iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** X **Month of publication:** October 2026

DOI: https://doi.org/10.22214/ijraset.2026.85445

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue X Oct 2026- Available at www.ijraset.com

A Comprehensive Review of Driven Framework for Intelligent Attack Detection and Dynamic Security Monitoring in Modern Digital Infrastructure

Monalika Devendra Kakde[1], Dr. Sushma V. Telrandhe[2], Prof. Priyadarshani S. Gotmare[3]
[1]*PG Student, Department of Computer Science And Engineering, Guru Nanak Institute of Engineering & Technology, Nagpur, Maharashtra, India*
[2]*Assistant Professor,Department of Computer Science And Engineering, Guru Nanak Institute of Engineering & Technology, Nagpur, Maharashtra, India*
[3]*Assistant Professor, Department of Computer Science And Engineering, Guru Nanak Institute of Engineering & Technology, Nagpur, Maharashtra, India*

Abstract: ***The rapid growth of cloud computing, Internet of Things (IoT) devices, enterprise networks, and interconnected digital services has increased the complexity of cybersecurity threats. Traditional signature-based security mechanisms often struggle to identify zero-day attacks, evolving malware, and previously unseen malicious activities. This review paper examines the application of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) in intelligent cyberattack detection and dynamic security monitoring. It reviews commonly investigated algorithms, including Random Forest, Extreme Gradient Boosting (XGBoost), Support Vector Machine (SVM), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and anomaly detection techniques. Existing research is compared in terms of detection capability, computational requirements, adaptability, false-positive rates, and deployment challenges. The review also examines network traffic analysis, behavioral monitoring, real-time alert generation, and automated incident response. Major challenges include imbalanced datasets, concept drift, adversarial attacks, limited generalization to unseen threats, and the difficulty of deploying computationally intensive models in resource-constrained environments. The review identifies opportunities for hybrid AI architectures, explainable detection, privacy-preserving collaborative learning, and feedback-driven security monitoring. It concludes that combining accurate threat classification with continuous monitoring and carefully controlled response mechanisms represents a promising direction for improving cybersecurity resilience across modern digital infrastructure.***
Keywords: Artificial Intelligence, Cybersecurity, Intrusion Detection, Machine Learning, Deep Learning, Threat Detection, Dynamic Security Monitoring, Network Security etc.

I. INTRODUCTION

Modern digital infrastructure relies on cloud platforms, enterprise networks, connected devices, and online services to support critical operations. This interconnected environment increases exposure to malware, ransomware, phishing, denial-of-service attacks, unauthorized access, and other evolving cyber threats. Consequently, cybersecurity has shifted from conventional perimeter protection toward continuous monitoring, behavioral analysis, and intelligent threat detection [1]–[3].

Traditional signature-based intrusion detection systems identify threats using previously recognized patterns. Although effective against known attacks, these systems may fail to identify previously unseen threats and variations of existing attacks. Anomaly-based detection attempts to address this limitation by identifying deviations from normal network or system behavior. However, legitimate changes in traffic and user activity can also produce false alarms [4], [5].

Artificial Intelligence provides techniques for analyzing large volumes of network traffic, system logs, and security events. Machine learning algorithms can classify known attack patterns, while deep learning methods can learn complex relationships and sequential behavior from appropriately prepared data [6]–[8]. These capabilities make AI a promising component of intelligent intrusion detection and cybersecurity analytics. Dynamic security monitoring extends detection beyond isolated classification tasks. It involves continuously observing network behavior, analyzing security events, prioritizing potential threats, and generating alerts for investigation. Integrating AI with these monitoring functions may help security teams identify incidents more quickly and manage large-scale security data more efficiently [9], [10].

©IJRASET: All Rights are Reserved

However, practical deployment remains challenging. Model performance can vary across datasets and network environments, while imbalanced attack categories, concept drift, adversarial manipulation, and computational overhead can reduce reliability. High detection accuracy alone does not guarantee effective security if the model generates excessive false positives or responds too slowly [11], [12].

