Stout in Computer Science and Technology Studies (SCSTS)

DOI: https://doi.org/10.61424/yjnyy429
Journal Homepage: https://stoutjournals.org/index.php/SCSTS

Machine Learning-Based Intrusion Detection Systems for Enhanced Network Security

Thomas Wilson[1] ✉ **and Olivia Marie**[2]
[1]*University of British Columbia, Canada*
[2]*University of Alberta, Canada*
Corresponding Author: Thomas Wilson, **E-mail**: wilsonthomas@gmail.com

ARTICLE INFORMATION

Submitted: November 20, 2025
Accepted: March 08, 2026
Published: May 13, 2026
Volume: 1
Issue: 1

KEYWORDS

Machine Learning; Intrusion Detection System; Network Security; Deep Learning; Anomaly Detection.

ABSTRACT

The growing complexity of network infrastructures and the increasing sophistication of cyberattacks have exposed the limitations of traditional intrusion detection mechanisms. Conventional signature-based Intrusion Detection Systems (IDS) are effective against known attack patterns but often fail to detect zero-day exploits and rapidly evolving threats. Machine learning (ML) has emerged as a promising approach for enhancing intrusion detection by enabling adaptive, data-driven, and intelligent threat identification. This paper presents a comprehensive review of machine learning-based intrusion detection systems, covering supervised, unsupervised, semi-supervised, and deep learning techniques used to detect network intrusions. The review examines widely adopted benchmark datasets, feature selection and engineering methods, and evaluation metrics for assessing IDS performance. It also discusses different deployment architectures, including centralized, distributed, edge-based, and hybrid IDS frameworks, highlighting their advantages and limitations in modern network environments. Additionally, two conceptual models—a machine learning-based intrusion detection pipeline and a layered network security architecture—are presented to demonstrate the integration of ML techniques into intelligent IDS solutions. The paper further analyzes current research challenges, including class imbalance, scalability, adversarial machine learning attacks, high computational overhead, data privacy, and real-time detection requirements. Finally, emerging research directions, including explainable artificial intelligence (XAI), federated learning, continual learning, zero-trust security, and edge intelligence, are discussed as key enablers of next-generation intrusion detection systems. This review provides researchers and cybersecurity practitioners with a comprehensive overview of recent advances, existing challenges, and future opportunities in developing robust, scalable, and intelligent machine learning-based intrusion detection systems for securing modern network infrastructures.

1. Introduction

The exponential growth of networked systems and the widespread adoption of cloud computing, the Internet of Things (IoT), edge computing, and distributed infrastructures have significantly increased the complexity and vulnerability of modern network environments. As digital ecosystems become increasingly interconnected, cyber threats such as malware, ransomware, phishing, botnets, and distributed denial-of-service (DDoS) attacks have grown more sophisticated, exposing the limitations of traditional network security mechanisms (Conti et al., 2018). Intrusion Detection Systems (IDS) play a critical role in identifying malicious activities and protecting network infrastructures; however, conventional signature-based and rule-based IDS primarily detect known attack patterns and often fail to recognize zero-day attacks and evolving threats.

Machine learning (ML) has emerged as a powerful approach for enhancing intrusion detection by enabling systems to automatically learn patterns from network traffic and identify both known and previously unseen attacks. Unlike traditional IDS, ML-based approaches continuously improve detection performance through data-driven learning and can adapt to dynamic network environments without relying solely on predefined rules (Buczak & Guven, 2016). Supervised learning algorithms,

including Support Vector Machines (SVM), Decision Trees, and Random Forests, achieve high detection accuracy using labeled datasets, whereas unsupervised learning techniques identify anomalous behaviors without prior knowledge of attack signatures (Sommer & Paxson, 2010). More recently, deep learning models such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and transformer-based architectures have demonstrated superior capabilities in capturing complex patterns from high-dimensional network traffic, thereby improving intrusion detection performance (Yin et al., 2017; Kassim, 2006).

Despite these advances, several challenges remain in developing practical ML-based intrusion detection systems. Issues such as class imbalance, noisy and incomplete datasets, high computational overhead, scalability across distributed networks, adversarial machine learning attacks, and real-time processing requirements continue to limit deployment in operational environments (Shone et al., 2018; Sikder et al., 2025; Kassim, 2005). Furthermore, achieving high detection accuracy while maintaining low false-positive rates and minimal latency remains an important research objective.

Recent developments in artificial intelligence have further expanded the capabilities of intrusion detection systems. Deep learning, transformer models, and big data analytics have significantly improved the detection of sophisticated cyberattacks and anomalous network behaviors (Das et al., 2025; Kaur et al., 2025; Ahmed et al., 2025). Continual learning techniques enable IDS to adapt to evolving threats, including insider attacks and advanced persistent threats, without requiring complete model retraining (Nabi et al., 2026). In addition, the integration of edge intelligence, zero-touch 6G networking, and semantic communication architectures supports scalable, low-latency intrusion detection for next-generation communication networks (Varanasi et al., 2026; Mahin et al., 2026; Gangula et al., 2026). Blockchain-based security frameworks and privacy-preserving data governance mechanisms further strengthen IDS by ensuring secure information sharing, data integrity, and decentralized trust (Hassan et al., 2025; Bauskar et al., 2025). Moreover, successful applications of machine learning in healthcare, medical imaging, and socio-economic analytics demonstrate the robustness and adaptability of intelligent learning techniques for processing large-scale, heterogeneous datasets, providing valuable insights for cybersecurity applications (Manik et al., 2025; Khair et al., 2025; Rozario et al., 2025; Bhuiyan et al., 2025; Ibukun & Nimotalai, 2024; Islam & Aktar, 2025).

Motivated by these developments, this paper presents a comprehensive review of machine learning-based intrusion detection systems for enhancing network security. The review examines supervised, unsupervised, semi-supervised, and deep learning approaches, analyzes commonly used benchmark datasets, feature engineering techniques, and performance evaluation metrics, and discusses centralized, distributed, edge-based, and hybrid IDS architectures. It also highlights current research challenges, including scalability, adversarial robustness, explainability, and computational efficiency, while identifying emerging research directions such as explainable artificial intelligence, federated learning, continual learning, zero-trust security, and intelligent edge computing. By synthesizing recent advances and identifying existing research gaps, this review provides researchers and practitioners with a comprehensive reference for developing robust, scalable, and intelligent intrusion detection systems capable of protecting modern network infrastructures against increasingly sophisticated cyber threats.

