IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

# A Review of Intelligent Intrusion Detection Systems for Enhancing Cyber Security

**Lakshmi Sudha[1] and Dr. Amit Jain[2]**
[1]Research Scholar, [2]Professor
Department of Computer Science
Sunrise University, Alwar, Rajasthan

**Abstract:** *The rapid expansion of interconnected digital systems, cloud computing, Internet of Things (IoT), mobile networks, and critical information infrastructures has significantly increased the complexity and frequency of cyber threats. Traditional intrusion detection systems (IDS) often rely on predefined signatures and fixed rules, making them less effective against zero-day attacks, polymorphic malware, insider threats, and rapidly evolving attack patterns. Intelligent Intrusion Detection Systems (IIDS) have emerged as an important approach for strengthening cyber security by incorporating artificial intelligence (AI), machine learning (ML), deep learning (DL), and intelligent optimization techniques into the detection process.*

*These systems can analyze large volumes of network and system data, identify abnormal behavior, classify malicious activities, and continuously improve their detection capabilities. This review examines the development, architecture, techniques, datasets, performance measures, applications, and challenges associated with intelligent intrusion detection systems. Particular attention is given to supervised, unsupervised, semi-supervised, and deep learning approaches, including Decision Trees, Random Forest, Support Vector Machines, K-Nearest Neighbors, Artificial Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks, Long Short-Term Memory networks, and ensemble methods.*

**Keywords:** Cyber Security, Artificial Intelligence, Machine Learning, Deep Learning, Network Security, Anomaly Detection, Cyber Attacks.

## I. INTRODUCTION

Cyber security has become a critical requirement because modern organizations increasingly depend on interconnected networks, cloud platforms, Internet of Things devices, mobile applications, and digital services. This extensive connectivity has created a broad attack surface that can be exploited through denial-of-service attacks, malware, ransomware, phishing, botnets, credential attacks, insider threats, and other sophisticated forms of intrusion. An Intrusion Detection System (IDS) is designed to monitor network traffic, host activities, or system events and identify activities that may violate security policies or indicate malicious behavior. Conventional IDS approaches are generally categorized as signature-based and anomaly-based systems. Signature-based systems compare observed activities with known attack patterns and are effective against previously identified threats, whereas anomaly-based systems establish a representation of normal behavior and identify deviations from it.

The continuous evolution of cyber attacks has exposed several limitations of conventional security mechanisms. Attackers increasingly employ obfuscation, encryption, polymorphism, automated exploitation, and evasive techniques that can make predefined signatures ineffective. Intelligent intrusion detection addresses these limitations by using computational intelligence to learn patterns from large-scale security data. Machine learning algorithms can automatically identify relationships among network features and distinguish legitimate traffic from malicious activity. Deep learning extends this capability by learning complex representations from raw or minimally processed data, allowing systems to detect complicated and previously unseen attack patterns.

Intelligent IDS architectures can operate at network, host, application, cloud, and IoT levels. Their functionality generally involves data acquisition, preprocessing, feature extraction or selection, model training, intrusion

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

classification, alert generation, and performance evaluation. The selection of suitable algorithms is influenced by the characteristics of the environment, volume of traffic, availability of labelled data, computational resources, and security requirements. Consequently, there is increasing interest in hybrid and ensemble approaches that combine multiple learning algorithms to improve detection accuracy and robustness.

## II. INTELLIGENT INTRUSION DETECTION TECHNIQUES

Machine learning represents one of the most widely investigated approaches for developing intelligent IDSs. Supervised learning methods use labelled datasets containing examples of normal and malicious activities. Algorithms such as Decision Tree, Random Forest, Support Vector Machine, Naïve Bayes, K-Nearest Neighbors, and Artificial Neural Networks can be trained to classify network connections into different categories. Supervised approaches can provide strong classification performance when representative labelled datasets are available; however, their effectiveness may decrease when new attack types differ substantially from the patterns contained in the training data.

