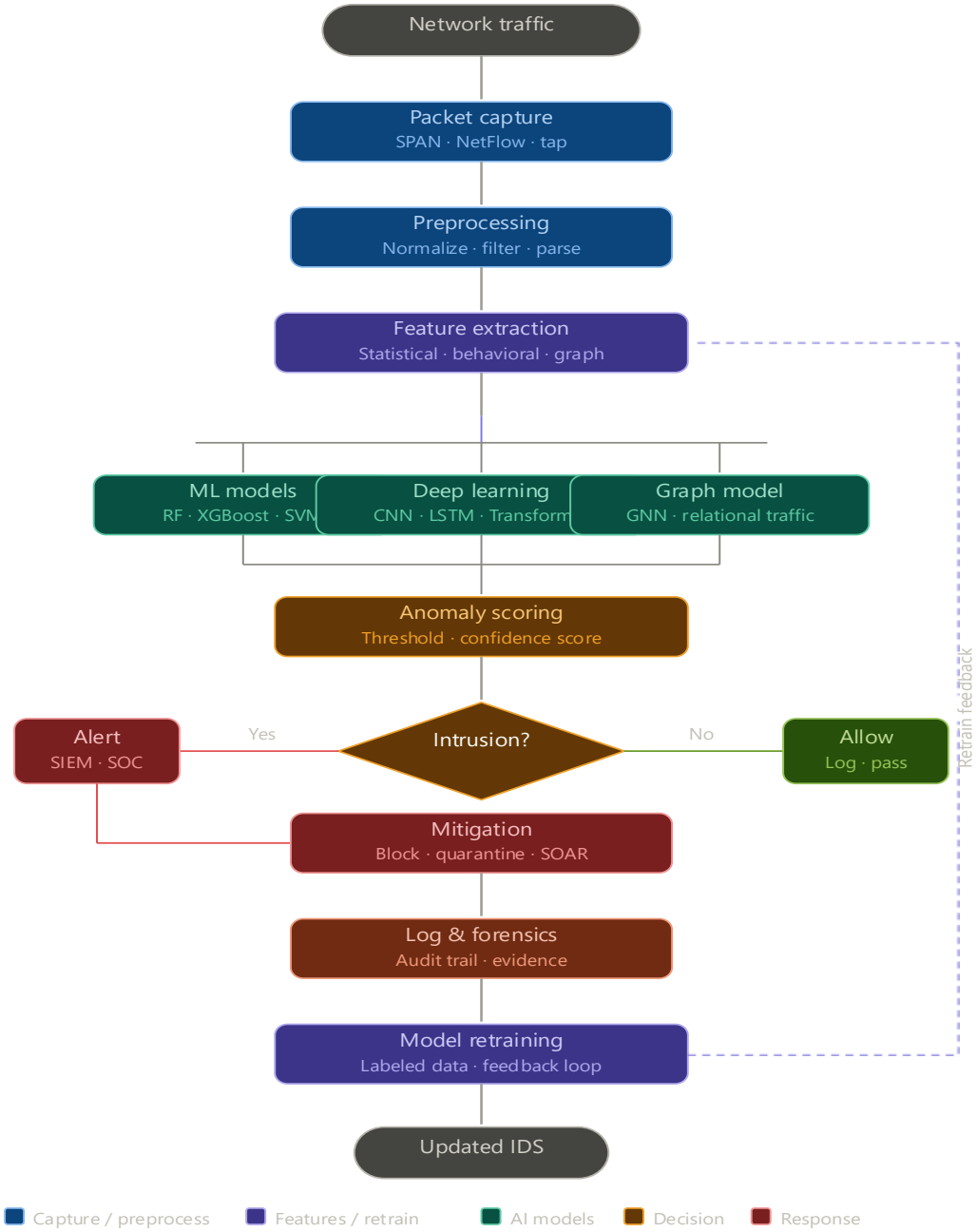

Fig. 1. Architecture of AI Driven IDS

Machine Learning and Deep Learning algorithms are used to train the intrusion detection model. Algorithms such as Random Forest, Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) help in classifying network traffic into normal and malicious categories. These AI techniques improve detection accuracy and reduce false alarm rates compared to traditional IDS methods.