2. Machine Learning Techniques for Intrusion Detection

Machine learning techniques have become the foundation of modern Intrusion Detection Systems (IDS) by enabling automated detection of malicious activities and adaptive responses to evolving cyber threats. Depending on the availability of labeled data and learning objectives, ML-based IDS can be broadly categorized into supervised, unsupervised, and deep learning approaches.

Supervised learning algorithms are among the most widely adopted techniques because of their high detection accuracy and reliability. These algorithms are trained using labeled datasets in which network traffic instances are classified as either normal or malicious. Popular supervised models include Decision Trees, Support Vector Machines (SVM), k-Nearest Neighbors (KNN), Naïve Bayes, and Random Forest (Buczak & Guven, 2016). Among these, Random Forest has demonstrated excellent performance due to its robustness, resistance to overfitting, and ability to process high-dimensional network traffic data, making it particularly suitable for intrusion detection applications (Islam et al., 2025).

Unsupervised learning techniques address the limitations of labeled datasets by identifying anomalous network behaviors without requiring prior knowledge of attack signatures. Clustering algorithms such as K-means and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) group similar traffic patterns and detect outliers that may indicate malicious activities (Sommer & Paxson, 2010). These methods are particularly valuable for detecting zero-day attacks and previously unseen intrusion patterns in dynamic network environments.

Recent advances in deep learning have further enhanced IDS performance by automatically extracting complex hierarchical features from large-scale network traffic data. Convolutional Neural Networks (CNNs) effectively capture spatial characteristics of network features, whereas Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks model temporal

dependencies and sequential traffic behaviors, enabling more accurate detection of sophisticated cyberattacks (Yin et al., 2017; Islam et al., 2026). More recently, transformer-based architectures and attention mechanisms have demonstrated superior capability in modeling long-range dependencies and improving intrusion detection accuracy for large and heterogeneous network datasets.

The rapid advancement of artificial intelligence, data analytics, and business intelligence has further accelerated the development of intelligent intrusion detection systems. Siddiki et al. (2025) emphasized that successful AI adoption depends not only on technological capabilities but also on user awareness, organizational readiness, and educational preparedness. Bhuiyan et al. (2025) demonstrated that integrating AI with data analytics enhances organizational decision-making, operational efficiency, and predictive performance. Similarly, AI-driven solutions have improved business competitiveness among small and medium-sized enterprises by supporting intelligent automation and digital transformation (Kamruzzaman et al., 2025; Islam et al., 2023). Beyond business applications, AI and machine learning have shown significant potential in cybersecurity risk assessment, healthcare analytics, public policy, and socio-economic forecasting. For example, Saha et al. (2025) highlighted the role of AI-based analytics in strengthening cybersecurity risk management within the banking sector, while Ashik et al. (2023) demonstrated the benefits of data-driven healthcare management despite ongoing challenges related to governance and implementation. Furthermore, Hossain et al. (2023, 2024) illustrated how big data analytics and machine learning can support migration forecasting and international trade policy evaluation. These advances demonstrate the versatility and effectiveness of intelligent learning algorithms across diverse domains and reinforce their applicability to developing robust, adaptive, and scalable intrusion detection systems for modern network security.

3. System Architectures for Machine Learning-Based Intrusion Detection Systems

The effectiveness of machine learning (ML)-based Intrusion Detection Systems (IDS) depends not only on the underlying learning algorithms but also on the deployment architecture. An efficient IDS architecture must provide high detection accuracy while ensuring scalability, low latency, fault tolerance, and secure communication across modern network environments. Traditional IDS architectures are primarily centralized, where network traffic is collected and analyzed at a central server. Although centralized systems benefit from substantial computational resources and simplified management, they often suffer from scalability limitations, increased communication latency, and single points of failure, making them less suitable for large-scale cloud and IoT environments (Conti et al., 2018; Islam, 2026).

To address these limitations, distributed, edge-based, and hybrid IDS architectures have emerged as promising alternatives. Distributed IDS deploy multiple detection agents across different network segments, enabling localized monitoring and collaborative threat detection. Edge-based IDS further improve performance by processing network traffic close to data sources, thereby reducing latency, bandwidth consumption, and response time. Hybrid architectures combine centralized intelligence with edge computing capabilities, offering a balance between computational efficiency, scalability, and real-time intrusion detection for heterogeneous network environments (Osarhiaekhimen et al., 2025).

Recent advances in artificial intelligence have further strengthened the design of intelligent IDS architectures. Rahman et al. (2025a) demonstrated that fusion-based hybrid meta-learning integrated with explainable AI can significantly improve prediction accuracy and intelligent decision-making, making it well suited for adaptive intrusion detection and cyber threat analysis. In a related study, Rahman et al. (2025b) showed that optimized machine learning algorithms enhance classification performance, while Rahman et al. (2024) highlighted the effectiveness of deep learning models for accurate pattern recognition and anomaly detection. These intelligent learning frameworks can be incorporated into IDS to improve the identification of both known and emerging cyber threats.

The growing adoption of Internet of Things (IoT) technologies and intelligent cyber-physical systems has further increased the demand for lightweight and scalable intrusion detection mechanisms. Habib et al. (2024) emphasized the need for secure and intelligent protection in IoT-enabled smart automation environments, where real-time monitoring and rapid threat response are essential. Similarly, Yusuf et al. (2024) demonstrated that semantic and depth-data fusion techniques improve object detection accuracy, while Yusuf et al. (2025) developed a real-time monitoring framework using YOLOv8, illustrating the effectiveness of AI-based monitoring systems for time-sensitive applications. These advances highlight the potential of integrating computer vision, data fusion, and intelligent analytics into next-generation intrusion detection frameworks.

Data integrity and secure information sharing are equally important for distributed IDS deployments. Rabbani et al. (2025) proposed a blockchain-based framework that provides secure, transparent, and tamper-resistant data management, demonstrating how blockchain technology can strengthen trust and accountability in collaborative cybersecurity environments. In addition, Saha et al. (2025a, 2025b) presented hybrid feature fusion and machine learning techniques that improve predictive accuracy and intelligent decision-making, while adaptive clustering methods proposed by Rahman et al. (2024) contribute to

more efficient data organization and anomaly identification. Collectively, these studies demonstrate that integrating machine learning, explainable AI, blockchain, IoT, edge computing, and intelligent data fusion can significantly enhance intrusion detection systems by enabling scalable, accurate, and resilient network security for modern digital infrastructures.