This review therefore examines AI algorithms, dynamic monitoring approaches, evaluation methods, and recent research directions. Its main objective is to synthesize the existing literature, compare the capabilities and limitations of established techniques, and identify research opportunities for developing more adaptive, reliable, and scalable cybersecurity frameworks.

II. LITERATURE REVIEW

The reviewed literature demonstrates the development of intrusion detection from conventional rule-based methods to machine learning, deep learning, hybrid architectures, and adaptive security systems. Recent surveys emphasize the importance of selecting appropriate datasets, evaluating multiple algorithms, and considering deployment limitations alongside detection performance [1], [2].

Yang et al. reviewed methods and datasets for anomaly-based network intrusion detection, highlighting the diversity of detection techniques and the need for systematic evaluation [3]. Research by Hore et al. proposed a multistage deep learning framework targeting zero-day, out-of-distribution, and adversarial evasion attacks, demonstrating the importance of robustness beyond conventional classification [4].

Other studies investigate hybrid machine and deep learning approaches for intrusion detection [5], intelligent packet-level monitoring [6], and real-time traffic analysis [7]. Research on IoT and industrial IoT security also explores deep transfer learning and lightweight models to accommodate constrained computing resources [8].

Federated learning has emerged as a complementary direction because it enables collaborative model training without requiring organizations to pool all their raw security data centrally [9], [10]. Recent research further emphasizes concept drift, model interpretability, and adversarial robustness as important challenges for deploying AI-based intrusion detection in changing environments [11], [12].

A. Summary of literature

Table 1: Summary of selected literature

Reference	Research focus	Major contribution	Limitation or open challenge
[1], [2]	ML/DL intrusion detection surveys	Organize algorithms, datasets, and evaluation methods	Lack of universal performance across environments
[3]	Anomaly detection methods and datasets	Systematic analysis of existing research	Dataset representativeness and reproducibility
[4]	Robust sequential deep learning	Targets zero-day and adversarial evasion scenarios	Requires broader real-world validation
[5]	Hybrid ML/DL detection	Combines complementary learning approaches	Computational cost and transferability
[6]	Intelligent network intrusion detection	Supports packet-level threat analysis	Operational adaptation remains challenging
[7]	Real-time network attack detection	Investigates detection over live traffic	Accuracy and multi-class performance trade-offs
[8]	IoT/IIoT transfer learning	Addresses resource-aware detection	Generalization across device environments
[9], [10]	Federated intrusion detection	Supports privacy-aware collaborative learning	Communication costs and non-uniform data
[11]	Concept drift	Examines adaptation to changing traffic and attacks	Reliable adaptation with limited labels
[12]	Adversarial robustness	Reviews attacks, defenses, and evaluation gaps	Robustness against realistic attack scenarios

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

III. AI ALGORITHMS FOR CYBERATTACK DETECTION

AI-based intrusion detection generally involves supervised classification, unsupervised anomaly detection, deep representation learning, or combinations of these approaches. The most suitable method depends on the availability of labeled data, the attack categories of interest, the volume of traffic, and the computational resources available [1]–[5].

A. Machine learning algorithms

Random Forest (RF): Random Forest combines predictions from multiple decision trees. It is useful for structured network-flow data, nonlinear relationships, and feature-importance analysis. Its effectiveness depends on representative training data and suitable model configuration.

Extreme Gradient Boosting (XGBoost): XGBoost builds an ensemble of decision trees sequentially, improving predictions by focusing on previous errors. It is suitable for tabular security data but may require careful tuning to control overfitting and computational cost.

Support Vector Machine (SVM): SVM identifies decision boundaries between normal and malicious traffic. It can perform well on appropriately prepared datasets, although training and inference may become expensive for large-scale traffic and complex kernel configurations.

B. Deep learning algorithms

Convolutional Neural Networks (CNNs): CNNs learn hierarchical patterns from structured representations of network data. Their success depends on appropriate feature representation, data quantity, and computational resources.