The proposed system is capable of identifying both known and unknown attacks by learning traffic patterns automatically. It can detect cyber threats such as Denial of Service (DoS), Distributed Denial of Service (DDoS), phishing, malware,

 This work is licensed under a Creative Commons Attribution 4.0 International License

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15564

and unauthorized access attacks. Deep learning models further enhance the system by identifying complex attack patterns in large-scale network environments.

The AI-driven IDS provides better adaptability, faster response, and improved scalability for modern networks including cloud computing and IoT environments. The proposed system enhances overall network security by providing intelligent, automated, and real-time intrusion detection capabilities.

V. METHODOLOGY

The methodology of the proposed AI Driven IDS System involves multiple stages for detecting malicious activities in network traffic. The system uses Artificial Intelligence, Machine Learning, and Deep Learning techniques to analyze network behavior and identify cyber threats efficiently.

A. Data Collection

In the first stage, network traffic data is collected from various network devices such as routers, servers, switches, and end-user systems. The collected data contains information related to packets, protocols, source IP addresses, destination IP addresses, and traffic behavior.

B. Data Preprocessing

The collected network data may contain duplicate, incomplete, or irrelevant information. Data preprocessing is performed to clean the dataset and improve the quality of input data. Techniques such as data cleaning, normalization, and feature selection are used to prepare the data for training and testing.

C. Feature Extraction

Feature extraction is an important step in identifying relevant attributes from network traffic. Important features such as packet size, connection duration, protocol type, and traffic patterns are extracted to improve intrusion detection performance and reduce computational complexity.

D. Model Training

Machine Learning and Deep Learning algorithms are trained using the processed dataset. Algorithms such as Random Forest, Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Long Short-Term Memory (LSTM) are used for learning network traffic patterns and attack behaviors.

E. Traffic Classification

The trained AI models classify network traffic into normal and malicious categories. The system identifies different types of attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), phishing, malware, and unauthorized access attacks.

F. Alert and Response

When malicious activity is detected, the IDS generates alerts and notifies network administrators. The system can also perform automatic response actions such as blocking suspicious traffic and updating attack logs for future analysis.

G. Continuous Learning

The proposed AI-driven IDS continuously improves its detection capability by updating the database with new attack patterns and retraining the learning models. This helps the system adapt to evolving cyber threats and improves overall network security performance.

