The Eastasouth Journal of Information System and Computer Science
Vol. 4, No. 01, August 2026, pp. 29-42
ISSN: 3025-566X, DOI: 10.58812/esiscs.v4i01

A Machine Learning-Based Intrusion Detection Framework for Enhanced Network Security

Ranobir Hasan[1], Hira Jamal[2], Kamal[3], Khan[4], Amit Kumar[5], Antu Roy[6]
[1,2,3,4,5,6] Department of Computer Application, National University, Gazipur, Bangladesh

Article Info

Article history:

Received July, 2026
Revised July, 2026
Accepted Aug, 2026

Keywords:

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

ABSTRACT

The rapid expansion of interconnected networks, cloud computing, Internet of Things (IoT) devices, and digital communication technologies has significantly increased the complexity of modern cyber threats, making traditional network security mechanisms increasingly inadequate. Intrusion Detection Systems (IDS) are essential components of cybersecurity infrastructures, designed to monitor network activities and identify malicious behavior before it compromises system integrity. However, conventional signature-based and rule-based IDS are primarily effective against previously known attack patterns and often fail to detect zero-day attacks, advanced persistent threats (APTs), and other evolving cyber threats. To address these limitations, machine learning (ML) has emerged as a transformative technology that enables adaptive, intelligent, and data-driven intrusion detection by learning complex patterns from network traffic and system behavior. This review presents a comprehensive analysis of machine learning-based intrusion detection systems, covering a wide range of techniques including supervised learning, unsupervised learning, ensemble learning, and deep learning models. The paper examines widely used benchmark datasets, feature selection and feature engineering methods, data preprocessing techniques, and commonly adopted performance evaluation metrics for assessing intrusion detection effectiveness. It also reviews various IDS deployment architectures, including centralized, distributed, edge-based, cloud-enabled, and hybrid frameworks, highlighting their strengths and limitations in different networking environments. To provide a clear understanding of intelligent intrusion detection mechanisms, the review introduces two conceptual frameworks: a machine learning-based intrusion detection pipeline that illustrates the end-to-end process from data acquisition to threat classification, and a layered network security architecture demonstrating the integration of ML techniques into modern cybersecurity infrastructures. Furthermore, the paper discusses critical challenges affecting the deployment of ML-based IDS, including data imbalance, scalability, computational complexity, model interpretability, adversarial machine learning attacks, privacy preservation, and real-time processing constraints.

Corresponding Author:

Name: Amit Kumar
Institution: Department of Computer Application, National University, Gazipur, Bangladesh.
Email: evankd375@gmail.com

1. INTRODUCTION

The exponential growth of interconnected network infrastructures, together with the widespread adoption of cloud computing, the Internet of Things (IoT), edge computing, software-defined networking (SDN), and distributed cyber-physical systems, has fundamentally transformed modern communication environments. While these technological advancements have improved connectivity, scalability, and service delivery, they have also expanded the attack surface, making network infrastructures increasingly vulnerable to sophisticated cyber threats. Cyberattacks such as malware, ransomware, phishing, botnets, advanced persistent threats (APTs), insider attacks, and distributed denial-of-service (DDoS) attacks continue to evolve in complexity and frequency, posing significant risks to data confidentiality, system availability, and organizational operations [1].

Intrusion Detection Systems (IDS) constitute a fundamental component of network security architectures by continuously monitoring network traffic and identifying malicious activities before they compromise system integrity. Traditional IDS primarily employ signature-based and rule-based detection mechanisms that compare observed traffic against predefined attack signatures or manually crafted security rules. Although these approaches remain effective for detecting previously known attacks, they exhibit limited capability in identifying zero-day exploits, polymorphic malware, and rapidly evolving attack strategies. Their reliance on static knowledge bases significantly reduces their adaptability to dynamic network environments, resulting in increased false negatives and delayed threat detection [2]. To overcome these limitations, machine learning (ML) has emerged as a transformative technology for intelligent intrusion detection. Unlike conventional approaches, ML-based IDS automatically learn behavioral patterns from historical and real-time network traffic, enabling adaptive detection of both known and previously unseen attacks without requiring explicitly defined signatures. Through data-driven learning, machine learning models continuously improve their detection capability, making them well suited for protecting modern heterogeneous network environments characterized by rapidly changing cyber threats [2].

The unsupervised learning approaches, such as k-means clustering, hierarchical clustering, and density-based algorithms, identify anomalies by discovering hidden structures within unlabeled data, making them particularly valuable for detecting previously unknown attack patterns [3]. Recent advances in deep learning have further enhanced the effectiveness of intrusion detection systems by enabling automatic feature extraction and hierarchical pattern recognition from high-dimensional network data. Deep learning architectures including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and Transformer-based models can capture complex temporal and spatial relationships within network traffic that are often difficult to identify using conventional machine learning techniques. Yin et al. [4] demonstrated that deep learning models significantly improve intrusion detection accuracy while reducing the need for extensive manual feature engineering. Nevertheless, these models require substantial computational resources, extensive training datasets, and careful hyperparameter optimization, presenting practical challenges for real-time deployment.

