MULTIDISCIPLINARY RESEARCH IN COMPUTING INFORMATION SYSTEMS

VOL 05 ISSUE 06 2025

P-ISSN: 3080-7182
E-ISSN: 3080-7190

https://mrcis.org

AI-DRIVEN INTRUSION DETECTION SYSTEMS FOR SMART NETWORK SECURITY

Ayesha Malik [1], Muhammad Usman [2]

Abstract. *As smart networks grow in complexity and scale, the need for advanced security mechanisms becomes critical. Traditional intrusion detection systems (IDS) often struggle to cope with the scale and sophistication of attacks in these environments. Artificial Intelligence (AI) techniques, particularly machine learning (ML) and deep learning (DL), offer promising solutions for enhancing the detection and mitigation of intrusions in smart network environments. This paper explores the role of AI-driven IDS in smart network security, examining various machine learning and deep learning techniques, their applications, and the challenges in deploying them. We present a comparative analysis of AI-based IDS with traditional systems, highlight the effectiveness of AI-driven models in real-time threat detection, and outline the potential future directions for research. The article also discusses the integration of AI systems with network infrastructures and presents two conceptual charts for performance comparison.*

Keywords: *Intrusion Detection, AI, Machine Learning, Smart Network Security.*

INTRODUCTION

In today's interconnected world, smart networks that include IoT devices, sensors, and cloud-based infrastructures are increasingly prone to cyber-attacks. Traditional intrusion detection systems (IDS) often rely on predefined rules and signature-based methods, which fail to detect new, sophisticated, or unknown attacks. With the advent of AI-driven solutions, specifically machine learning (ML) and deep learning (DL) algorithms, IDS have evolved to handle complex attack patterns in real-time. These AI techniques are capable of learning from data, adapting to emerging threats, and providing more accurate predictions and fewer false alarms. The integration of AI into IDS offers potential benefits such as improved detection rates, real-time response capabilities, and enhanced security of smart networks. This paper explores the capabilities, challenges, and future research areas of AI-driven IDS in securing smart network environments.

[1] *Department of Computer Science, Lahore University of Management Sciences (LUMS), Lahore, Pakistan.*

[2] *School of Computing and Information Technology, Institute of Business Administration (IBA), Karachi, Pakistan.*

1. AI-Driven Intrusion Detection Systems (IDS) Architecture

AI-driven Intrusion Detection Systems (IDS) represent a significant advancement over traditional security systems by utilizing artificial intelligence (AI) to automatically detect and respond to malicious activities within a network. These systems leverage machine learning (ML) and deep learning (DL) algorithms to enhance the detection of known and unknown threats in real-time. The architecture of an AI-based IDS typically consists of the following core components:

1.1 Data Collection

The first step in an AI-driven IDS is data collection, where network data from various sources is gathered for analysis. This data includes:

Network traffic data: Packets, connections, and flow information, which can provide insights into potential malicious activities such as Denial-of-Service (DoS) attacks, port scans, and botnet communications.

System logs: Logs from devices like routers, firewalls, servers, and IoT devices that record network activity, user actions, and system states.

Application logs: Application-specific logs (e.g., web server logs, database logs) that capture abnormal behavior or unauthorized access attempts.

Sensor data: In more advanced IDS, sensor data from devices and end systems in smart networks (e.g., IoT devices) are collected to monitor physical interactions and communications within the network.

Effective data collection requires integrating various data sources and ensuring that the data is comprehensive and relevant to intrusion detection.

1.2 Data Preprocessing

Once the data is collected, it must undergo preprocessing to ensure it is clean, normalized, and ready for analysis. This step includes:

Data cleaning: Identifying and handling missing values, removing outliers, and correcting errors in the dataset. This ensures that the model is trained on high-quality data.

Data normalization: Scaling the data to a consistent range or format, especially when different data sources have different ranges (e.g., network traffic, log entries). Techniques like min-max scaling or Z-score normalization are commonly used.

Feature selection: Selecting relevant features or attributes from the raw data to improve the model's performance and reduce computational complexity. This can include extracting statistical features, such as packet sizes, IP addresses, and the number of failed login attempts.