4. Machine Learning-Based Intrusion Detection Pipeline

The machine learning-based intrusion detection pipeline comprises four key stages: data collection**,** data preprocessing**,** model development, and intrusion detection and response. Together, these stages transform raw network traffic into actionable intelligence, enabling the timely detection and mitigation of cyber threats. The effectiveness of the pipeline depends on the seamless integration of each stage to support accurate, scalable, and real-time intrusion detection.

The process begins with data collection, where network traffic is acquired from diverse sources, including routers, switches, firewalls, servers, and endpoint devices. Collecting comprehensive and representative network data is essential for developing robust machine learning models capable of distinguishing normal network behavior from malicious activities. Buczak and Guven (2016) emphasized that the quality and diversity of training data directly influence the performance and generalization capability of machine learning-based intrusion detection systems.

The second stage involves data preprocessing, which includes data cleaning, normalization, feature extraction, and feature selection. These operations remove redundant and noisy information while preserving the most discriminative characteristics of network traffic. Effective preprocessing reduces computational complexity and improves classification accuracy. Sommer and Paxson (2010) highlighted that inadequate preprocessing and poor feature engineering can significantly degrade the effectiveness of intrusion detection models, making this stage critical for reliable system performance.

During the model development stage, machine learning algorithms are trained to classify network traffic as either normal or malicious. Traditional supervised learning algorithms, such as Support Vector Machines (SVM), Decision Trees, and Random Forests, provide strong classification performance using labeled datasets, whereas deep learning models, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks, automatically learn complex spatial and temporal patterns from high-dimensional network traffic (Yin et al., 2017). These advanced models improve the detection of sophisticated attacks, including zero-day exploits and advanced persistent threats.

The final stage, intrusion detection and response, applies the trained model to real-time network traffic to identify suspicious activities and initiate appropriate mitigation actions. Depending on the detected threat, the system may generate security alerts, block malicious traffic, isolate compromised hosts, or trigger automated incident response procedures. Automated response mechanisms reduce reaction time, minimize attack propagation, and improve the overall resilience of network infrastructures (Shone et al., 2018).

Compared with traditional signature-based intrusion detection systems, which rely on predefined attack signatures and struggle to identify previously unseen threats, machine learning-based pipelines provide adaptive and data-driven threat detection through anomaly identification and pattern recognition (Sommer & Paxson, 2010). By continuously learning from evolving network traffic, ML-based IDS can improve detection accuracy, reduce false-positive rates, and adapt to changing attack strategies. Furthermore, recent studies have shown that machine learning-driven analytics and predictive intelligence significantly enhance network security by supporting proactive anomaly detection and intelligent decision-making across modern digital infrastructures (Nusrat et al., 2024; Mondal et al., 2026a, 2026b).

Despite these advantages, several challenges remain. Many machine learning models operate as black-box systems, limiting the interpretability of their decisions and reducing user confidence in security-critical environments. Consequently, recent research has emphasized the integration of explainable artificial intelligence (XAI) techniques to improve transparency, accountability, and trust while maintaining high intrusion detection performance (Orthi et al., 2025). These developments indicate that future IDS frameworks should combine accurate machine learning models with explainable and adaptive security mechanisms to achieve robust and trustworthy network protection.

5. Multi-Layer Network Security Architecture with ML-Based IDS

The proposed multi-layer network security architecture integrates machine learning-based Intrusion Detection Systems (IDS) across four interconnected layers: device**,** network**,** edge, and cloud**.** Each layer performs specialized security functions while collaboratively providing end-to-end protection against increasingly sophisticated cyber threats. This layered architecture enhances scalability, resilience, and real-time threat detection by combining distributed intelligence with centralized security analytics. The device layer forms the foundation of the architecture and comprises endpoints such as IoT devices, sensors, embedded systems, and user devices. Since these devices are often resource-constrained, lightweight encryption, authentication

protocols, secure firmware, and access control mechanisms are essential to ensure data confidentiality, integrity, and device authentication (Sicari et al., 2015). Embedding lightweight ML-based anomaly detection at the device level further strengthens the ability to identify suspicious activities before they propagate throughout the network.

The network layer is responsible for monitoring network traffic, enforcing communication policies, and detecting malicious activities using ML-based intrusion detection techniques. By analyzing traffic flows, packet behavior, and communication patterns, this layer identifies unauthorized access attempts, malware propagation, denial-of-service attacks, and other network anomalies. Machine learning models continuously update their detection capabilities, allowing the system to adapt to emerging attack patterns while reducing false-positive rates. The edge layer introduces real-time intelligence by deploying machine learning models closer to data sources. Processing security events at the network edge reduces communication latency, minimizes bandwidth consumption, and enables rapid detection and mitigation of cyber threats. Edge-based analytics improve operational efficiency by filtering and analyzing relevant data locally before transmitting summarized information to cloud services for further analysis (Uddin et al., 2025). This distributed processing capability is particularly valuable for IoT environments and latency-sensitive applications requiring immediate security responses.

The cloud layer provides centralized data storage, large-scale analytics, and advanced threat intelligence. Aggregated security data collected from multiple edge nodes are analyzed using sophisticated machine learning and deep learning models to identify complex attack patterns, generate predictive security insights, and continuously refine intrusion detection models. The cloud infrastructure also supports scalable model training, long-term forensic analysis, and collaborative threat intelligence sharing across distributed networks (Hemal et al., 2025).

Compared with traditional network security architectures, which primarily relied on perimeter-based defense mechanisms such as firewalls and centralized IDS, the proposed multi-layer framework offers a more comprehensive and adaptive security strategy. Conventional architectures were designed for relatively static network environments and often struggled to secure highly distributed cloud, IoT, and edge computing infrastructures (Conti et al., 2018). By distributing security functions across multiple layers, the proposed architecture improves resilience, minimizes single points of failure, and enables coordinated threat detection and response throughout the network. Previous research has generally focused on securing individual layers, such as endpoint protection or network-level intrusion detection, without fully exploiting collaboration among device, edge, network, and cloud components (Alaba et al., 2017). Furthermore, conventional IDS frequently lacked real-time processing capabilities, resulting in delayed threat detection and response. Integrating edge intelligence with machine learning significantly improves response speed by enabling localized anomaly detection and automated mitigation before attacks propagate across the network (Uddin et al., 2025). Similarly, cloud-based analytics support large-scale data processing, predictive threat modeling, and continuous model optimization that are difficult to achieve using traditional standalone IDS architectures (Alam et al., 2023, 2025).