Long Short-Term Memory (LSTM): LSTM networks model sequential dependencies in time-ordered events. They can help identify evolving traffic behavior, but require careful sequence construction and may introduce additional training and inference latency.

Transformer-based models: Attention mechanisms can capture relationships among features or events across sequences. Their potential for detecting complex attack patterns is promising, but model size and resource requirements must be considered.

C. Anomaly detection and hybrid approaches

Anomaly detection methods identify observations that differ from learned normal behavior. Isolation Forest and autoencoders are examples of techniques that can identify unusual activity without requiring every attack type to be labeled. However, anomalies are not necessarily malicious.

Hybrid approaches combine supervised classification with anomaly detection or multiple learning architectures. Such designs may improve attack coverage, but their actual benefits must be established using independent datasets, consistent evaluation metrics, and realistic deployment conditions [3]–[8].

Table 2. Comparative assessment of AI algorithms

Algorithm	Learning approach	Main strength	Key limitation	Suitable application
Random Forest	Supervised	Robust structured-data classification	Ensemble memory and inference costs	Network-flow classification
XGBoost	Supervised	Effective feature interactions	Hyperparameter sensitivity	Tabular attack detection
SVM	Supervised	Decision-boundary classification	Scaling to very large datasets	Small or medium datasets
CNN	Deep learning	Learns complex feature patterns	Requires suitable input representation	Traffic-feature analysis
LSTM	Deep learning	Models sequential dependencies	Training and latency costs	Temporal behavior analysis
Transformer	Deep learning	Captures long-range relationships	High computational requirements	Complex traffic sequences
Isolation Forest	Unsupervised	Detects unusual observations	May flag legitimate rare behavior	Anomaly screening
Autoencoder	Unsupervised/self-supervised	Learns normal-data representations	Threshold selection and drift sensitivity	Novelty detection
Hybrid model	Combined	Can balance known-attack classification and anomaly screening	Greater system complexity	Multi-stage threat detection

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

IV. DYNAMIC SECURITY MONITORING TECHNIQUES

Dynamic security monitoring extends attack detection into a continuous operational process. Rather than analyzing only a fixed dataset, the system repeatedly collects events, evaluates activity, and communicates suspicious behavior to security personnel or other authorized response systems.

A. Network traffic analysis

Network traffic analysis examines flow statistics, packet metadata, communication patterns, protocols, and connection behavior. Feature-based models can classify traffic and identify known attack categories. Real-time systems must also consider processing throughput, buffering, feature extraction delays, and the cost of inspecting high-volume traffic [6], [7].

B. Behavioral monitoring

Behavioral monitoring examines deviations in user actions, device behavior, connection frequency, and system activity. It can help identify unusual behavior that signature-based methods may miss. However, legitimate workload changes may resemble malicious activity, so contextual information and alert thresholds are important.

C. Alert generation and threat prioritization

Detection results can be converted into alerts containing the event time, suspected attack category, affected asset, model confidence, and relevant evidence. Threat prioritization can consider severity, confidence, asset importance, and potential operational impact. Alert quality should be assessed by both detection effectiveness and the number of unnecessary notifications.

D. Incident response

A monitoring framework may support incident investigation, notification, isolation recommendations, and other policy-controlled response actions. High-impact actions should require appropriate authorization, safeguards, and audit records. An AI prediction should not automatically be treated as proof of malicious activity.

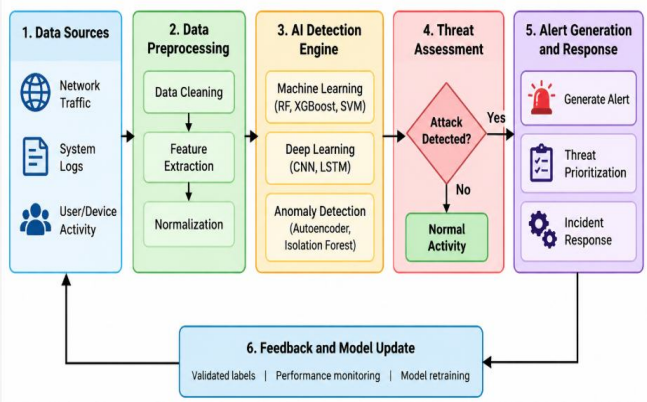


Figure 1. Conceptual workflow of AI-driven attack detection and dynamic monitoring

Figure 1. Conceptual workflow synthesized from the reviewed intrusion detection and adaptive security literature. It represents a proposed framework, not a tested implementation.