Furthermore, machine learning models are susceptible to adversarial attacks in which carefully crafted inputs manipulate model predictions or evade detection mechanisms, reducing system robustness and reliability [5]. Real-world implementation additionally requires careful consideration of computational latency, resource utilization, model updating strategies, and deployment scalability across distributed network environments [6]. Recent research has

demonstrated substantial improvements in intrusion detection through the integration of advanced artificial intelligence techniques. Deep learning, big data analytics, ensemble learning, transformer-based architectures, and graph neural networks have significantly enhanced the capability of IDS to detect sophisticated cyberattacks and complex network anomalies [7], [8], [9]. Continual learning approaches further strengthen IDS by enabling adaptive model updates that continuously learn from evolving attack behaviors, thereby improving resilience against insider threats and emerging attack vectors across large-scale infrastructures [10]. Similarly, zero-touch 6G communication frameworks, semantic communication architectures, and distributed AI models facilitate scalable, low-latency intrusion detection suitable for next-generation communication networks [11], [12], [13]. These technologies support real-time monitoring while reducing dependence on centralized cloud infrastructures, thereby improving both efficiency and resilience.

Blockchain-based architectures strengthen trust, ensure data integrity, and facilitate secure information sharing among distributed security entities. Complementary privacy-preserving data governance frameworks further improve compliance, transparency, and collaborative cybersecurity analytics while protecting sensitive organizational information [14], [15]. Predictive analytics, intelligent medical diagnosis, image analysis, financial forecasting, socio-economic modeling, and decision support systems have successfully employed advanced AI algorithms to analyze complex, high-dimensional datasets with remarkable accuracy [16], [17], [18], [19].

This review paper aims to provide a comprehensive analysis of machine learning-based intrusion detection systems by examining their underlying methodologies, learning paradigms, system architectures, benchmark datasets, feature engineering techniques, evaluation metrics, and practical deployment challenges. The review synthesizes recent advances in artificial intelligence, deep learning, blockchain, edge intelligence, and privacy-preserving technologies while identifying existing research gaps and future opportunities.

2. MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION

During training, the models learn discriminative patterns that enable them to accurately classify previously unseen network activities. Commonly used supervised learning algorithms include Decision Trees (DT), Support Vector Machines (SVM), k-Nearest Neighbors (KNN), Naïve Bayes (NB), Random Forest (RF), Logistic Regression (LR), and Gradient Boosting methods [2]. Among these, Random Forest has gained widespread popularity because of its robustness, resistance to overfitting, and ability to process high-dimensional cybersecurity data efficiently. Clustering algorithms such as K-means, Density-Based Spatial Clustering of Applications with Noise (DBSCAN), Hierarchical Clustering, and Gaussian Mixture Models group similar observations together while identifying data instances that significantly deviate from normal behavior as potential intrusions [3].

Convolutional Neural Networks (CNNs) are widely employed to extract spatial features from network packets and flow records, whereas Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks effectively capture sequential and temporal dependencies in network traffic, enabling accurate detection of evolving attack behaviors [4]. Siddiki et al. [20] emphasize that the successful adoption of AI depends not only on technological infrastructure but also on organizational readiness, user knowledge, educational background, trust, and willingness to engage with intelligent systems. Likewise, Bhuiyan et al. [21] demonstrate that integrating AI with advanced data analytics substantially improves organizational performance by

enhancing decision accuracy, predictive capabilities, operational efficiency, and strategic planning.

Within the business sector, particularly among small and medium-sized enterprises (SMEs), AI-powered analytics have become valuable tools for optimizing business operations, reducing operational costs, improving customer engagement, and strengthening competitive advantage [22]. Similarly, Islam et al. [23] report that the integration of business intelligence and data analytics accelerates digital transformation by enabling organizations to make data-driven decisions, improve resource utilization, and enhance organizational resilience in increasingly competitive markets.

The applications of AI and advanced analytics extend well beyond commercial environments. In the financial sector, Saha et al. [24] demonstrate that machine learning and predictive analytics significantly improve cybersecurity risk assessment by identifying vulnerabilities, detecting fraudulent activities, and strengthening institutional security frameworks. Within healthcare, AI-driven analytics improve clinical decision-making, operational efficiency, patient outcome prediction, and healthcare resource management while simultaneously introducing important challenges related to data governance, interoperability, privacy, and ethical AI deployment [25], [26], [27]. Furthermore, big data analytics has become an important tool for addressing broader societal challenges. Hossain et al. [28] show that predictive analytics can support policymakers in forecasting migration patterns associated with climate change, economic instability, and geopolitical conflicts, while Hossain et al. [29] demonstrate that machine learning techniques can evaluate international trade policies and provide valuable insights for evidence-based governance and economic planning.

3. SYSTEM ARCHITECTURES FOR ML-BASED IDS

Centralized architectures benefit from substantial computational resources and simplified model management, enabling the deployment of complex machine learning and deep learning algorithms. However, they also suffer from several limitations, including increased communication latency, bandwidth consumption, limited scalability, and vulnerability to single points of failure. As network size and traffic volume continue to grow, centralized systems may struggle to meet the real-time requirements of modern cybersecurity environments [1].

Recent advances in artificial intelligence have further strengthened IDS architectures by integrating intelligent perception, adaptive analytics, and real-time monitoring technologies. Yusuf et al. [30] proposed semantic and depth-data fusion techniques that improve feature representation and object detection accuracy through multimodal data integration. Although developed for intelligent vision applications, these multimodal fusion methodologies provide valuable insights for intrusion detection systems by demonstrating how heterogeneous data sources can be effectively combined to improve anomaly detection and situational awareness. Similarly, Yusuf et al. [31] developed a real-time monitoring framework based on the YOLOv8 deep learning architecture for public safety applications, illustrating the capability of AI-powered systems to perform rapid event detection with high computational efficiency.