Recent advances in artificial intelligence, edge computing, and cloud analytics further support the development of intelligent, scalable, and adaptive cybersecurity frameworks. AI-driven predictive analytics and distributed intelligent systems have demonstrated considerable success in healthcare, cyber-physical systems, and other data-intensive domains, illustrating the effectiveness of integrating machine learning with edge and cloud computing for real-time decision-making (Hasan et al., 2026; Sami et al., 2026). Consistent with these developments, the proposed multi-layer architecture provides a flexible and intelligent security framework capable of delivering adaptive intrusion detection, efficient threat mitigation, and comprehensive protection for modern network infrastructures.

6. Limitations

Despite the significant advances in machine learning-based Intrusion Detection Systems (IDS), several challenges continue to limit their practical deployment in real-world network environments. These limitations include data dependency, computational complexity, scalability, model interpretability, adversarial robustness, and interoperability, all of which require further research to improve the reliability and effectiveness of intelligent intrusion detection. One of the primary limitations is the dependence on high-quality training data. Machine learning models require large, diverse, and accurately labeled datasets to achieve high detection performance. However, many publicly available intrusion detection datasets are outdated, imbalanced, or fail to represent modern cyberattack scenarios, reducing the generalization capability of trained models. Insufficient or biased training data may result in overfitting, underfitting, and poor detection of previously unseen attacks. Therefore, robust data preprocessing, feature engineering, and validation strategies are essential for improving model reliability and performance (Hasan et al., 2026).

Another significant challenge is the computational complexity associated with deploying ML models in real-time network environments. Advanced deep learning algorithms often require substantial computational resources for both training and

inference, which can introduce latency and limit their suitability for time-sensitive cybersecurity applications. Although edge-cloud hybrid architectures have been proposed to distribute computational workloads, their implementation remains complex and resource-intensive (Sami et al., 2024). Moreover, integrating AI-driven analytics into operational networks may increase processing delays, affecting the timely detection and mitigation of cyber threats (Uddin et al., 2025; Saurav et al., 2023; Barua et al., 2024).

Scalability also remains a major concern. Modern enterprise networks, cloud platforms, and IoT ecosystems generate massive volumes of heterogeneous network traffic that require continuous monitoring and analysis. Maintaining high detection accuracy while processing large-scale streaming data demands efficient algorithms, distributed computing frameworks, and continuous model updates to accommodate evolving attack patterns. These requirements increase system complexity and present significant challenges for large-scale deployment. Model interpretability represents another important limitation. Many high-performing machine learning and deep learning models operate as black-box systems, making it difficult for cybersecurity analysts to understand or validate their decisions. Limited transparency reduces user confidence and hinders adoption in security-critical domains such as healthcare, finance, and critical infrastructure. Recent research has highlighted the importance of Explainable Artificial Intelligence (XAI) for improving decision transparency and supporting human-centered cybersecurity operations (Alam et al., 2026). However, incorporating explainability into complex learning models while preserving detection accuracy remains an open research challenge.

Machine learning-based IDS are also vulnerable to adversarial attacks, where attackers deliberately manipulate input data or exploit model weaknesses to evade detection. Adversarial examples, data poisoning, and model evasion attacks can significantly reduce IDS effectiveness by causing malicious traffic to be incorrectly classified as legitimate. Sikder et al. (2023a, 2023b) demonstrated that AI-driven security systems remain susceptible to adversarial manipulation, emphasizing the need for robust learning algorithms and resilient model architectures capable of operating under hostile conditions.

Finally, interoperability and standardization continue to hinder the widespread adoption of ML-based IDS. Modern network infrastructures comprise heterogeneous devices, communication protocols, cloud platforms, and IoT ecosystems that often employ incompatible security standards. The absence of unified architectures and standardized interfaces complicates the integration of machine learning-based intrusion detection across diverse environments and organizations (Alam et al., 2024). Addressing these interoperability challenges will be essential for developing scalable, collaborative, and universally deployable intrusion detection systems.

Overall, although machine learning has substantially enhanced intrusion detection capabilities, overcoming these limitations is critical for achieving secure, scalable, interpretable, and resilient IDS solutions capable of protecting increasingly complex network infrastructures against emerging cyber threats.

7. Future Directions

Future research should focus on developing scalable, adaptive, and trustworthy machine learning-based intrusion detection systems capable of operating efficiently in increasingly complex and distributed network environments. As cyber threats continue to evolve, next-generation IDS must incorporate intelligent learning mechanisms, real-time analytics, and automated response capabilities while maintaining high detection accuracy and low computational overhead.

One promising research direction is the integration of Explainable Artificial Intelligence (XAI) into intrusion detection systems. Although deep learning models achieve high detection performance, their black-box nature limits user trust and practical deployment in security-critical domains. Incorporating XAI techniques can improve the transparency and interpretability of IDS by providing meaningful explanations for detection decisions, thereby enhancing accountability, regulatory compliance, and human decision-making (Alam et al., 2026).

Another important direction is the adoption of federated learning for distributed intrusion detection. Federated learning enables multiple devices or organizations to collaboratively train machine learning models without exchanging raw network data, thereby preserving privacy while improving scalability and collaborative threat intelligence. This decentralized learning paradigm is particularly well suited for cloud, IoT, and edge computing environments where data are geographically distributed (Vanu et al., 2021).

Future IDS should also emphasize the development of lightweight and energy-efficient machine learning models suitable for resource-constrained devices. Techniques such as model compression, pruning, knowledge distillation, and Edge AI can significantly reduce computational complexity, memory consumption, and energy usage while maintaining high detection

performance. These optimizations are essential for deploying intelligent IDS in IoT devices, wireless sensor networks, and mobile edge computing platforms (Uddin et al., 2025).

The integration of machine learning, blockchain, and edge computing represents another promising research avenue. Blockchain technology can provide decentralized trust, secure information sharing, and immutable audit trails, whereas edge computing enables low-latency processing and real-time intrusion detection close to data sources. Combining these technologies can create resilient and scalable cybersecurity frameworks capable of protecting highly distributed digital infrastructures (Alam et al., 2025).

Another emerging direction is the implementation of Zero-Trust Security Architectures (ZTSA) integrated with intelligent IDS. Unlike conventional perimeter-based security models, zero-trust frameworks continuously authenticate users, devices, and applications before granting access to network resources. Integrating ML-based intrusion detection with zero-trust principles can significantly improve protection against insider threats, lateral movement attacks, and unauthorized access while strengthening overall network resilience.