V. COMPARATIVE ANALYSIS AND DISCUSSION

The literature indicates that algorithm performance varies according to dataset characteristics, attack distribution, feature engineering, and evaluation methodology. Consequently, results obtained from different studies should not be compared directly unless their experimental conditions are sufficiently similar [1]–[3].

A. Dataset comparison

Benchmark datasets are essential for developing and evaluating intrusion detection systems. However, their age, traffic characteristics, attack categories, and class distributions influence the conclusions that can be drawn from experimental results.

Table 3: Dataset comparison

Dataset	Main characteristics	Advantages	Limitations
KDD Cup 99	Historical network connections and attack records	Useful for understanding foundational IDS research	Outdated traffic and redundancy
NSL-KDD	Refined version of KDD-based intrusion data	Reduces some redundancy and sampling issues	Does not fully represent current threats
UNSW-NB15	Normal traffic and multiple contemporary attack categories	Supports multi-class evaluation	Synthetic and testbed conditions may limit generalization
CICIDS2017	Benign traffic and multiple simulated attacks	Includes diverse traffic features and attack scenarios	Lab-generated traffic may not represent all operational networks
CSE-CIC-IDS2018	Extended collection of benign and malicious traffic	Supports larger-scale attack analysis	Dataset complexity and distribution can affect reproducibility
TON_IoT	Telemetry and network data from IoT and operating-system environments	Useful for heterogeneous IoT and IIoT security studies	Domain-specific characteristics can affect transferability

The UNSW-NB15 dataset was developed to address limitations in older benchmarks, while CICIDS2017 and TON_IoT provide additional traffic and attack scenarios for evaluating modern detection approaches [13]–[16].

B. Evaluation metrics

A reliable comparison should use multiple metrics rather than relying exclusively on accuracy.

Table 4: Evaluation metrics

Metric	Purpose	Importance
Accuracy	Proportion of all correctly classified records	General performance, but may be misleading with imbalanced data
Precision	Proportion of predicted attacks that are actual attacks	Indicates the reliability of alerts
Recall	Proportion of actual attacks detected	Measures attack coverage
F1-score	Harmonic mean of precision and recall	Balances detection and alert reliability
False-positive rate	Proportion of normal records incorrectly classified as attacks	Indicates unnecessary alert burden
Detection latency	Time required to identify a threat	Important for real-time monitoring
Throughput	Amount of traffic processed per unit time	Indicates operational scalability

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Resource consumption CPU, memory, and other computing requirements Important for edge and IoT deployment
For imbalanced datasets, macro-averaged F1-score, per-class recall, and false-positive rate provide useful complementary information. Operational evaluation should additionally measure latency, throughput, and resource consumption.

C. *Overall discussion*

The literature suggests that tree-based algorithms provide practical options for structured network data, while deep learning models can capture more complex feature relationships and sequential patterns. Hybrid methods may combine these advantages but also increase system complexity.
Research on real-time detection demonstrates that processing speed and classification performance must be considered together. Similarly, federated and adaptive approaches introduce additional trade-offs involving communication costs, privacy, model stability, and robustness [7]–[12].
A major implication is that a practical security framework should integrate detection with continuous monitoring, controlled alert generation, and validated model updates. These functions should be evaluated together rather than treated as independent measures of success.

VI. RESEARCH GAPS AND CHALLENGES

Despite advances in AI-based cybersecurity, the literature identifies several unresolved challenges.

A. *Zero-day and unseen attacks*

Models trained on known attack categories may fail to recognize substantially different attack patterns. Anomaly detection and out-of-distribution analysis are promising approaches, but their effectiveness must be tested against previously unseen attacks [4], [12].