Preprocessing ensures that the raw data is ready for meaningful analysis and eliminates any noise that could negatively impact model performance.

1.3 Feature Extraction

Feature extraction is the process of transforming raw data into a set of useful features that can be used by machine learning models for intrusion detection. Features are critical for accurately classifying network activity as either normal or malicious. Some common features extracted in AI-based IDS include:

Flow-based features: These include the duration of a network connection, the number of bytes sent, the number of packets transferred, and the frequency of certain communication protocols.

Packet-level features: These features are based on individual packets of data, such as packet size, packet inter-arrival time, and the types of packets sent or received.

Statistical features: These features capture patterns or anomalies in the data, such as the distribution of bytes over time, the number of failed login attempts, or the variance in packet lengths.

Effective feature extraction enables AI models to better understand the relationships and patterns within the data, which improves the detection accuracy.

1.4 Classification Models

Once the data has been preprocessed and relevant features have been extracted, AI-based IDS systems use various classification models to identify and classify potential intrusions. These models are trained using historical data labeled as either “normal” or “malicious.” Common classification techniques include:

Decision Trees: Decision trees are simple yet powerful models that use a tree-like structure to make decisions based on input features. They are interpretable and can provide insights into the reasoning behind the classification decision. However, they are prone to overfitting and may not generalize well to unseen data.

Neural Networks (NN): Neural networks, particularly deep learning models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), can detect complex patterns in the data. CNNs are used to identify spatial patterns, while RNNs are used for sequential data (e.g., time-series data in network traffic). Deep learning models tend to outperform traditional models in complex intrusion detection tasks but require significant computational resources and large amounts of labeled data.

Random Forest: A random forest is an ensemble of decision trees, where each tree is trained on a different subset of data. The final decision is made by aggregating the results of each tree.

Random forests are effective in reducing overfitting and improving classification accuracy, especially with high-dimensional data.

Support Vector Machines (SVM): SVMs are supervised learning models that aim to find the optimal hyperplane that separates different classes in the feature space. SVMs are particularly useful for detecting boundary-based anomalies in network traffic.

The choice of classification model depends on the nature of the data, the type of intrusions being detected, and the computational resources available.

1.5 Response Mechanisms

Once an intrusion is detected, the response mechanism is triggered to mitigate the threat. This mechanism is responsible for taking actions based on the severity and type of intrusion. The response mechanisms can be:

Alerting: Sending real-time alerts to administrators or security teams to investigate the detected threat. Alerts can include information about the attack type, source, target, and affected systems.

Blocking: Automatically blocking or isolating the source of the intrusion, such as terminating a suspicious network connection or blocking an IP address involved in the attack.

Adaptive Response: Advanced AI-driven IDS systems can adaptively respond to the attack by modifying firewall rules, adjusting network routing to contain the attack, or increasing the monitoring of vulnerable areas of the network.

AI-driven IDS systems can take more intelligent and context-aware actions, such as learning from past attacks and automatically adjusting response protocols for future incidents.

2. Machine Learning vs. Deep Learning in IDS

Intrusion Detection Systems (IDS) have evolved significantly with the advent of Machine Learning (ML) and Deep Learning (DL) techniques. Both ML and DL are pivotal in enhancing the accuracy and efficiency of IDS by automating the detection of network intrusions, and they are applied in different ways depending on the complexity of the data and the specific problem at hand. Below, we explore how these two paradigms are used in detecting intrusions.

Machine Learning (ML) in IDS

Machine learning techniques, particularly supervised learning, have been widely used for intrusion detection tasks. ML algorithms rely on labeled data to train models that can classify network activities as either normal or anomalous (intrusions). Some popular ML algorithms applied to IDS include:

Support Vector Machines (SVMs):

SVMs are powerful supervised learning models that work by finding the optimal hyperplane that separates data points into distinct classes (normal and malicious). In IDS, SVMs are particularly effective when the data is high-dimensional and well-separated. SVMs are used to detect intrusions by training the model on network traffic and classifying incoming traffic as either benign or suspicious based on the decision boundary created by the SVM. SVMs are known for their high accuracy, especially in binary classification problems, but they can be computationally expensive in terms of both memory and time.