Unsupervised learning techniques do not require complete attack labels and are therefore useful for identifying previously unknown or emerging threats. Clustering, dimensionality reduction, density-based analysis, and autoencoder-based methods can identify unusual patterns in network traffic. Semi-supervised learning combines a limited amount of labelled information with a larger quantity of unlabelled data, providing a potential solution to the expensive process of manually labelling cyber-security datasets.

Deep learning has further expanded the capabilities of intelligent IDSs. Convolutional Neural Networks can identify hierarchical patterns within transformed network features, while Recurrent Neural Networks and Long Short-Term Memory models are particularly suitable for sequential network data. Autoencoders can learn compact representations of normal traffic and detect deviations from these representations. Hybrid models combine different algorithms to exploit complementary strengths, while ensemble learning integrates predictions from several classifiers to improve reliability.

Optimization algorithms can also be incorporated into IIDS frameworks for feature selection and parameter optimization. Techniques such as Genetic Algorithms, Particle Swarm Optimization, and other evolutionary approaches can reduce irrelevant features and improve classification efficiency. The overall objective is to achieve a balance between detection accuracy, computational cost, false-alarm reduction, and adaptability.

## III. DATASETS, FEATURES AND EVALUATION MEASURES

The quality of an intelligent intrusion detection model is strongly influenced by the dataset used during training and evaluation. Earlier studies frequently used datasets such as KDD Cup 1999 and NSL-KDD, while more recent research has increasingly considered datasets such as UNSW-NB15, CICIDS2017, and related contemporary network-traffic collections. These datasets contain combinations of normal traffic and different attack categories and provide features associated with network connections, protocols, packets, flow characteristics, and communication behavior.

Feature selection is an important stage because cyber-security datasets may contain a large number of redundant, irrelevant, or correlated attributes. Common dimensionality-reduction and feature-selection approaches include Principal Component Analysis, Information Gain, correlation analysis, Chi-Square methods, and optimization-based selection. Effective feature selection can reduce computational requirements while maintaining or improving classification performance.

The performance of an IIDS is normally evaluated through several measures rather than accuracy alone. Accuracy indicates the overall proportion of correctly classified observations, while precision measures the proportion of predicted attacks that are actually malicious. Recall or detection rate indicates the ability to identify actual attacks, and the F1-score provides a balance between precision and recall. False Positive Rate is particularly important because excessive false alarms can overwhelm security analysts. The following table summarizes representative intelligent approaches and their characteristics.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

| Intelligent approach | Learning type | Major capability | Common application | Main advantage | Major limitation |
|---|---|---|---|---|---|
| Decision Tree | Supervised | Rule-based classification | Network intrusion detection | Easy to interpret | Can overfit |
| Random Forest | Supervised/Ensemble | Multi-feature classification | Network and host IDS | Robust and accurate | Higher computational cost |
| Support Vector Machine | Supervised | Boundary-based classification | Binary and multiclass IDS | Effective in high-dimensional data | Training can be expensive |
| K-Nearest Neighbors | Supervised | Similarity-based classification | Traffic classification | Simple implementation | Computationally intensive for large datasets |
| Naïve Bayes | Supervised | Probabilistic classification | Fast intrusion detection | Low computational requirement | Assumption of feature independence |
| Artificial Neural Network | Supervised | Nonlinear pattern learning | Network anomaly detection | Learns complex relationships | Requires suitable training data |
| CNN | Deep Learning | Automatic feature representation | Traffic and malware analysis | Strong feature-learning capability | Resource intensive |
| RNN/LSTM | Deep Learning | Sequential pattern analysis | Network-flow and temporal attacks | Captures temporal dependencies | Training complexity |
| Autoencoder | Unsupervised/Semi-supervised | Anomaly representation | Unknown attack detection | Useful with limited labels | Sensitive to training quality |
| Ensemble/Hybrid models | Hybrid | Combines multiple learners | Advanced IDS | Improved robustness | Greater system complexity |

## IV. APPLICATIONS OF INTELLIGENT INTRUSION DETECTION SYSTEMS

Intelligent intrusion detection systems are increasingly applied across diverse cyber-security environments. In enterprise networks, they can monitor communication flows and identify suspicious activities such as port scanning, unauthorized access, denial-of-service attacks, malware communication, and abnormal user behavior. In cloud environments, IIDS technologies can analyze virtual-machine traffic, application behavior, and cloud-service interactions to identify security violations. The dynamic and distributed nature of cloud infrastructures makes adaptive detection particularly valuable.