Machine learning architectures have also benefited from advances in adaptive learning and intelligent data processing. Rahman et al. [32] introduced adaptive clustering techniques that dynamically organize complex datasets according to evolving data characteristics, providing improved scalability and flexibility for intelligent analytical systems. Likewise, Saha et al. [33] demonstrated the effectiveness of advanced machine learning techniques for

predictive analytics, while Saha et al. [34] proposed hybrid feature fusion methods that significantly enhance classification performance by integrating complementary feature representations.

Recent developments in explainable artificial intelligence (XAI) and hybrid learning frameworks have further expanded the capabilities of intelligent intrusion detection systems. Rahman et al. (2025) demonstrated that fusion-based hybrid meta-learning models combined with explainable AI significantly improve predictive performance and intelligent decision-making. Their comparative evaluation of multiple machine learning algorithms, together with U-Net-based detection architectures, highlights the effectiveness of AI-driven models for complex pattern recognition, anomaly detection, and automated threat classification. Integrating explainability into IDS architectures not only improves prediction accuracy but also increases transparency, enabling cybersecurity analysts to understand and validate automated security decisions more effectively.

Secure communication and trustworthy data management have become equally important considerations in modern IDS architectures. Rabbani et al. [35] introduced blockchain-based security frameworks that provide decentralized, immutable, and transparent mechanisms for maintaining data integrity, authenticating network transactions, and securely sharing cybersecurity information across distributed environments. The rapid expansion of IoT-enabled smart environments has further increased the demand for intelligent and scalable intrusion detection solutions. Habib et al. [36] emphasized that interconnected smart automation systems continuously exchange sensitive information through heterogeneous communication networks, making them attractive targets for increasingly sophisticated cyberattacks.

4. MACHINE LEARNING-BASED INTRUSION DETECTION PIPELINE

Traditional intrusion detection systems primarily relied on signature-based methods, which detect attacks by matching predefined patterns. While effective for known threats, these systems fail to identify new or evolving attacks [3]. In contrast, the machine learning-based pipeline in Figure 1 enhances detection capabilities by leveraging anomaly detection and pattern recognition. This integrated approach ensures that data flows seamlessly through the system, enabling real-time threat detection. Also, Drawing on Nusrat et al. [37] and Mondal et al. [38], [39], machine learning-based intrusion detection systems enhance network security through analytics, anomaly detection, and predictive intelligence across digital infrastructures.

Furthermore, traditional IDS systems often suffer from high false positive rates and limited adaptability. Machine learning models address these issues by continuously learning from new data and adapting to changing network conditions [6]. Deep learning models, in particular, have shown significant improvements in detecting complex and previously unseen attack patterns [4]. However, ML-based IDS are not without limitations. Many models operate as “black boxes,” making it difficult to interpret their decisions. Recent studies suggest that incorporating explainable AI techniques can improve transparency and trust in these systems [40].

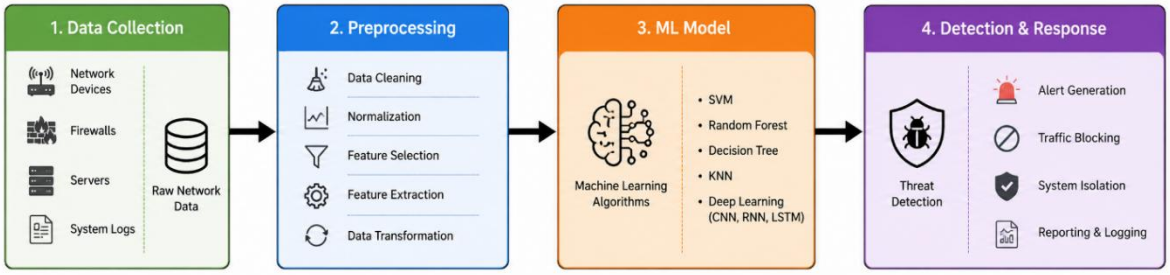

Figure 1. Machine Learning-Based Intrusion Detection Pipeline

The effectiveness of any machine learning-based intrusion detection system largely depends on the quality, diversity, and representativeness of the collected data. Comprehensive data acquisition enables learning algorithms to recognize complex behavioral patterns associated with both legitimate and malicious activities, thereby improving detection accuracy and generalization performance [2]. Sommer and Paxson [3] emphasize that inadequate preprocessing and poor feature selection can significantly reduce the effectiveness of intrusion detection systems, making this stage one of the most critical components of the overall pipeline. The third stage focuses on machine learning model development, where intelligent algorithms are trained to distinguish normal network behavior from malicious activities. Depending on the application, supervised, unsupervised, semi-supervised, or deep learning techniques may be employed. Supervised learning algorithms such as Support Vector Machines (SVM), Decision Trees, Random Forest, Gradient Boosting, and Artificial Neural Networks learn from labeled datasets to classify network traffic accurately. Unsupervised learning methods identify anomalous behavior without requiring predefined attack labels, making them valuable for detecting previously unknown cyber threats. Deep learning models, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) networks, Autoencoders, and Transformer-based architectures, further enhance intrusion detection by automatically extracting hierarchical features from complex network traffic and learning long-term temporal dependencies. Yin et al. [4] demonstrated that deep learning techniques significantly outperform conventional machine learning models in detecting sophisticated cyberattacks and previously unseen intrusion patterns.