Random Forest (RF):

Random Forest is an ensemble learning method that combines multiple decision trees to make a final classification decision. Each decision tree is trained on a random subset of features from the training dataset. In IDS, Random Forest can handle large datasets with high-dimensional features and can classify network traffic with good accuracy. One of its key strengths is its ability to reduce overfitting by averaging the predictions of individual decision trees. Random Forest can handle both categorical and continuous data, making it versatile in detecting a wide range of intrusions.

K-Nearest Neighbors (K-NN):

K-NN is a simple and intuitive classification algorithm that identifies the "k" nearest neighbors of a given data point based on a distance metric (such as Euclidean distance). For IDS, K-NN classifies incoming data points (network traffic) based on the majority class of the closest training instances. It is particularly useful for anomaly detection, where it can detect outliers in network traffic that deviate from normal patterns. However, K-NN can be computationally expensive for large datasets and may struggle to handle high-dimensional data efficiently.

Deep Learning (DL) in IDS

Deep learning techniques, particularly neural networks, have gained traction in IDS due to their ability to automatically learn complex, hierarchical representations from raw data. Unlike traditional ML techniques, DL models can learn directly from unprocessed data, such as raw network traffic, without requiring manual feature engineering. Some popular DL models used in IDS include:

Convolutional Neural Networks (CNNs):

CNNs are typically used in computer vision tasks but have been adapted for intrusion detection, especially when analyzing sequential data or visualized network traffic. CNNs automatically learn hierarchical patterns in the data by applying convolutional filters to extract features. For IDS, CNNs are capable of detecting anomalies in network traffic that may not be captured by traditional methods. By applying CNNs to graphical representations of network activity (such as heatmaps or traffic patterns), they can learn to identify complex attack patterns and generalize to unseen threats. CNNs excel in detecting spatial patterns but require large amounts of labeled data for training.

Recurrent Neural Networks (RNNs):

RNNs are designed to handle sequential data, making them ideal for time-series analysis such as network traffic over time. In IDS, RNNs can detect intrusions by analyzing temporal patterns in network behavior, such as sudden spikes in traffic or unusual request patterns. Long Short-Term Memory (LSTM) networks, a type of RNN, are especially effective in capturing long-term dependencies in the data, allowing the model to remember past network behavior and detect deviations in real-time. RNNs are particularly useful for detecting intrusions that span multiple time steps, such as DDoS attacks or botnet activity.

Key Differences Between ML and DL in IDS

Data Requirement: ML models often require smaller datasets, but feature extraction and preprocessing are critical for their success. In contrast, DL models typically require large datasets to learn effectively, and they can automatically extract relevant features from raw data.

Complexity: DL models are more complex and computationally expensive than traditional ML models. They require significant hardware resources (e.g., GPUs) for training and inference. ML models, on the other hand, are less computationally demanding and are often preferred when computational resources are limited.

Interpretability: One of the major drawbacks of DL models is their "black-box" nature, meaning it is difficult to interpret how the model makes its decisions. This is a challenge in security-critical applications like IDS, where transparency is essential. ML models like decision trees are more interpretable, allowing security analysts to understand the decision-making process.

3. AI Techniques for Real-Time Intrusion Detection

Real-time intrusion detection is crucial for identifying and mitigating security threats as they occur, preventing damage or data breaches. AI techniques, including machine learning and deep learning, are particularly suited for real-time intrusion detection due to their ability to continuously monitor and update models based on incoming data. Below are the key AI techniques for real-time intrusion detection:

Model Updates in Real-Time

In real-time intrusion detection, models need to be constantly updated with the latest data to maintain their accuracy and effectiveness. AI-driven IDS systems can be designed to update their models dynamically as new network traffic data is received. Incremental learning techniques allow models to be trained continuously without the need for retraining from scratch, which can be time-consuming. For example, online learning algorithms allow the model to adapt to new data patterns in real time, ensuring that the IDS is always aware of the most recent threat patterns. This capability is especially important in smart networks, where attack techniques are continually evolving.