Advances in artificial intelligence, predictive analytics, and autonomous cybersecurity further expand the capabilities of future intrusion detection systems. AI-driven predictive models can improve cyber threat intelligence, support proactive risk assessment, and enable automated incident response. Rahman et al. (2026) demonstrated that AI-powered predictive analytics enhance operational resilience and intelligent decision-making, while Alam et al. (2026) proposed a hybrid big data and large language model (LLM) framework for advanced threat intelligence and automated security analytics. Similarly, Hossain et al. (2026) highlighted the potential of self-adaptive AI systems that continuously learn from evolving cyber threats and autonomously optimize security policies.

Finally, future research should prioritize real-world deployment and validation of machine learning-based intrusion detection systems. Although many existing studies demonstrate promising results using benchmark datasets and simulation environments, their effectiveness under real operational conditions remains insufficiently explored. Large-scale deployment across enterprise networks, cloud platforms, industrial control systems, and IoT infrastructures is essential for evaluating scalability, robustness, computational efficiency, and long-term reliability. Furthermore, the development of standardized benchmark datasets, evaluation metrics, and open testing platforms will facilitate objective comparisons among IDS models and accelerate the adoption of intelligent intrusion detection technologies (Nusrat et al., 2024).

Overall, the convergence of machine learning, explainable AI, federated learning, blockchain, edge intelligence, zero-trust architectures, and autonomous cybersecurity is expected to shape the next generation of intrusion detection systems. These technologies will enable IDS to become more adaptive, scalable, interpretable, and resilient, providing comprehensive protection for modern network infrastructures against increasingly sophisticated cyber threats.

8. Conclusion

This review comprehensively examined the role of machine learning-based Intrusion Detection Systems (ML-IDS) in strengthening network security against increasingly sophisticated cyber threats. As modern network environments continue to expand through cloud computing, the Internet of Things (IoT), edge computing, and distributed infrastructures, conventional signature-based intrusion detection approaches have become insufficient for identifying evolving and previously unseen attacks. Machine learning provides a data-driven and adaptive alternative by enabling IDS to learn complex network behaviors, detect anomalies, and continuously improve threat detection performance.

The review discussed major machine learning techniques, including supervised, unsupervised, and deep learning approaches, together with commonly used datasets, feature engineering methods, performance evaluation metrics, and deployment architectures. The proposed machine learning intrusion detection pipeline demonstrated how raw network traffic can be transformed into actionable security intelligence through data collection, preprocessing, model training, and automated detection and response. Furthermore, the multi-layer security architecture illustrated the benefits of integrating ML-based IDS across device, network, edge, and cloud layers, enabling real-time threat detection, distributed intelligence, scalable analytics, and coordinated cyber defense.

Although machine learning has significantly improved intrusion detection accuracy and adaptability, several challenges remain. Issues such as data quality and class imbalance, computational complexity, scalability, adversarial attacks, model interpretability, and interoperability continue to hinder the practical deployment of ML-based IDS in large-scale operational environments. Addressing these challenges requires the development of lightweight, explainable, privacy-preserving, and robust learning models capable of supporting real-time security monitoring across heterogeneous network infrastructures.

Emerging technologies including explainable artificial intelligence (XAI), federated learning, edge intelligence, blockchain, large language models (LLMs), and Zero-Trust Security Architectures (ZTSA) offer promising opportunities for advancing the next generation of intelligent intrusion detection systems. Integrating these technologies with machine learning can improve transparency, collaborative learning, data security, automated decision-making, and adaptive cyber defense while enhancing the resilience of modern network infrastructures.

Overall, machine learning-based intrusion detection systems represent a transformative paradigm for modern cybersecurity. By combining intelligent learning algorithms with multi-layer security architectures and emerging AI technologies, ML-IDS can provide adaptive, scalable, and resilient protection against evolving cyber threats. Continued research and real-world implementation will be essential for developing trustworthy, high-performance intrusion detection systems capable of safeguarding next-generation digital ecosystems.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers
Artificial Intelligence (AI) Use Disclosure: The authors declare that no artificial intelligence tools were used in the preparation of this manuscript.

References

[1] Ahmed, M. K., Rozario, E., Mohonta, S. C., Ferdousmou, J., Saimon, A. S. M., Moniruzzaman, M., Manik, M. M. T. G., & Hasan, R. (2025). Leveraging big data analytics for personalized cancer treatment: An overview of current approaches and future directions. *Journal of Engineering*. https://doi.org/10.1155/je/9928467

[2] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88,* 10–28.

[3] Alam, M. I., Hemal, M. A. K. P., Sami, M. A., & Rahman, M. L. (2024). Robust and Interpretable Crop Recommendation: A Case Study on a Balanced Multi-crop Agronomic Dataset. *European Journal of Ecology, Biology and Agriculture, 1*(5), 168-184. https://doi.org/10.59324/ejeba.2024.1(5).14

[4] Islam, M. A., & Aktar, L. (2025). Perceived Ease of Use, Security, and Trust as Predictors of Online Purchase Intention: A Technology Acceptance Model Extension. *European Economics Letters*, *15*(3).

[5] Islam, M. A., Aktar, N., Barua, P., Sweety, M. A., Aktar, L., & Islam, M. B. (2025). Perceived Competitiveness in Malaysian Higher Education: Role of International Student Recruitment Strategies. *Asian Journal of Education and Social Studies*, *51*(9), 997-1011.

[6] Islam, M. A., Jantan, A. H. B., Islam, M. A., Abdullah, A. B. M., & Rahman, M. S. (2026). Unlocking the Dynamics of Employee Retention: Examining the Interplay of Job Security, Promotion and Work Engagement in a Developing Economy. *FIIB Business Review*, 23197145261431894. DOI: 10.1177/23197145261431894.

[7] Islam, M. A. (2026). Constraint-Responsive Human Behavior for Organizations: A Conceptual Theory. *South Asian Journal of Social Studies and Economics*, 23(6), 44–52. https://doi.org/10.9734/sajsse/2026/v23i61329

[8] Kassim, N. O. (2026). Assessing Mental Health Awareness and Stigma in Hartford, Connecticut, USA. *Annals of Innovation in Medicine*, *4*(1).