B. *High false-positive rates*

Legitimate changes in network traffic may be incorrectly classified as attacks. Reducing false positives without sacrificing recall remains essential for practical monitoring.

C. *Concept drift and evolving threats*

Traffic patterns, user behavior, and attacker strategies change over time. Static models can become less reliable when their training data no longer reflects the operational environment [11].

D. *Dataset limitations*

Benchmark datasets may contain outdated attacks, artificial traffic distributions, class imbalance, or limited environmental diversity. These limitations can lead to optimistic results that do not transfer to real networks [2], [3].

E. *Adversarial robustness*

Attackers may deliberately manipulate inputs to evade machine learning models. Detection systems therefore need robustness testing and safeguards against manipulated training data and inference-time attacks [12].

F. *Scalability and computational cost*

Complex deep learning models can require substantial memory, processing power, and training time. These requirements may restrict deployment on IoT devices, edge gateways, and high-throughput networks.

G. *Explainability and trust*

Security administrators need understandable evidence for important threat decisions. Explainable AI can help interpret model predictions, but explanations must be evaluated for reliability and usefulness in operational settings.

H. *Integration with incident response*

Detection alone does not guarantee effective protection. Additional research is needed to integrate reliable threat classification with prioritized alerts, policy-based mitigation, audit trails, and appropriate human oversight.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VII. FUTURE RESEARCH DIRECTIONS

The reviewed literature suggests the following directions for developing more reliable AI-driven cybersecurity systems.

1) Hybrid AI architectures: Combine supervised classification with anomaly detection to cover known attack categories and potentially novel behavior.
2) Adaptive learning: Investigate validated retraining and drift-detection mechanisms to accommodate changes in network behavior without destabilizing the model.
3) Explainable AI: Incorporate interpretable evidence to help analysts understand why an event was flagged as suspicious.
4) Federated learning: Explore privacy-preserving collaboration between organizations or devices without centrally pooling all raw traffic data.
5) Lightweight detection models: Develop computationally efficient models for edge computing, IoT, and high-throughput monitoring.
6) Robustness evaluation: Test models against adversarial examples, data poisoning, class imbalance, and previously unseen attack scenarios.
7) Multi-source monitoring: Investigate the combination of network flows, system logs, user behavior, and threat intelligence for richer security context.
8) Controlled automated response: Integrate alerts with authorized response mechanisms, using confidence thresholds, policy checks, and human approval for high-impact actions.
9) Standardized evaluation: Use independent datasets, time-separated testing, per-class metrics, latency measurements, and reproducible experimental settings.
10) Continuous performance monitoring: Track changes in false-positive rates, detection performance, resource consumption, and operational effectiveness after deployment.

These directions provide opportunities to develop cybersecurity frameworks that are more adaptive, transparent, scalable, and resilient to emerging threats.

VIII. CONCLUSION

This review examined the role of Artificial Intelligence, Machine Learning, and Deep Learning in intelligent cyberattack detection and dynamic security monitoring. The literature demonstrates that Random Forest, XGBoost, SVM, CNN, LSTM, anomaly detection, and hybrid approaches offer different capabilities for analyzing network traffic and identifying malicious behavior. However, no single technique provides universally reliable performance across all environments.

Important challenges include unseen attacks, false-positive alerts, dataset limitations, concept drift, adversarial manipulation, computational overhead, and integration with incident-response processes. These challenges indicate that effective cybersecurity requires more than high classification accuracy. Detection reliability, processing speed, explainability, adaptability, and operational safeguards must also be considered.

Future research should investigate integrated AI frameworks that combine attack classification, anomaly detection, continuous monitoring, threat prioritization, and carefully validated model updates. Privacy-preserving learning, lightweight architectures, and explainable security decisions also offer promising directions.