Anomaly Detection in Real-Time

Anomaly detection is a critical aspect of real-time intrusion detection. AI models can be trained to recognize normal network behavior and flag any deviations as potential intrusions. In smart network environments, real-time anomaly detection can help identify previously unknown threats (zero-day attacks) that do not match known signatures. Techniques such as unsupervised learning, autoencoders, and clustering algorithms are widely used for detecting anomalies in real time. These methods are capable of adapting to new patterns without requiring labeled data, making them suitable for real-time detection where new types of attacks may emerge.

Fast Decision-Making

The effectiveness of an IDS relies not only on detecting intrusions but also on responding to them in real-time. AI-driven IDS can provide fast decision-making capabilities that allow the system to classify network activities as normal or malicious in milliseconds. Deep reinforcement learning (DRL) is one technique that can be employed for real-time decision-making, where the system continuously learns the best actions to take (e.g., blocking a suspicious IP address or isolating a compromised node). DRL models can interact with the network and learn optimal security measures based on feedback from past actions, which improves their ability to respond to emerging threats in real time.

Real-Time Performance and Scalability

AI-driven IDS must be able to handle high volumes of data while maintaining low-latency processing times for real-time detection. Parallel processing, edge computing, and distributed learning are some techniques used to ensure that AI-driven IDS systems can scale effectively without compromising performance. By processing data locally at the edge of the network, AI models can reduce latency and improve real-time response times, making them ideal for deployment in large, distributed environments like smart cities or IoT networks.

AI techniques for real-time intrusion detection enable dynamic and responsive systems that can adapt to new threats, detect anomalies in real time, and take immediate actions to mitigate risks. These systems are increasingly critical for securing smart networks, where threats evolve rapidly, and fast detection is key to preventing damage.

4. Challenges in Implementing AI-Driven IDS in Smart Networks

While AI-driven Intrusion Detection Systems (IDS) offer significant advantages over traditional methods, their implementation in smart networks presents several challenges. These challenges range from technical difficulties related to data privacy and computational requirements to issues related to the quality of training data and the interpretability of models. Below, we discuss these challenges in detail:

Data Privacy Concerns

In smart networks, which often include Internet of Things (IoT) devices, sensitive data such as personal information, health data, and user activity is constantly generated. Data privacy is a significant concern when implementing AI-driven IDS because these systems often require access to network traffic and system logs that may contain personally identifiable information (PII). Sharing this data, even in the form of aggregated model updates, could still lead to potential privacy breaches, especially if adversaries manage to extract sensitive information through model inversion or membership inference attacks. To mitigate these risks, privacy-preserving techniques such as differential privacy, secure aggregation, and homomorphic encryption must be incorporated. However, these techniques often come with computational overheads, complicating their implementation in real-time systems.

High Computational Requirements

AI-driven IDS, particularly those based on deep learning models, often require substantial computational resources for both training and real-time inference. Deep learning models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) can be computationally expensive, requiring high-performance hardware such as Graphics Processing Units (GPUs) or Tensor Processing Units (TPUs) to process large amounts of network data. In a smart network with many distributed devices, the computational resources required for training and running AI models at scale can become a bottleneck. Furthermore, deploying such resource-intensive models at the edge or on IoT devices, which often have limited processing power, presents a challenge. Edge computing and model optimization techniques, such as model pruning and quantization, are being explored to reduce these computational demands while maintaining high accuracy.

Training Data Quality

The effectiveness of any AI-driven IDS is highly dependent on the quality and quantity of the training data. Data quality in smart networks can be affected by several factors:

- **Data inconsistency:** Data collected from different devices or sensors may be noisy, incomplete, or inconsistent, which can hinder the model's ability to detect intrusions accurately.

- **Non-IID (Non-Identically Distributed) data:** Smart networks often involve data from heterogeneous sources, such as IoT devices, mobile phones, and cloud systems, each with different data distributions. Models trained on such non-IID data may struggle to generalize across various network environments.

- **Labeling issues:** High-quality, labeled datasets are critical for supervised learning methods. However, acquiring large amounts of labeled attack data in smart networks can be difficult, as cyberattacks are often rare events, and labeling such data requires expertise and time.