The final stage, threat detection and automated response, utilizes the trained machine learning model to analyze incoming network traffic in real time and identify potential intrusions. Once suspicious activities are detected, the system automatically initiates appropriate mitigation strategies, including security alert generation, malicious traffic blocking, connection termination, user authentication, quarantine of compromised devices, and system isolation. Automated response mechanisms substantially reduce detection-to-response latency, limiting the spread and impact of cyberattacks while improving the overall resilience of network infrastructures. Shone et al. [6] emphasize that integrating intelligent response mechanisms with intrusion detection significantly enhances operational efficiency and minimizes damage caused by rapidly evolving cyber threats.

Furthermore, machine learning significantly reduces one of the major limitations of traditional intrusion detection systems—the high false positive rate. Conventional IDS often generate excessive security alerts, increasing analyst workload and reducing operational efficiency. Machine learning algorithms continuously refine their decision boundaries using newly observed network behavior, improving classification performance while minimizing false alarms. Shone et al. [6] report that adaptive learning models provide substantially greater

flexibility and robustness than static rule-based systems, particularly in large-scale enterprise networks. Deep learning models further strengthen intrusion detection by identifying complex, nonlinear relationships within high-dimensional network traffic that conventional algorithms frequently fail to capture [4].

Recent advances in artificial intelligence continue to enhance machine learning-based intrusion detection systems through predictive analytics, anomaly detection, and intelligent cyber defense. Drawing on the findings of Nusrat et al. [37] and Mondal et al. [38], [39], AI-driven intrusion detection frameworks combine advanced analytics, adaptive learning, and predictive intelligence to improve network monitoring across modern digital infrastructures. Recent research therefore emphasizes the integration of Explainable Artificial Intelligence (XAI) techniques to improve model interpretability, transparency, and accountability. Explainable AI enables cybersecurity analysts to understand why specific network activities are classified as malicious, facilitating more informed decision-making and increasing confidence in automated intrusion detection systems [40].

5. MULTI-LAYER NETWORK SECURITY ARCHITECTURE WITH ML-BASED IDS

The proposed multi-layer network security architecture, illustrated in Figure 2, is organized into four interconnected layers: Device Layer, Network Layer, Edge Layer, and Cloud Layer. Each layer performs specialized security functions while collaboratively providing comprehensive protection against cyber threats in modern network environments. This layered architecture enables distributed security management, intelligent threat detection, and adaptive response across heterogeneous network infrastructures.

The Device Layer forms the foundation of the architecture and consists of endpoints such as IoT sensors, user devices, embedded systems, and other resource-constrained network components. Since these devices typically possess limited computational and storage capabilities, lightweight security mechanisms including encryption, authentication, secure firmware, and integrity verification are employed to safeguard sensitive information and prevent unauthorized access. Implementing efficient security protocols at this layer is essential for ensuring data confidentiality, integrity, and device authenticity while minimizing computational overhead [41].

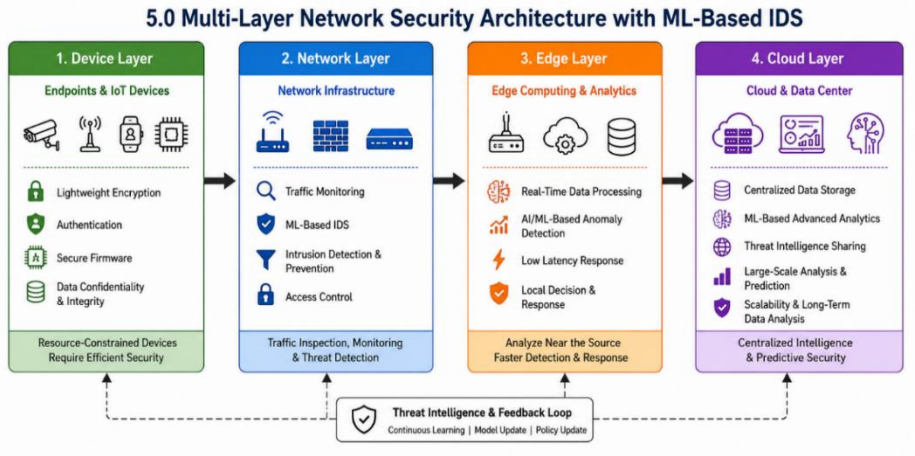

Figure 2. Multi-Layer Network Security Architecture with Machine Learning-Based Intrusion Detection System (ML-Based IDS)

The Edge Layer introduces intelligent, real-time data processing by deploying artificial intelligence (AI) and machine learning (ML) models closer to data sources. Instead of transmitting all network traffic to centralized servers, edge computing enables local analysis and anomaly detection, significantly reducing communication latency and accelerating cyber threat response. By processing relevant information at the network edge, this layer improves detection accuracy, minimizes bandwidth consumption, and supports rapid containment of security incidents, making it particularly suitable for IoT environments, industrial control systems, and time-sensitive applications [42]. In addition, cloud-based infrastructures facilitate long-term security analytics, collaborative threat intelligence sharing, model retraining, and scalable deployment of AI-driven cybersecurity solutions, thereby enhancing the overall resilience of the network [43].

Traditional network security architectures primarily relied on perimeter-based defense mechanisms, where security functions were concentrated within a single layer using technologies such as firewalls or centralized intrusion detection systems. Although these approaches performed adequately in relatively static network environments, they are increasingly ineffective against the distributed, dynamic, and heterogeneous nature of modern communication networks [1]. In contrast, the proposed multi-layer architecture distributes security intelligence across multiple interconnected layers, enabling coordinated monitoring, analysis, and response throughout the entire network infrastructure.