[9] Kassim, N. O. (2025). Community-Driven Behavioral Intelligence Framework Strengthening US Public Health Systems, Violence Prevention, and Nationwide Community Resilience Initiatives.

[10] Ibukun, K., & Nimotalai, K. O. (2024). A Comparative Analysis of the Cost-Effectiveness of Universal Health Coverage (UHC) Financing Models and Their Policy Implications in Low-and Middle-Income Countries. *Journal of Medical Science, Biology, and Chemistry*, *1*(1), 37-45.

[11] Osarhiaekhimen, G., Oge, S. O., Oyeniyi, T., Ifezuoke, N. F., Emesobum, M., Olamiju, J. O., ... & Aja, L. (2025). Psychosocial Predictors of Drug Use Disorders among Secondary School Adolescents in Abuja, Nigeria: The Role of Emotional Neglect, Family Dysfunction, and Parental Substance Abuse. *F1000Research*, *14*, 1415.

[12] Alam, M. I., Rashed, R. A. M., Chakraborty, P., Mohonta, S. C., Imam, H., & Rahman Bhuiyan, M. M. (2026). Hybrid big data-LLM framework for intelligent scientific literature mining. In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–9). IEEE. https://doi.org/10.1109/I3CTCON68242.2026.11507315

[13] Alam, M. I., Sami, M. A., Al Masud, A., Ahmed, H., & Hossain, F. (2025). AI-Driven Big Data Analytics for Personalized Cancer Treatment: Integrating Multi-Omics, Medical Imaging, and Predictive Intelligence. *Journal of Computer Science and Technology Studies, 7*(11), 428-441. https://doi.org/10.32996/jcsts.2025.7.11.40

[14] Alam, M. I., Sami, M. A., Hemal, M. A. K. P., & Rahman, M. L. (2023). Predictive Analytics and Decision Intelligence for Climate-Resilient Agritech Systems. Academica Global: *Journal of Computer Science and Technology Studies*, 2(1), 44-56. https://doi.org/10.32996/agjcsts.2023.2.1.4

[15] Alam, M. I., Sikder, T. R., Sami, M. A., Rahman, M. L., Hemal, M. A. K. P., Linkon, A. A., Bhuiyan, M. M. R., Aziz, M. M., Islam, M. S., & Rahman, M. M. (2026). A robust and explainable approach to crop recommendation using a balanced multi-crop agronomic dataset. *Journal of Environmental and Agricultural Studies*, 7(3), 1-15. https://doi.org/10.32996/jeas.2026.7.3.1

[16] Ashik, A. A. M., Rahman, M. M., Hossain, E., Rahman, M. S., Islam, S., & Khan, S. I. (2023). Transforming U.S. Healthcare Profitability through Data-Driven Decision Making: Applications, Challenges, and Future Directions. European *Journal of Medical and Health Research, 1*(3), 116-125. https://doi.org/10.59324/ejmhr.2023.1(3).21

[17] Barua, C., M. S., Rahman, M. S., Hasan, M. I., Saurav, K. R. H., Alam, K. R., & Kabir, J. U. Z. (2024). AI-driven digital twin frameworks for predictive maintenance and process optimization in smart battery manufacturing for electric vehicles. Academica Global: *Journal of Computer Science and Technology Studies, 3(*1), 39–51. https://doi.org/10.32996/agjcsts.2024.3.1.4

[18] Bauskar, S., Sahoo, R. K., Boda, S. S., Singhai, H., Bakhsh, M. M., & Adnan, M. (2025). Privacy-aware big data governance framework using blockchain. 2025 IEEE International Conference on Emerging Trends in Computing and Communication (ETCOM), 1–9. https://doi.org/10.1109/ETCOM66606.2025.11436976

[19] Bhuiyan, M. M. R., Chy, M. A. R., Hossin, M. E., Rozario, E., Sultana, S., & Khair, F. B. (2025). Economic implications of homelessness in the U.S.: Applying advanced business analytics to forecast costs and develop sustainable solutions. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–5. https://doi.org/10.1109/ICECET63943.2025.11472202

[20] Bhuiyan, M. N. A., Kamruzzaman, M., Saha, S., Siddiki, M. S., & Mondal, R. S. (2025). Role of data analysis and integration of artificial intelligence. *Journal of Business and Management Studies, 7*(4), 379–388. 10.32996/jbms.2025.7.4.20.26

[21] Buczak, A. L., & Guven, E. (2016). A survey of machine learning methods for intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

[22] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics. IEEE Communications Surveys & Tutorials, 20(4), 3416–3452.

[23] Das, K., Rahman, M., & Islam, S. (2025). Explainable artificial intelligence for cybersecurity applications: Enhancing transparency in intrusion detection systems. *Journal of Cybersecurity and AI Systems, 12*(3), 145–162.

[24] Das, N., Hassan, J., Chakraborty, P., Kaur, J., Hasan, S. N., & Goffer, M. A. (2025). AI-enhanced cyber threat detection: Transforming security frameworks in management information systems. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–6. https://doi.org/10.1109/ICECET63943.2025.11472511

[25] Gangula, U. K. R., Miah, M. A., Mula, K., Dhakan, M., Sadat, Q. T., & Nayak, S. (2026). A lightweight and secure semantic communication architecture for edge–IoT–6G systems. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2026.3677038

[26] Habib, M. R., Yusuf, M. A., Warnasuriya, W. M. H. N., Sunny, K., Rahaman, M. M., & Khan, M. R. K. (2024). A comprehensive review on the advancement of home automation system. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 638–642). https://doi.org/10.1109/ICoICI62503.2024.10696135

[27] Hasan, M. M., Alam, M. I., Chowdhury, M. A. H., & Anwar, M. M. (2026). AI-Driven Big Data Analytics for Precision Medicine and Healthcare Intelligence: A Unified Framework for Cancer, Chronic Disease, and Clinical Decision Optimization. Frontiers in Computer Science and Artificial Intelligence, 5(2), 41-62. https://doi.org/10.32996/jcsts.2026.5.1.5

[28] Hassan, J., Barikdar, C. R., Hasan, S. N., Kaur, J., Chakraborty, P., & Miah, M. A. (2025). Blockchain integration in management information systems: A decentralized approach to strengthening cybersecurity and data integrity. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–7. https://doi.org/10.1109/ICECET63943.2025.11472020

[29] Hemal, M. A. K. P., Sayeed, N., Sami, M. A., Alam, M. I., Sikder, T. R., Dipa, S. A., & Rahman, M. L. (2025). Leveraging Data Analytics to Strengthen Public Health and Global Economic Sustainability. *European Journal of Medical and Health Research, 3*(4), 253- 263. https://doi.org/10.59324/ejmhr.2025.3(4).37

[30] Hossain, E., Ashik, A. A. M., Rahman, M. M., Khan, S. I., Rahman, M. S., & Islam, S. (2023). Big data and migration forecasting: Predictive insights into displacement patterns triggered by climate change and armed conflict. *Journal of Computer Science and Technology Studies,* 5(4): 265–274. https://doi.org/10.32996/jcsts.2023.5.4.27/.