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 5, May 2026

DOI: 10.17148/IJARCCE.2026.15564

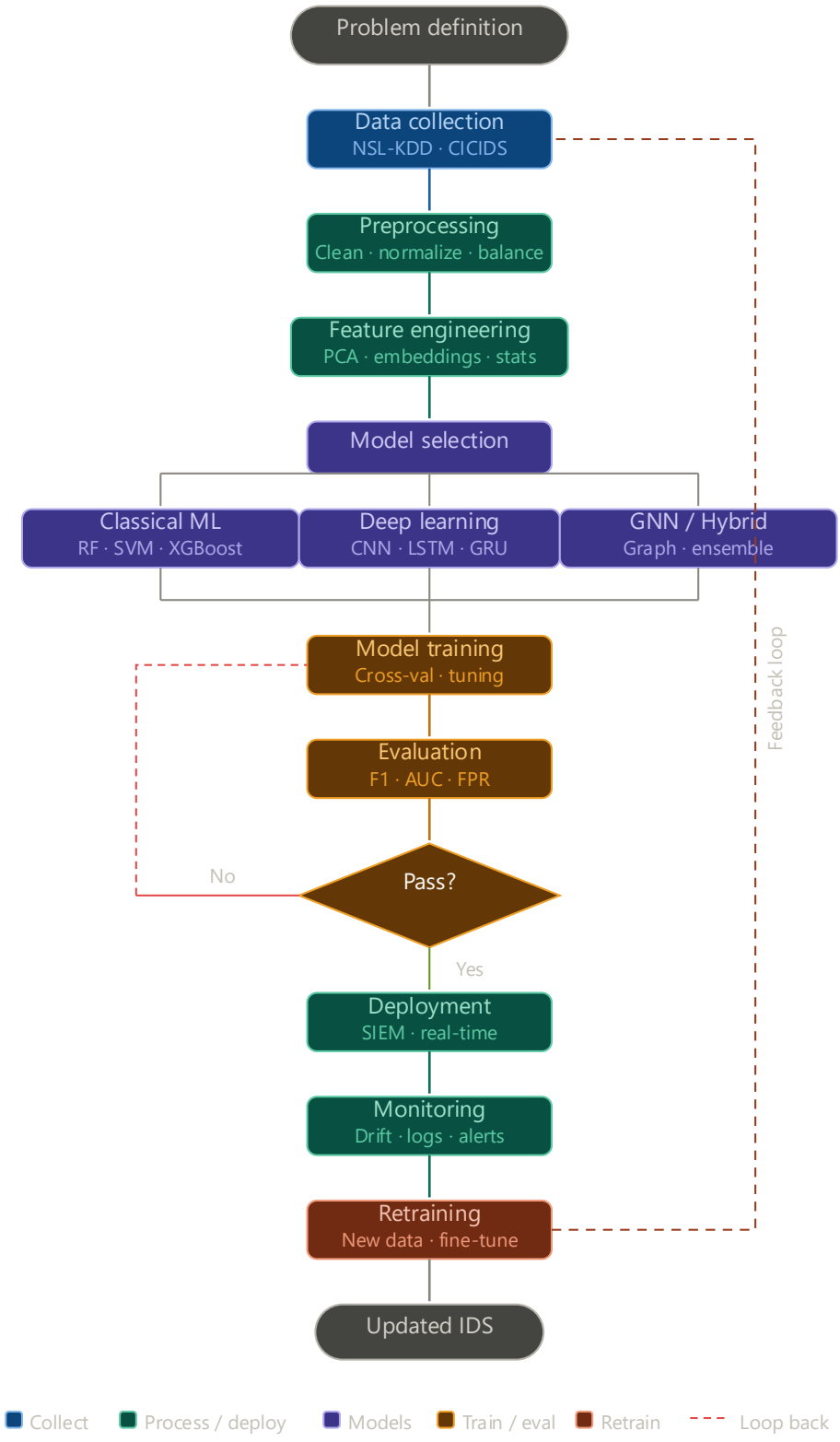

Fig. 2. Methodology of AI Driven IDS System

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 5, May 2026

DOI: 10.17148/IJARCCE.2026.15564

VI. ADVANTAGES

The AI Driven IDS System provides several advantages over traditional intrusion detection methods. Artificial Intelligence and Machine Learning techniques improve the efficiency and accuracy of detecting cyber threats in modern network environments.

1. Improved Detection Accuracy
   AI-based IDS can identify malicious activities with higher accuracy compared to traditional signature-based systems.
2. Detection of Unknown Attacks
   The system can detect zero-day and unknown attacks by analyzing abnormal network behavior patterns.
3. Reduced False Alarm Rate
   Machine Learning algorithms help reduce false positives and false negatives during intrusion detection.
4. Real-Time Monitoring
   The proposed system continuously monitors network traffic and detects threats in real time.
5. Automatic Learning Capability
   AI models automatically learn from network data and improve detection performance over time.
6. Faster Response to Threats
   The system quickly identifies suspicious activities and generates alerts for immediate action.
7. Scalability
   The proposed IDS can efficiently handle large-scale network traffic generated in cloud computing and IoT environments.
8. Improved Network Security
   AI-driven IDS enhances the overall confidentiality, integrity, and availability of network resources.

VII. APPLICATIONS

The AI Driven IDS System has various applications in protecting modern computer networks and digital infrastructures from cyber threats. The use of Artificial Intelligence and Machine Learning techniques improves security performance in different environments.