Earlier studies typically focused on isolated security mechanisms, such as endpoint protection or network-level intrusion detection, without adequately considering the interactions among different architectural layers [44]. Furthermore, conventional IDS architectures often lacked real-time processing capabilities, resulting in delayed intrusion detection and slower incident response. The incorporation of an intelligent Edge Layer addresses these limitations by enabling localized anomaly detection, low-latency processing, and immediate response to cyber threats, thereby substantially improving overall detection efficiency and system resilience [42]. Similarly, the integration of cloud-based analytics supports large-scale data aggregation, predictive threat intelligence, and continuous machine learning model optimization, capabilities that were largely absent from earlier intrusion detection frameworks [45], [46].

Recent advances in artificial intelligence, edge computing, and cloud analytics further demonstrate the importance of integrating distributed intelligence within cybersecurity architectures. Studies have shown that combining AI-powered analytics, edge intelligence, and cloud computing enables scalable, adaptive, and intelligent security frameworks capable of supporting critical applications such as healthcare, smart cities, industrial Internet of Things (IIoT), and other cyber-physical systems [47], [48].

6. LIMITATIONS

Despite the significant advances in machine learning-based intrusion detection systems (ML-based IDS), several technical and operational challenges continue to limit their effectiveness in real-world network environments. Hasan et al. [47] emphasize that data-driven cybersecurity models require robust preprocessing, feature engineering, and validation techniques to ensure reliable and accurate intrusion detection. Inadequate data representation may result in overfitting or underfitting, ultimately reducing detection accuracy and increasing false alarm rates. Integrating AI-driven analytics into operational cybersecurity platforms may therefore introduce processing latency, potentially delaying threat detection and automated response. Such delays are particularly problematic in mission-critical applications where immediate mitigation is

essential to prevent service disruption and data compromise [42], [49], [27].

To address these limitations, researchers have proposed hybrid architectures that combine edge computing with cloud-based analytics. Edge computing enables localized processing of network traffic, reducing communication latency and enabling faster anomaly detection, while cloud platforms provide centralized storage, large-scale data analytics, and continuous model retraining. Although hybrid architectures improve scalability and detection performance, their deployment remains technically challenging due to resource management, communication overhead, synchronization requirements, and infrastructure complexity [50].

Model interpretability represents another major concern in intelligent intrusion detection systems. Many advanced machine learning and deep learning algorithms operate as "black-box" models whose internal decision-making processes are difficult for cybersecurity analysts to understand. This lack of transparency reduces user confidence, complicates forensic investigations, and limits the adoption of AI-driven IDS in highly regulated sectors such as healthcare, finance, and critical infrastructure. Recent studies advocate the integration of Explainable Artificial Intelligence (XAI) to improve model transparency by providing interpretable explanations for intrusion detection decisions [51], [52].

Machine learning-based IDS are also vulnerable to adversarial machine learning attacks. Cyber attackers can deliberately manipulate network traffic by generating carefully crafted adversarial inputs that mislead learning algorithms into classifying malicious activities as legitimate network behavior. These attacks significantly reduce the reliability of intrusion detection systems and expose critical network infrastructures to undetected cyber threats. Sikder et al. [53], [54] demonstrated that AI-driven cybersecurity systems are susceptible to adversarial manipulation, emphasizing the necessity for robust adversarial training, secure model architectures, and resilient learning strategies capable of resisting malicious perturbations. The absence of standardized data formats, communication protocols, interoperability frameworks, and architectural guidelines limits the seamless integration of ML-based IDS across heterogeneous organizational infrastructures [55].

7. FUTURE DIRECTIONS

One of the most promising research directions is the integration of Explainable Artificial Intelligence (XAI) into intrusion detection systems. Although deep learning models have demonstrated outstanding detection performance, their "black-box" nature often limits user trust and practical deployment in security-critical domains. XAI techniques improve transparency by providing interpretable explanations for model predictions, enabling cybersecurity analysts to understand why specific network activities are classified as malicious. Enhanced interpretability facilitates forensic analysis, supports regulatory compliance, and increases confidence in automated decision-making, particularly within healthcare, finance, industrial control systems, and other mission-critical infrastructures where accountability is essential [56], [52]. This decentralized training paradigm preserves privacy, reduces communication overhead, and complies with increasingly stringent data protection regulations. Federated learning is particularly suitable for Internet of Things (IoT) ecosystems, edge computing environments, and geographically distributed enterprise networks where sensitive security information cannot be centrally aggregated [57].

Techniques such as model compression, network pruning, knowledge distillation, quantization, and edge AI optimization can substantially improve computational efficiency without significantly compromising predictive

performance. These optimization strategies enable intelligent intrusion detection to be deployed directly on edge devices, supporting low-latency security monitoring and real-time cyber defense [42]. Together with cloud-based analytics for large-scale threat intelligence, these technologies create resilient and scalable intrusion detection frameworks capable of protecting modern distributed infrastructures [46]. These adaptive capabilities substantially improve cyber resilience, operational continuity, and recovery performance following security incidents. Rahman et al. [58] demonstrated that AI-powered predictive analytics enhances resilience and operational decision-making within digital ecosystems, while Hossain et al. [59] emphasized the importance of self-adaptive artificial intelligence for continuous learning, autonomous system management, and improved cybersecurity performance. Similarly, Alam et al. [60] proposed a hybrid big data and large language model (LLM) framework capable of supporting advanced threat intelligence, automated security analytics, and intelligent decision support for modern cybersecurity applications.