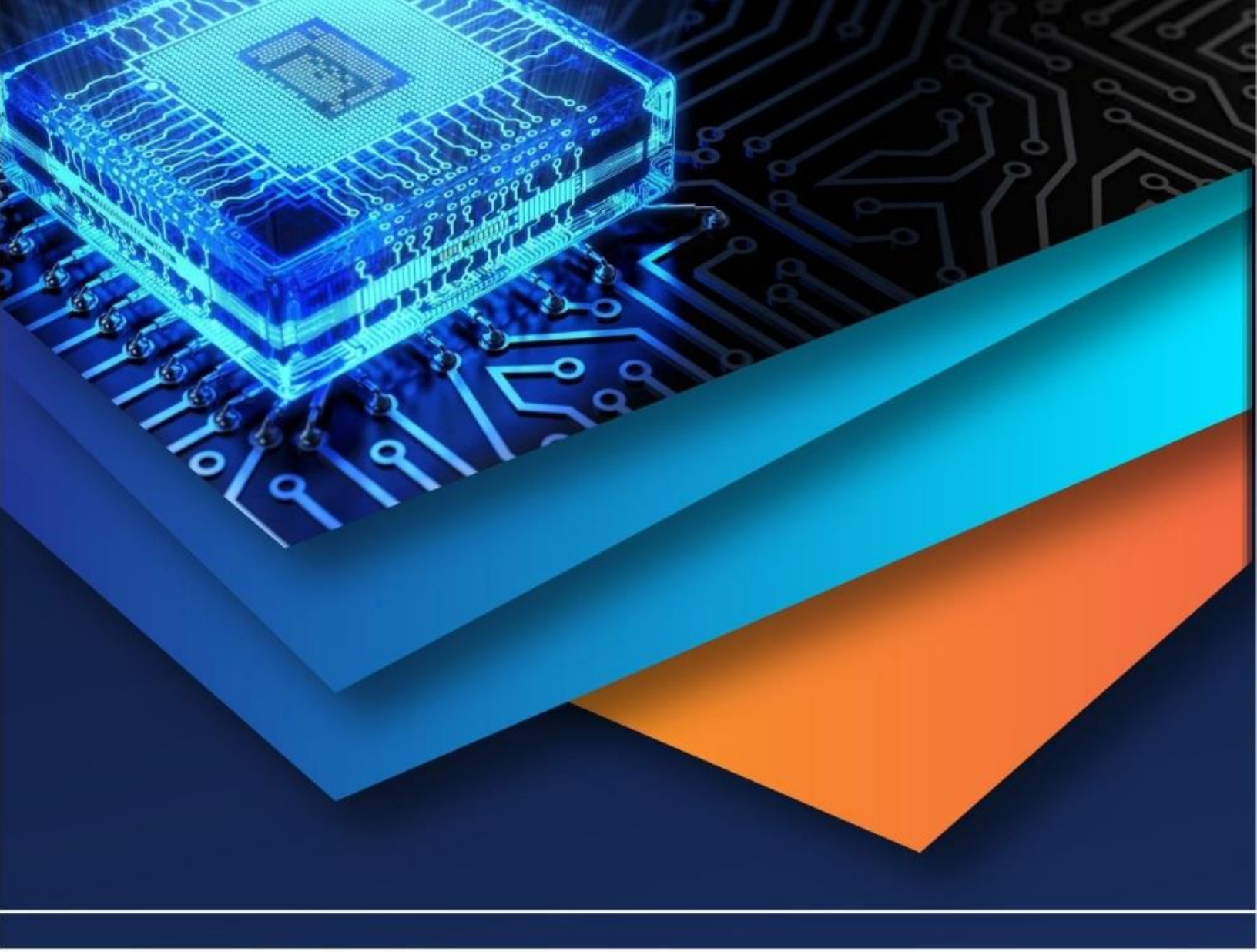
Overall, the literature supports continued development of AI-driven cybersecurity frameworks capable of improving threat visibility and assisting timely security decisions. Their practical value, however, must be established through reproducible experiments and realistic deployment evaluations rather than assumed from model architecture alone.