1. Banking and Financial Systems
   AI-based IDS helps protect online banking systems and financial transactions from cyberattacks, fraud, and unauthorized access.
2. Cloud Computing Security
   The system monitors cloud network traffic and detects malicious activities in cloud environments to ensure secure data storage and communication.
3. Internet of Things (IoT) Security
   AI-driven IDS provides protection for IoT devices and smart systems against malware, botnets, and unauthorized network access.
4. Healthcare Systems
   Hospitals and healthcare organizations use IDS to secure patient records and medical devices from cyber threats and data breaches.
5. Educational Institutions
   Schools, colleges, and universities use intrusion detection systems to protect academic data and online learning platforms.
6. Enterprise Network Security
   Organizations use AI-based IDS to monitor employee activities, detect insider threats, and secure confidential business information.
7. Government and Defense Systems
   Government agencies and defense networks use intelligent IDS systems to protect sensitive information and national security infrastructures.
8. Smart Cities and Industrial Networks
   AI-driven IDS helps secure smart city infrastructure, industrial control systems, and communication networks from cyberattacks.

 This work is licensed under a Creative Commons Attribution 4.0 International License

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 5, May 2026

DOI: 10.17148/IJARCCE.2026.15564

VIII. CHALLENGES

Although AI Driven Intrusion Detection Systems provide significant improvements in network security, several challenges still exist in implementing and maintaining these systems effectively.

1. Large Volume of Network Data
   Modern networks generate massive amounts of traffic data, making real-time analysis and intrusion detection computationally complex.
2. High Computational Requirements
   Deep Learning algorithms require powerful hardware resources, high processing capability, and large memory for training and deployment.
3. False Positive and False Negative Alerts
   AI models may sometimes incorrectly classify normal traffic as malicious or fail to detect actual attacks, affecting system reliability.
4. Dataset Quality and Availability
   Training Machine Learning models requires high-quality and balanced datasets. Incomplete or outdated datasets can reduce detection accuracy.
5. Evolving Cyber Threats
   Cyberattacks continuously evolve, making it difficult for IDS systems to adapt quickly to new and sophisticated attack patterns.
6. Privacy and Security Concerns
   Network traffic analysis may involve sensitive information, raising concerns regarding user privacy and data protection.
7. Complexity of AI Models
   Some Deep Learning models are highly complex and difficult to interpret, making system management and maintenance challenging.
8. Implementation Cost
   Developing and deploying AI-driven IDS systems may require high infrastructure and maintenance costs for organizations.

IX. CONCLUSION

Network security has become a major concern due to the rapid increase in cyber threats and malicious activities in modern communication systems. Traditional Intrusion Detection Systems are unable to effectively detect advanced and unknown attacks because they mainly rely on predefined signatures and static security rules.

This paper presented a seminar-based study on an AI Driven IDS System in Network Security using Machine Learning and Deep Learning techniques. The proposed system improves intrusion detection performance by analyzing network traffic patterns, identifying abnormal activities, and detecting cyber threats in real time. AI-based approaches such as Random Forest, Support Vector Machine, Convolutional Neural Network, and Long Short-Term Memory help improve detection accuracy and reduce false alarm rates.

The study highlights the importance of Artificial Intelligence in enhancing modern network security systems. AI-driven IDS provides better adaptability, scalability, and faster response against evolving cyberattacks in cloud computing, IoT, enterprise, and smart network environments.

In the future, AI-based Intrusion Detection Systems can be further improved by integrating advanced Deep Learning models, Explainable AI techniques, and real-time threat intelligence systems to provide stronger and more intelligent cybersecurity solutions.

X. REFERENCES

[1]. Mahdi Zamani and Mahnush Movahedi, “Machine Learning Techniques for Intrusion Detection.”
[2]. Richard Kimanzi, Peter Kimanga, Dedan Cherori, and Patrick K. Gikunda, “Deep Learning Algorithms Used in Intrusion Detection Systems - A Review.”
[3]. Ziadoon K. Maseer, Robiah Yusof, Baidaa Al-Bander, Abdu Saif, and Qusay Kanaan Kadhim, “Systematic Review for Anomaly Network Intrusion Detection Systems: Detection Methods, Dataset, Validation Methodology, and Challenges.”