Another emerging research area is the application of Large Language Models (LLMs) and Generative AI to intrusion detection and cyber threat intelligence. LLMs can assist security analysts by automatically summarizing security events, interpreting alerts, correlating attack patterns, generating incident reports, and supporting interactive cybersecurity decision-making. Integrating generative AI with traditional machine learning models offers significant opportunities for improving situational awareness, security automation, and threat intelligence management in complex cybersecurity environments [61], [62], [63], [64], [65].

Finally, future research should place greater emphasis **on** real-world deployment, benchmarking, and operational validation of machine learning-based intrusion detection systems. Although many proposed IDS frameworks demonstrate promising performance using publicly available benchmark datasets, relatively few studies evaluate their effectiveness under real-world operational conditions. Simulated datasets often fail to capture the complexity, diversity, and unpredictability of contemporary network traffic and evolving cyber threats. Consequently, large-scale field deployments, longitudinal performance evaluations, and industry-academic collaborative experiments are necessary to assess scalability, robustness, latency, energy efficiency, adversarial resilience, and long-term operational effectiveness [37].

8. CONCLUSION

This review highlights the growing importance of machine learning-based intrusion detection systems (ML-based IDS) in addressing the increasing complexity, scale, and sophistication of modern cyber threats. As network environments continue to evolve through the widespread adoption of cloud computing, Internet of Things (IoT), edge computing, and distributed digital infrastructures, conventional signature-based intrusion detection systems have become insufficient for identifying zero-day attacks, advanced persistent threats (APTs), and rapidly evolving attack patterns. Machine learning has emerged as a transformative technology that enables intelligent, adaptive, and data-driven intrusion detection by continuously learning from network traffic and recognizing both known and previously unseen malicious activities. Despite these significant advancements, several important challenges remain. Machine learning-based intrusion detection systems continue to face issues related to data quality, class imbalance, computational complexity, scalability, model interpretability, adversarial machine learning attacks, interoperability, and privacy preservation. The reliance on large, representative training datasets and computationally intensive learning algorithms limits deployment in resource-constrained environments, while the black-

box nature of many deep learning models reduces transparency and user trust. Addressing these limitations requires the development of lightweight, scalable, explainable, and adversarial robust machine learning models capable of operating efficiently across heterogeneous and distributed network environments. In conclusion, machine learning-based intrusion detection systems represent a transformative paradigm for modern network cybersecurity. By combining intelligent learning algorithms with multi-layered security architectures, distributed computing, and emerging AI technologies, ML-based IDS provide adaptive, scalable, and resilient solutions for protecting contemporary digital infrastructures. As cyber threats continue to evolve, the integration of advanced machine learning techniques with explainable, privacy-preserving, and autonomous cybersecurity frameworks will play a pivotal role in developing the next generation of intelligent network defense systems capable of ensuring secure, reliable, and trustworthy digital environments.

FUNDING

This research received no external funding.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[2] A. L. Buczak and E. Guven, "A survey of machine learning methods for intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[3] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," *in IEEE Symposium on Security and Privacy*, pp. 305–316, 2010.

[4] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[5] T. R. Sikder, N. Sayeed, M. J. Hossain, M. I. Faruk, M. I. Alam, S. M. M. Uddin, and M. Adnan, "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*, vol. 11, no. 4, 2025. doi: 10.22399/ijcesen.4533

[6] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "Deep learning approach for intrusion detection system," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

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

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

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

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

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

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

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

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

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

[16] M. M. T. G. Manik, A. S. M. Saimon, M. K. Ahmed, S. Hossain, M. Moniruzzaman, and M. S. Islam, "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*, 2025. doi: 10.1007/978-3-032-05548-4_33

[17] F. B. Khair, A. S. M. Saimon, S. Hossain, et al., "Deep neural network-based imaging system for efficient pancreatic tumor identification," *Intelligent Decision Technologies*, vol. 19, no. 6, pp. 4118–4129, 2025. doi: 10.1177/18724981251381581

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

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

[20] M. S. Siddiki, R. S. Mondal, M. N. A. Bhuiyan, M. Kamruzzaman, and S. Saha, "Assessment the knowledge, attitudes, education, knowledge, attitude and practices toward artificial intelligence," *Journal of Business and Management Studies*, vol. 7, no. 5, pp. 106–116, 2025. doi: 10.32996/jbms.2025.7.5.9

[21] M. N. A. Bhuiyan, M. Kamruzzaman, S. Saha, M. S. Siddiki, and R. S. Mondal, "Role of data analysis and integration of artificial intelligence," *Journal of Business and Management Studies*, vol. 7, no. 4, pp. 379–388, 2025. doi: 10.32996/jbms.2025.7.4.20.26

[22] M. Kamruzzaman, S. Saha, M. S. Siddiki, R. S. Mondal, and M. N. A. Bhuiyan, "Applications of artificial intelligence in small and medium scale business," *Journal of Business and Management Studies*, vol. 7, no. 4, pp. 314–325, 2025. doi: 10.32996/jbms.2025.7.4.20.21

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

[24] S. Saha, M. S. Siddiki, R. S. Mondal, M. N. A. Bhuiyan, and M. Kamruzzaman, "Risk assessment of cyber security in the banking sector," *Journal of Business and Management Studies*, vol. 7, no. 4, pp. 208–218, 2025. doi: 10.32996/jbms.2025.7.4.12