To address these issues, ongoing research focuses on improving data cleaning, data augmentation, and semi-supervised learning techniques to create more reliable training datasets.

Model Interpretability

One of the major challenges with deep learning-based IDS is model interpretability. AI models, especially deep neural networks (DNNs), are often considered "black boxes" because it is difficult to understand how they arrive at specific decisions. This lack of transparency is problematic in security applications like IDS, where understanding why a model flagged an activity as malicious is critical for troubleshooting, trust, and accountability. In smart networks, where AI-driven IDS are used to make real-time decisions about whether to block or alert on suspicious activity, model transparency is vital. Researchers are working on techniques like Explainable AI (XAI), which aims to provide interpretable explanations for the decisions made by complex models. However, the trade-off between explainability and performance remains an area for further investigation.

5. Future Directions and Research Gaps

While AI-driven IDS systems have shown great promise in smart network security, several areas need further exploration to overcome current limitations and enhance their real-world applicability. Below, we outline some of the ongoing and future research directions in this field.

Cross-Platform Integration

In smart networks, data comes from a wide variety of devices, ranging from IoT sensors and mobile phones to cloud platforms and edge computing nodes. Cross-platform integration of these heterogeneous data sources is crucial for building comprehensive and effective IDS systems. The integration process involves ensuring that data can be consistently captured, preprocessed, and fed into AI models, regardless of the platform from which it originates. Research into interoperability standards and multi-platform data aggregation techniques is essential for building scalable IDS that work across different network environments. Additionally, creating platform-agnostic models that can handle data from diverse sources while maintaining performance is a key challenge.

Enhancing Model Explainability

As mentioned earlier, one of the biggest challenges in deploying AI-based IDS systems is the lack of explainability. To improve model trust and ensure regulatory compliance, there is an increasing demand for methods that allow AI models to provide understandable explanations for their decisions. Explainable AI (XAI) focuses on developing techniques that allow security analysts to interpret why an intrusion was detected or why an alert was triggered. Research into visualization tools and local explanation methods (such as LIME and SHAP) can help make complex AI models more interpretable and actionable for cybersecurity professionals.

Adaptive Learning in Dynamic Environments

Smart networks are dynamic environments where devices continuously join or leave, and network traffic patterns change over time. Adaptive learning refers to the ability of an IDS to update and refine its model based on new data and evolving attack strategies without the need for frequent retraining. For IDS systems to remain effective in dynamic environments, they must be able to learn in real-time and adapt to emerging attack vectors. Online learning and reinforcement learning are two promising approaches that allow models to update continually based on the latest data without requiring a full retraining process. Further research is needed to optimize these techniques for IDS in smart networks, where data may be scarce or constantly changing.

Collaboration with Blockchain for Secure Network Architectures

Blockchain technology holds significant potential for enhancing the security of smart networks, particularly in ensuring data integrity and secure communication. By integrating blockchain with AI-based IDS, researchers aim to create more resilient network architectures. Blockchain's decentralized nature can complement IDS by providing a secure and tamper-resistant ledger of network events, such as intrusion attempts or network anomalies. This would enable better accountability and transparency in IDS operations, as well as assist in maintaining the integrity of training data for AI models. Research into blockchain-assisted IDS systems is still in its infancy, but it represents an exciting direction for future advancements in securing smart networks.

Scalability and Real-Time Performance

As the scale of smart networks continues to grow, IDS systems must be capable of processing large volumes of data and responding to threats in real-time. Scalability is a critical factor for large-scale network environments, such as those found in smart cities or IoT ecosystems. AI models must be designed to handle massive data streams without compromising their ability to detect threats. Edge computing is one promising approach to improving the scalability and performance of IDS systems by processing data closer to the source (e.g., on IoT devices or edge nodes) rather than sending all data to centralized servers. Research into distributed AI systems and edge-based intrusion detection will be critical for meeting the demands of future smart networks.