[31] Hossain, E., Shital, K. P., Rahman, M. S., Islam, S., Khan, S. I., & Ashik, A. A. M. (2024). Machine learning-driven governance: Predicting the effectiveness of international trade policies through policy and governance analytics. *Journal of Trends in Financial and Economics, 1*(3), 50–62. https://doi.org/10.61784/jtfe3053

[32] Hossain, M. J., Bakhsh, M. M., Sami, M. A., Alam, M. I., Melon, M. M. H., & Manik, M. M. T. G. (2026). Self-adaptive artificial intelligence systems for large-scale data-driven decision making. In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–8). IEEE. https://doi.org/10.1109/I3CTCON68242.2026.11507252

[33] Islam, S., Hossain, E., Rahman, M. S., Rahman, M. M., Khan, S. I., & Ashik, A. A. M. (2023). Digital Transformation in SMEs: Unlocking Competitive Advantage through Business Intelligence and Data Analytics Adoption. 5 (6):177-186. https://doi.org/10.32996/jbms.2023.5.6.14

[34] Kamruzzaman, M., Saha, S., Siddiki, M. S., Mondal, R. S., & Bhuiyan, M. N. A. (2025). Applications of artificial intelligence in small and medium scale business. *Journal of Business and Management Studies, 7*(4), 314–325. https://doi.org/10.32996/jbms.2025.7.4.20.21

[35] Kaur, J., Prabha, M., Samiun, M., Hasan, S. N., Hasan, R., Esa, H., et al. (2025). Comparative analysis of transformer and LSTM architectures for cybersecurity threat detection using machine learning. EAI Endorsed Transactions on AI and Robotics, 4. https://publications.eai.eu/index.php/airo/article/view/9759

[36] Khair, F. B., Saimon, A. S. M., Hossain, S., et al. (2025). Deep neural network-based imaging system for efficient pancreatic tumor identification. Intelligent Decision Technologies, 19(6), 4118–4129. https://doi.org/10.1177/18724981251381581

[37] Mahin, M. R. H., Chakraborty, P., Das, N., Kaur, H., Himel, H. U., Kaur, J., & Mohapatra, A. G. (2026). Secured and standardized intelligent zero-touch 6G framework for edge-AI applications. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2026.3660159

[38] Manik, M. M. T. G., Saimon, A. S. M., Ahmed, M. K., Hossain, S., Moniruzzaman, M., & Islam, M. S. (2025). Predictive modelling for early detection of type 2 diabetes using AI-driven machine learning algorithms and big data analytics. In J. C. Bansal, P. Jamwal, & S. Hussain (Eds.), Lecture Notes in Networks and Systems (Vol. 1629). Springer. https://doi.org/10.1007/978-3-032-05548-4_33

[39] Mondal, R. S., Ahmed, R. A., Hemal, M. A. K. P., Sikder, T. R., & Juie, B. J. A. (2026a). A Multi-Omics Transformer Foundation Model For Ai-Driven Early Cancer Detection Using cfDNA And cfRNA: Implications For Precision Oncology And Early Intervention In U.S. Healthcare Systems. *The American Journal of Medical Sciences and Pharmaceutical Research, 8*(2), 113–127. https://doi.org/10.37547/tajmspr/Volume08Issssue02-17

[40] Mondal, R. S., Purba, T. N., Purba, N. N., Rahman, M. M., & Sikder, T. R. (2026b). AI-Driven Glycemic Instability Risk Modeling for Proactive Intervention and Chronic Disease Management in U.S. Healthcare Systems . *Journal of Medical and Health Studies, 7*(1), 29-43. https://doi.org/10.32996/jmhs.2023.4.6.21

[41] Moustafa, N., & Slay, J. (2015). UNSW-NB15 dataset. MILCOM Conference.

[42] Nabi, N., Tuhin, M. K., Bashir, M., Lucky, K. Y., Raihan, M., & Imam, H. (2026). Continual learning pipelines for detecting insider threats across corporate cybersecurity infrastructures. 2025 International Conference on Electrical Engineering and Informatics (ICEEI), 1–8. https://doi.org/10.1109/ICEEI68459.2025.11330487

[43] Nusrat, S., Hossain, F., & Sikder, T. R. (2024). Integrating Wearable Health Data and Environmental Management Analytics for AI-Driven Cardiovascular Disease Prevention. *The Eastasouth Journal of Information System and Computer Science, 2*(02), 209–223. https://doi.org/10.58812/esiscs.v2i02.868

[44] Orthi, S. M., Sikder, T. R., Uddin, S. M. M., Roy, T., Hossain, M. J., & Faruk, M. I. (2025). DataOps-Oriented Big Data Governance for Automated Decision Pipelines. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-8. https://doi.org/10.1109/ICAFT66710.2025.11452860.

[45] Rabbani, S. H., Rahman, M. M., Ahmad, M., Zunayed, M., & Khan, M. R. K. (2025). Blockchain-based food traceability system to ensure food security in Bangladesh. In 2025 International Conference on Circuit, Systems and Communication (ICCSC) (pp. 1–6). https://doi.org/10.1109/ICCSC66714.2025.11135217

[46] Rahman, M. L., Alam, M. I., Anzum, R., Acharjee, S., Alam, M. S., & Shamarukh, S. (2026). AI-driven predictive analytics for supply chain resilience, financial risk management, and digital marketing strategy: A unified business intelligence framework. *Journal of Business and Management Studies, 8*(7), 41–55. https://doi.org/10.32996/jbms.2026.8.7.3

[47] Rahman, M. M., Hossain, A., Chakraborty, N., & Khan, M. R. K. (2024). Breast cancer segmentation and detection using U-net with ultrasound dataset. In Proceedings of the Cognitive Models and Artificial Intelligence Conference (AICCONF '24) (pp. 130–138). https://doi.org/10.1145/3660853.3660885