[25] A. A. M. Ashik, M. M. Rahman, E. Hossain, M. S. Rahman, S. Islam, and S. I. Khan, "Transforming U.S. Healthcare Profitability through Data-Driven Decision Making: Applications, Challenges, and Future Directions," *European Journal of Medical and Health Research*, vol. 1, no. 3, pp. 116-125, 2023. doi: 10.59324/ejmhr.2023.1(3).21

[26] K. R. Alam, K. R. H. Saurav, J. U. Z. Kabir, M. S. Rahman, M. I. Hasan, and C. Barua, "AI-driven digital marketing analytics and leadership strategies for sustainable business innovation: A mixed-methods research study," *The American Journal of Management and Economics Innovations, 6(12), 83–102. Retrieved from*, 2024. [Online]. Available: https://theamericanjournals.com/index.php/tajmei/article/view/7400

[27] C. Barua, M. S. Rahman, M. I. Hasan, K. R. H. Saurav, K. R. Alam, and J. U. Z. Kabir, "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*, vol. 3, no. 1, pp. 39–51, 2024. doi: 10.32996/agjcsts.2024.3.1.4

[28] E. Hossain, A. A. M. Ashik, M. M. Rahman, S. I. Khan, M. S. Rahman, and S. Islam, "Big data and migration forecasting: Predictive insights into displacement patterns triggered by climate change and armed conflict," *Journal of Computer Science and Technology Studies*, vol. 5, no. 4, pp. 265–274, 2023. doi: 10.32996/jcsts.2023.5.4.27/

[29] E. Hossain, K. P. Shital, M. S. Rahman, S. Islam, S. I. Khan, and A. A. M. Ashik, "Machine learning-driven governance: Predicting the effectiveness of international trade policies through policy and governance analytics," *Journal of Trends in Financial and Economics*, vol. 1, no. 3, pp. 50–62, 2024. doi: 10.61784/jtfe3053

[30] M. A. Yusuf, M. R. K. Khan, P. P. Saha, and M. M. Rahaman, "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*, 2024. doi: 10.1109/ICoICI62503.2024.10696627

[31] M. A. Yusuf, N. M. Chowdhury, P. D. Rone, P. P. Saha, M. I. Hossan, D. Sarkar, R. Paul, M. R. Hossain, and M. Chakraborty, "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. Available from:*, 2025. doi: 10.4108/airo.9785 [Online]. Available: https://publications.eai.eu/index.php/airo/article/view/978z5

[32] M. M. Rahman, F. F. Sifat, R. Islam, S. Molla, and M. R. K. Khan, "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*, 2024. doi: 10.1109/ICECET61485.2024.10698666

[33] P. P. Saha, M. M. Rahaman, M. T. Islam, and N. I. Chowdhury, "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*, 2025a. doi: 10.1109/ISCS69371.2025.11386016

[34] P. P. Saha, P. D. Rone, D. Sarkar, M. A. Yusuf, M. I. Hossan, and M. S. J. Mazumder, "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*, 2025b. doi: 10.1109/ESCI63694.2025.10988213

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

[36] M. R. Habib, M. A. Yusuf, W. M. H. N. Warnasuriya, K. Sunny, M. M. Rahaman, and M. R. K. Khan, "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*, 2024. doi: 10.1109/ICoICI62503.2024.10696135

[37] S. Nusrat, F. Hossain, and T. R. Sikder, "Integrating Wearable Health Data and Environmental Management Analytics for AI-Driven Cardiovascular Disease Prevention," *The Eastasouth Journal of Information System and Computer Science*, vol. 2, no. 02, pp. 209–223, 2024. doi: 10.58812/esiscs.v2i02.868

[38] R. S. Mondal, R. A. Ahmed, M. A. K. P. Hemal, T. R. Sikder, and B. J. A. Juie, "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*, vol. 8, no. 2, pp. 113–127, 2026a. doi: 10.37547/tajmspr/Volume08Issssue02-17

[39] R. S. Mondal, T. N. Purba, N. N. Purba, M. M. Rahman, and T. R. Sikder, "AI-Driven Glycemic Instability Risk Modeling for Proactive Intervention and Chronic Disease Management in U.S. Healthcare Systems," *Journal of Medical and Health Studies*, vol. 7, no. 1, pp. 29-43, 2026b. doi: 10.32996/jmhs.2023.4.6.21

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

[41] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in IoT," *Computer Networks*, vol. 76, pp. 146–164, 2015.

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

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

[44] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[45] M. I. Alam, M. A. Sami, M. A. K. P. Hemal, and M. L. Rahman, "Predictive Analytics and Decision Intelligence for Climate-Resilient Agritech Systems," *Academica Global: Journal of Computer Science and Technology Studies*, vol. 2, no. 1, pp. 44-56, 2023. doi: 10.32996/agjcsts.2023.2.1.4

[46] M. I. Alam, M. A. Sami, A. Al Masud, H. Ahmed, and F. Hossain, "AI-Driven Big Data Analytics for Personalized Cancer Treatment: Integrating Multi-Omics, Medical Imaging, and Predictive Intelligence," *Journal of Computer Science and Technology Studies*, vol. 7, no. 11, pp. 428-441, 2025. doi: 10.32996/jcsts.2025.7.11.40

[47] M. M. Hasan, M. I. Alam, M. A. H. Chowdhury, and M. M. Anwar, "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*, vol. 5, no. 2, pp. 41-62, 2026. doi: 10.32996/jcsts.2026.5.1.5