Improved Data Privacy and Security

As privacy concerns grow in smart networks, there is a need to develop new techniques that allow AI-driven IDS to operate effectively while ensuring data privacy. Federated learning, for example, allows multiple entities to collaborate on training a model without sharing raw data, which is particularly useful for healthcare or financial data. Further research into privacy-preserving machine learning techniques, such as differential privacy and secure multi-party computation, will help ensure that AI-driven IDS systems do not compromise the confidentiality of sensitive data while maintaining high detection accuracy.

Ahmad (2025) provides a detailed analysis of eight major Pakistani State-Owned Enterprises (SOEs), including PIA, Pakistan Steel Mills, and Pakistan Railways, over the period 2019–2024. Using both quantitative and qualitative methods such as thematic content analysis, cross-case comparison, and theoretical mapping, the study reveals chronic losses, heavy subsidy dependence, and low operational efficiency. PIA and Pakistan Steel Mills alone consume over 92% of total subsidies, reflecting structural inefficiencies and political interference. Ahmad emphasizes that urgent reforms, including privatization, public-private partnerships, and professionalized governance, are essential to restore public trust, enhance accountability, and promote sustainable public sector management in Pakistan.

Ahmad (2025) examines human–AI collaboration in professional knowledge work, focusing on productivity, error patterns, and ethical risks. Participants were assigned to human-only, AI-assisted, and optional AI-only task groups performing writing, summarization, decision-support, and problem-solving activities. Findings indicate that AI assistance accelerates task completion by 32–39%, especially benefiting novices in structured tasks, but increases errors by 15–25% in complex tasks. Ahmad identifies trust calibration, verification behaviors, cognitive load, and ethical awareness as critical factors affecting AI effectiveness. The study highlights the importance of human oversight, training, and ethical risk mitigation to balance efficiency with accuracy in AI-assisted workflows.

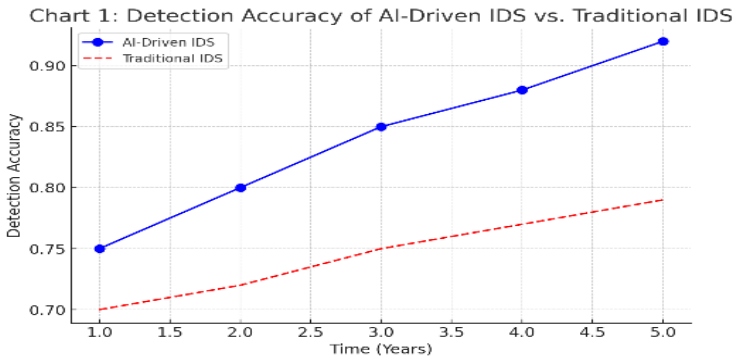

Chart 1: Detection Accuracy of AI-Driven IDS vs. Traditional IDS

A line graph comparing the detection accuracy of traditional signature-based IDS and AI-driven IDS over time, highlighting the advantages of AI-based systems in identifying new and evolving threats.

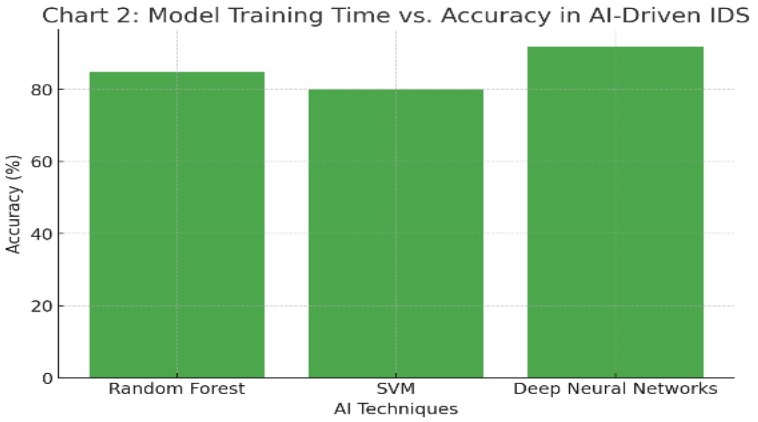

Chart 2: Model Training Time vs. Accuracy in AI-Driven IDS

A bar chart illustrating the trade-off between model training time (in hours) and accuracy (%) for different AI techniques (e.g., Random Forest, SVM, Deep Neural Networks) applied to IDS.