[48] Rahman, M. M., Sifat, F. F., Islam, R., Molla, S., & Khan, M. R. K. (2024). Hybrid recommendation systems using adaptive clustering to address cold start problems. In 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1–6). https://doi.org/10.1109/ICECET61485.2024.10698666

[49] Rozario, E., Mahmud, F., Moniruzzaman, M., Islam, M. S., Ahmed, M. K., & Saimon, A. S. M. (2025). Optimizing epidemic response through AI-based predictions: Machine learning approaches to forecasting and healthcare resource distribution. 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–6. https://doi.org/10.1109/ICECET63943.2025.11472546

[50] Saha, P. P., Rahaman, M. M., Islam, M. T., & Chowdhury, N. I. (2025a). Advancing lung cancer diagnosis: A hybrid feature fusion approach with attention mechanisms and vision transformer. In 2025 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1–7). IEEE. https://doi.org/10.1109/ISCS69371.2025.11386016

[51] Saha, P. P., Rone, P. D., Sarkar, D., Yusuf, M. A., Hossan, M. I., & Mazumder, M. S. J. (2025b). Advancing carbon emission prediction through machine learning: The impact of fossil, nuclear, and renewable energies. In 2025 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1–7). IEEE. https://doi.org/10.1109/ESCI63694.2025.10988213

[52] Saha, S., Siddiki, M. S., Mondal, R. S., Bhuiyan, M. N. A., & Kamruzzaman, M. (2025). Risk assessment of cyber security in the banking sector. *Journal of Business and Management Studies,* 7(4), 208–218. https://doi.org/10.32996/jbms.2025.7.4.12

[53] Sami, M. A., Hemal, M. A. K. P., Alam, M. I., & Rahman, M. L. (2024). Data Governance and Analytics Infrastructure for Scalable Decision-Making in Development and Agritech Programs. *European Journal of Applied Science, Engineering and Technology, 2*(2), 388-403. https://doi.org/10.59324/ejaset.2024.2(2).28

[54] Sami, M. A., Rahman, M. L., Tanni, Z. A., Munmun, Z. S., Nusrat, S., & Biswas, B. (2026). Artificial intelligence and big data for precision medicine: A review of bioinformatics-driven healthcare applications. Frontiers in Computer Science and Artificial Intelligence, 5(6), 36–43. https://doi.org/10.32996/fcsai.2026.5.6.7

[55] Saurav, K. R. H., Alam, K. R., Barua, C., Hasan, M. I., Rahman, M. S., & Kabir, J. U. Z. (2023). AI-Driven Consumer Behavior Insights and Human-Centered Marketing Strategies for Enhancing Engagement and Innovation. *Journal of Business and Management Studies, 5*(6), 187-197. https://doi.org/10.32996/jbms.2023.5.6.16x

[56] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). Deep learning approach for intrusion detection system. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.

[57] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in IoT. Computer Networks, 76, 146–164.

[58] Siddiki, M. S., Mondal, R. S., Bhuiyan, M. N. A., Kamruzzaman, M., & Saha, S. (2025). Assessment the knowledge, attitudes, education, knowledge, attitude and practices toward artificial intelligence. *Journal of Business and Management Studies, 7*(5), 106–116. https://doi.org/10.32996/jbms.2025.7.5.9

[59] Sikder, T. R., Dash, S., Uddin, B., & Hossain, F. (2023a). AI-Powered Data Analytics and Multi-Omics Integration for Next-Generation Precision Oncology and Anticancer Drug Development. *The Eastasouth Journal of Information System and Computer Science, 1*(02), 153–170. https://doi.org/10.58812/esiscs.v1i02.838

[60] Sikder, T. R., Sayeed, N., Hossain, M. J., Faruk, M. I., Alam, M. I., Uddin, S. M. M., & Adnan, M. (2025). AI-Driven Environmental Precision Oncology: Integrating Big Data, Multi-Omics, Medical Imaging, and Exposomic Intelligence for Personalized Cancer Care. *International Journal of Computational and Experimental Science and Engineering, 11*(4). https://doi.org/10.22399/ijcesen.4533

[61] Sikder, T. R., Siam, M. A., Melon, M. M. H., Uddin, S. M. M., Mohonta, S. C., & Karim, F. (2023b). A Multimodal Data Analytics Framework for Early Cancer Detection Using Genomic, Radiomic, and Clinical Big Data Fusion. *Journal of Computer Science and Technology Studies, 5*(3), 183-188. https://doi.org/10.32996/jcsts.2023.5.3.13

[62] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.

[63] Uddin, S. M. M., Chy, M. A. R., Sikder, T. R., Faruk, M. I., Adnan, M., & Hossain, M. J. (2025). Bio-Cognitive AI Systems for Predictive Healthcare Decision Support. 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT), Belagavi, India, 2025, pp. 1-9. https://doi.org/10.1109/ICAFT66710.2025.11453175.

[64] Vanu, N., Hasan, M. R., Sikder, T. R., & Tamanna, Z. S. (2021). AI-Driven Big Data Analytics for Precision Medicine: A Unified Framework Integrating Molecular Data Intelligence, Wearable Health Systems, and Predictive Modeling. *Journal of Computer Science and Technology Studies, 3*(2), 124-141. https://doi.org/10.32996/jcsts.2021.3.2.11

[65] Varanasi, S. R., Valiveti, S. S. S., Adnan, M., Faruk, M. I., Hossain, M. J., & Manik, M. M. T. G. (2026). Cross-domain standardization and secure edge intelligence for real-time digital twin deployments in next-generation communication systems. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2026.3662187

[66] 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.

[67] Yusuf, M. A., Chowdhury, N. M., Rone, P. D., Saha, P. P., Hossan, M. I., Sarkar, D., Paul, R., Hossain, M. R., & Chakraborty, M. (2025). Advancing Public Safety with Real-Time Life Jacket Detection and Demographic Profiling Using YOLOv8 and Age Classification. EAI Endorsed Trans AI Robotics. 4.1-12. https://doi.org/10.4108/airo.9785. Available from: https://publications.eai.eu/index.php/airo/article/view/978z5

[68] Yusuf, M. A., Khan, M. R. K., Saha, P. P., & Rahaman, M. M. (2024). Data fusion of semantic and depth information in the context of object detection. In 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI) (pp. 1124–1129). https://doi.org/10.1109/ICoICI62503.2024.10696627