[48] M. A. Sami, M. L. Rahman, Z. A. Tanni, Z. S. Munmun, S. Nusrat, and B. Biswas, "Artificial intelligence and big data for precision medicine: A review of bioinformatics-driven healthcare applications," *Frontiers in Computer Science and Artificial Intelligence*, vol. 5, no. 6, pp. 36–43, 2026. doi: 10.32996/fcsai.2026.5.6.7

[49] K. R. H. Saurav, K. R. Alam, C. Barua, M. I. Hasan, M. S. Rahman, and J. U. Z. Kabir, "AI-Driven Consumer Behavior Insights and Human-Centered Marketing Strategies for Enhancing Engagement and Innovation," *Journal of Business and Management Studies*, vol. 5, no. 6, pp. 187-197, 2023. doi: 10.32996/jbms.2023.5.6.16x

[50] M. A. Sami, M. A. K. P. Hemal, M. I. Alam, and M. L. Rahman, "Data Governance and Analytics Infrastructure for Scalable Decision-Making in Development and Agritech Programs," *European Journal of Applied Science, Engineering and Technology*, vol. 2, no. 2, pp. 388-403, 2024. doi: 10.59324/ejaset.2024.2(2).28

[51] M. I. Hasan, C. Barua, M. S. Rahman, K. R. Alam, J. U. Z. Kabir, and K. R. H. Saurav, "Resilient healthcare and critical urban infrastructure design using AI-driven engineering and project management systems," *Journal of Medical and Health Studies*, vol. 4, no. 6, pp. 20–34, 2023. doi: 10.32996/jmhs.2023.4.6.20

[52] M. I. Alam, T. R. Sikder, M. A. Sami, M. L. Rahman, M. A. K. P. Hemal, A. A. Linkon, M. M. R. Bhuiyan, M. M. Aziz, M. S. Islam, and M. M. Rahman, "A robust and explainable approach to crop recommendation using a balanced multi-crop agronomic dataset," *Journal of Environmental and Agricultural Studies*, vol. 7, no. 3, pp. 1-15, 2026. doi: 10.32996/jeas.2026.7.3.1

[53] T. R. Sikder, S. Dash, B. Uddin, and F. Hossain, "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*, vol. 1, no. 02, pp. 153–170, 2023a. doi: 10.58812/esiscs.v1i02.838

[54] T. R. Sikder, M. A. Siam, M. M. H. Melon, S. M. M. Uddin, S. C. Mohonta, and F. Karim, "A Multimodal Data Analytics Framework for Early Cancer Detection Using Genomic, Radiomic, and Clinical Big Data Fusion," *Journal of Computer Science and Technology Studies*, vol. 5, no. 3, pp. 183-188, 2023b. doi: 10.32996/jcsts.2023.5.3.13

[55] M. I. Alam, M. A. K. P. Hemal, M. A. Sami, and M. L. Rahman, "Robust and Interpretable Crop Recommendation: A Case Study on a Balanced Multi-crop Agronomic Dataset," *European Journal of Ecology, Biology and Agriculture*, vol. 1, no. 5, pp. 168-184, 2024. doi: 10.59324/ejeba.2024.1(5).14

[56] J. U. Z. Kabir, K. R. H. Saurav, M. S. Rahman, M. I. Hasan, C. Barua, K. R. Alam, and M. M. Rahman, "Financially sustainable strategic leadership and management with predictive analytics to strengthen nationwide U.S. healthcare quality and performance," *European Journal of Medical and Health Research, 1(3), 144–150. Eur J Med Health Res, 2023;1(3):144-50*, 2023. doi: 10.59324/ejmhr.2023.1(3).24

[57] N. Vanu, M. R. Hasan, T. R. Sikder, and Z. S. Tamanna, "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*, vol. 3, no. 2, pp. 124-141, 2021. doi: 10.32996/jcsts.2021.3.2.11

[58] M. L. Rahman, M. I. Alam, R. Anzum, S. Acharjee, M. S. Alam, and S. Shamarukh, "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*, vol. 8, no. 7, pp. 41–55, 2026. doi: 10.32996/jbms.2026.8.7.3

[59] M. J. Hossain, M. M. Bakhsh, M. A. Sami, M. I. Alam, M. M. H. Melon, and M. M. T. G. Manik, "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*, 2026. doi: 10.1109/I3CTCON68242.2026.11507252

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

[61] C. Barua, "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*, vol. 3, no. 1, pp. 39-51, 2024. doi: 10.32996/agjcsts.2024.3.1.4

[62] K. Das, M. Rahman, and S. Islam, "Explainable artificial intelligence for cybersecurity applications: Enhancing transparency in intrusion detection systems," *Journal of Cybersecurity and AI Systems*, vol. 12, no. 3, pp. 145–162, 2025.

[63] N. Moustafa and J. Slay, "UNSW-NB15 dataset," *in MILCOM Conference*, 2015.

[64] M. M. Rahman, A. Hossain, N. Chakraborty, and M. R. K. Khan, "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*, 2024. doi: 10.1145/3660853.3660885

[65] P. P. Saha, R. Paul, M. R. K. Khan, N. A. S. Siddique, and B. D. Sarker, "AI-driven modernization of medicare and medicaid enterprise systems: interoperability, claims analytics, and fraud detection frameworks," Journal of Intelligent Decision Making and Information Science, vol. 3, no. 5s, pp. 827–866, 2026, doi: 10.59543/jidmis.v3.1223.