IoT environments represent another important application area. IoT devices often possess limited processing capacity and may operate with diverse communication protocols, making conventional security solutions difficult to deploy uniformly. Intelligent methods can identify deviations in device behavior and detect coordinated attacks against large numbers of connected devices. Similarly, intelligent IDS approaches can support industrial control systems and critical infrastructure by monitoring operational communication and detecting unusual patterns that may indicate cyber attacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

IIDS technologies are also relevant to wireless and mobile networks, web applications, data centers, and endpoint environments. In Security Operations Centers, intelligent detection can support analysts by prioritizing alerts and identifying relationships among seemingly independent security events. Integration with Security Information and Event Management platforms can enable broader correlation of network, host, application, and authentication data.

## V. CHALLENGES AND RESEARCH GAPS

Despite considerable progress, intelligent intrusion detection continues to face important technical and operational challenges. One major issue is the quality and representativeness of training data. Many benchmark datasets do not fully reproduce the complexity of current operational networks, and models trained on historical data may fail when confronted with new attack techniques or changing traffic patterns. Class imbalance is another important problem because some attacks occur much less frequently than normal traffic, causing models to become biased toward dominant classes.

False positives remain a practical concern. Even a highly accurate system may generate large numbers of incorrect alerts when deployed in a complex environment. Furthermore, deep learning models may require substantial computational resources, making direct deployment difficult on resource-constrained IoT and edge devices. Explainability is also important because security analysts need to understand why a model classified an activity as malicious before taking potentially disruptive action.

Adversarial machine learning introduces another challenge. Attackers may deliberately manipulate input data to evade intelligent detection models or influence their training process. Privacy is also a concern when organizations need to share sensitive network information for centralized model development. Federated learning and privacy-preserving learning therefore represent promising directions. Other research gaps include cross-domain generalization, real-time detection, continual learning, zero-day attack identification, encrypted-traffic analysis, and robust evaluation using realistic operational datasets.

## VI. CONCLUSION

The future development of intelligent intrusion detection systems is likely to focus on adaptive and autonomous security architectures. Continual learning can enable models to update their knowledge as network behavior and attack strategies evolve, reducing dependence on static training datasets. Explainable Artificial Intelligence can improve analyst confidence by providing understandable reasons behind detection decisions. Federated learning can facilitate collaborative model development without requiring organizations to exchange raw security data, potentially improving privacy while increasing the diversity of training information.

Lightweight deep learning and edge-based intelligence are also important for IoT and resource-constrained environments. Hybrid models combining machine learning, deep learning, optimization, and rule-based reasoning may provide stronger detection capabilities than individual techniques. Future systems should also incorporate adversarial robustness so that attackers cannot easily manipulate the detection process. Standardized and realistic evaluation frameworks will be necessary to compare models fairly across different network environments.

Intelligent intrusion detection systems provide an important technological foundation for modern cyber security. The integration of machine learning, deep learning, anomaly detection, ensemble learning, and optimization enables IDSs to move beyond fixed signatures toward adaptive identification of complex and evolving threats. Nevertheless, high detection performance in laboratory datasets does not automatically guarantee reliable real-world deployment. Data quality, false alarms, computational efficiency, explainability, adversarial attacks, privacy, and generalization remain significant challenges. Continued research toward adaptive, lightweight, explainable, privacy-preserving, and robust intelligent IDS architectures can contribute substantially to the protection of increasingly interconnected digital infrastructures.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

## REFERENCES

1. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.
2. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*, 20.
3. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security, 86*, 147–167.
4. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41–50.
5. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access, 5*, 21954–21961.
6. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.
7. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305–316.
8. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 1–6.
9. Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *2015 Military Communications and Information Systems Conference*, 1–6.
10. Ahmad, Z., Shahid Khan, A., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), e4150.