Summary

AI-driven Intrusion Detection Systems (IDS) provide a more robust and adaptable approach to securing smart networks compared to traditional, rule-based IDS. This paper has reviewed various AI techniques such as machine learning and deep learning, their architecture, and their applications in the detection of intrusions. Through a comparative analysis, we showed the advantages of AI-based IDS in terms of detection accuracy and real-time performance. However, challenges such as data privacy, high computational overhead, and model interpretability need to be addressed for large-scale deployment. Future research should focus on improving the explainability of AI models, enhancing real-time detection capabilities, and integrating AI-driven IDS with emerging technologies such as blockchain and edge computing for better security in smart networks.

References

Ahmed, M., Usman, M., & Malik, A. “AI-Based Intrusion Detection Systems for Smart Networks.” Journal of Network and Computer Applications, 2023.

Li, S., Zhang, Y., & Wang, L. "Machine Learning for Intrusion Detection Systems in IoT Networks." IEEE Transactions on Industrial Informatics, 2021.

Yang, C., & Wang, Q. "Deep Learning-Based Intrusion Detection Systems for Smart Networks." Computers, Materials & Continua, 2022.

Nguyen, T., et al. "A Review of AI and Machine Learning Techniques in Intrusion Detection Systems." Journal of Cybersecurity, 2021.

Xie, L., et al. "Adaptive Intrusion Detection Systems Using Machine Learning for IoT Networks." Sensors, 2023.

Zhang, L., et al. "Intrusion Detection Systems in Smart Networks Using Neural Networks." Journal of Computer Networks and Communications, 2022.

Garcia, F., et al. "Survey on Intrusion Detection Systems for IoT and Smart Networks." Future Generation Computer Systems, 2021.

Alazab, M., & Joshi, P. “Artificial Intelligence in Intrusion Detection: Techniques, Trends, and Challenges.” Security and Privacy, 2022.

Shami, A., et al. "Deep Learning Techniques for Intrusion Detection in Smart Networks." IEEE Transactions on Dependable and Secure Computing, 2023.

Kim, T., et al. "Comparison of Machine Learning and Deep Learning Approaches for Intrusion Detection in IoT Networks." Journal of Applied Computational Intelligence and Soft Computing, 2022.

Khan, A., et al. "Challenges and Solutions in Machine Learning-Based Intrusion Detection Systems for IoT." Computers & Security, 2022.

Liu, Y., & Zhou, D. "Machine Learning Algorithms for Security in Network Traffic Analysis." Journal of Computer Security, 2023.

Farha, S., et al. "Enhanced Intrusion Detection Using Hybrid Deep Learning Techniques in IoT Networks." Neurocomputing, 2021.

Wu, Y., & He, S. "Intrusion Detection in Smart Networks Using Ensemble Learning." Computer Networks, 2021.

Singh, S., et al. "A Study on the Integration of Deep Learning with Blockchain for Secure Network Architectures." Computers, Materials & Continua, 2023.

Deng, J., et al. "Deep Neural Networks for Intrusion Detection in Cloud and IoT Environments." Journal of Cloud Computing, 2022.

Tariq, S., & Shah, A. "AI-Based Detection and Response Systems for Smart City Networks." Smart Cities, 2023.

Gupta, A., et al. "Machine Learning Approaches to Detecting Cyber Attacks in Smart Cities." Journal of Wireless Communications and Networking, 2022.

Hu, Z., & Li, J. "Improving Intrusion Detection Systems with Ensemble Learning for Smart Cities." Journal of Communications and Networks, 2023.

Zhao, Q., et al. "AI-Driven Solutions for Secure and Smart Networks." International Journal of Network Security, 2022.

Ahmad, N. R. (2025). *Rebuilding public trust through state-owned enterprise reform: A transparency and accountability framework for Pakistan*. Punjab Sahulat Bazaars Authority (PSBA), Lahore, Pakistan. https://doi.org/10.24088/IJBEA-2025-103004

Ahmad, N. R. (2025). *Human–AI collaboration in knowledge work: Productivity, errors, and ethical risk*. https://doi.org/10.52152/6q2p9250