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15564

[4]. Adel Alabbadi and Fuad Bajaber, "An Intrusion Detection System over the IoT Data Streams Using eXplainable Artificial Intelligence (XAI)."
[5]. Soham Chatterjee, Satvik Chaudhary, and Aswani Kumar Cherukuri, "Intrusion Detection System Using Deep Learning for Network Security."
[6]. Tanwir Ahmad, Dragos Truscan, Juri Vain, and Ivan Porres, "Early Detection of Network Attacks Using Deep Learning."
[7]. Rana Abou Khamis and Ashraf Matrawy, "Evaluation of Adversarial Training on Different Types of Neural Networks in Deep Learning-based IDSs."
[8]. Rana AbouKhamis, Omair Shafiq, and Ashraf Matrawy, "Investigating Resistance of Deep Learning-based IDS against Adversaries using min-max Optimization."
[9]. Mahdi Soltani, Behzad Ousat, Mahdi Jafari Siavoshani, and Amir Hossein Jahangir, "An Adaptable Deep Learning-Based Intrusion Detection System to Zero-Day Attacks."
[10]. Ismail Bibers, Osvaldo Arreche, and Mustafa Abdallah, "A Comprehensive Comparative Study of Individual ML Models and Ensemble Strategies for Network Intrusion Detection Systems."
[11]. MohammadNoor Injadat, Abdallah Moubayed, Ali Bou Nassif, and Abdallah Shami, "Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection."
[12]. Haiyan Xuan and Mohith Manohar, "Intrusion Detection System with Machine Learning and Multiple Datasets."
[13]. Saeid Jamshidi, Amin Nikanjam, Nafi Kawser Wazed, and Foutse Khomh, "Leveraging Machine Learning Techniques in Intrusion Detection Systems for Internet of Things."
[14]. Muhammad Azmi Umer, Khurum Nazir Junejo, Muhammad Taha Jilani, and Aditya P. Mathur, "Machine Learning for Intrusion Detection in Industrial Control Systems: Applications, Challenges, and Recommendations."
[15]. Amar Amouri, Vishwa T. Alaparthy, and Salvatore D. Morgera, "A Machine Learning Based Intrusion Detection System for Mobile Internet of Things."
[16]. Benjamin J. Radford, Leonardo M. Apolonio, Antonio J. Trias, and Jim A. Simpson, "Network Traffic Anomaly Detection Using Recurrent Neural Networks," arXiv:1803.10769, 2018.
[17]. Kathryn-Ann Tait, Jan Sher Khan, Fehaid Alqahtani, Awais Aziz Shah, Fadia Ali Khan, Mujeeb Ur Rehman, Wadii Boulila, and Jawad Ahmad, "Intrusion Detection using Machine Learning Techniques: An Experimental Comparison."
[18]. Mouhammad Alkasassbeh and Mohammad Almseidin, "Machine Learning Methods for Network Intrusion Detection."
[19]. Jaydip Sen and Sidra Mehtab, "Machine Learning Applications in Misuse and Anomaly Detection."
[20]. Xiaoxuan Wang and Rolf Stadler, "IT Intrusion Detection Using Statistical Learning and Testbed Measurements."
[21]. David Pujol-Perich, Jose Suarez-Varela, Albert Cabellos-Aparicio, and Pere Barlet-Ros, "Unveiling the Potential of Graph Neural Networks for Robust Intrusion Detection."
[22]. Kiymet Kaya, Elif Ak, Sumeyye Bas, Berk Canberk, and Sule Gunduz Oguducu, "X-CBA: Explainability Aided CatBoosted Anomal-E for Intrusion Detection System."
[23]. Yi Liu and Lanjian Wu, "Intrusion Detection Model Based on Improved Transformer."
[24]. Jamshed Ali Shaikh, Chengliang Wang, Muhammad Wajeeh Us Sima, Muhammad Arshad, Muhammad Owais, Dina S. M. Hassan, Reem Alkanhel, and Mohammed Saleh Ali Muthanna, "A deep Reinforcement learning-based robust Intrusion Detection System for securing IoMT Healthcare Networks."

 This work is licensed under a Creative Commons Attribution 4.0 International License