REFERENCES

[1] A. Hozouri, A. Mirzaei, and M. Effatparvar, “A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges,” Discover Artificial Intelligence, vol. 5, Art. no. 314, 2025. [Online]. Available: https://doi.org/10.1007/s44163-025-00578-1
[2] H. M. R. U. Rehman et al., “A systematic literature study of machine learning techniques based intrusion detection: Datasets, models, challenges, and future directions,” Journal of Big Data, vol. 12, Art. no. 264, 2025. [Online]. Available: https://doi.org/10.1186/s40537-025-01323-2
[3] Z. Yang, X. Liu, T. Li, D. Wu, J. Wang, Y. Zhao, and H. Han, “A systematic literature review of methods and datasets for anomaly-based network intrusion detection,” Computers & Security, vol. 116, Art. no. 102675, 2022. [Online]. Available: https://doi.org/10.1016/j.cose.2022.102675
[4] S. Hore, J. Ghadermazi, A. Shah, and N. D. Bastian, “A sequential deep learning framework for a robust and resilient network intrusion detection system,” Computers & Security, vol. 144, Art. no. 103928, 2024. [Online]. Available: https://doi.org/10.1016/j.cose.2024.103928
[5] M. Sajid et al., “Enhancing intrusion detection: A hybrid machine and deep learning approach,” Journal of Cloud Computing, vol. 13, Art. no. 123, 2024. [Online]. Available: https://doi.org/10.1186/s13677-024-00685-x

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[6] Y. A. Farrukh, S. Wali, I. Khan, and N. D. Bastian, "AIS-NIDS: An intelligent and self-sustaining network intrusion detection system," Computers & Security, Art. no. 103982, 2024. [Online]. Available: https://doi.org/10.1016/j.cose.2024.103982
[7] "A real-time deep learning-based approach for detecting network attacks," Big Data Research, vol. 36, Art. no. 100446, 2024. [Online]. Available: https://doi.org/10.1016/j.bdr.2024.100446
[8] B. Ahmad, Z. Wu, Y. Huang, and S. Ur Rehman, "Enhancing the security in IoT and IIoT networks: An intrusion detection scheme leveraging deep transfer learning," Knowledge-Based Systems, vol. 305, Art. no. 112614, 2024. [Online]. Available: https://doi.org/10.1016/j.knosys.2024.112614
[9] A. Belenguer, J. A. Pascual, and J. Navaridas, "A review of federated learning applications in intrusion detection systems," Computer Networks, vol. 258, Art. no. 111023, 2025. [Online]. Available: https://doi.org/10.1016/j.comnet.2024.111023
[10] I. Makris et al., "A comprehensive survey of federated intrusion detection systems: Techniques, challenges and solutions," Computer Science Review, vol. 56, Art. no. 100717, 2025. [Online]. Available: https://doi.org/10.1016/j.cosrev.2024.100717
[11] "Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems," Engineering Applications of Artificial Intelligence, Art. no. 109143, 2025. [Online]. Available: https://doi.org/10.1016/j.engappai.2024.109143
[12] "Adversarial robustness of deep learning-based intrusion detection systems: A systematic literature review of attacks, defenses, datasets, and open challenges," IEEE Access, vol. 14, pp. 149555–149591, 2026. [Online]. Available: https://doi.org/10.1109/ACCESS.2026.3733985
[13] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. Military Communications and Information Systems Conference (MilCIS), 2015, pp. 1–6. [Online]. Available: https://doi.org/10.1109/MilCIS.2015.7348942
[14] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. Int. Conf. Information Systems Security and Privacy (ICISSP), 2018, pp. 108–116. [Online]. Available: https://doi.org/10.5220/0006639801080116
[15] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in Proc. IEEE Symp. Computational Intelligence for Security and Defense Applications, 2009. [Online]. Available: https://doi.org/10.1109/CISDA.2009.5356528
[16] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, Art. no. 102419, 2020. [Online]. Available: https://doi.org/10.1016/j.jisa.2019.102419
[17] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016. [Online]. Available: https://doi.org/10.1109/COMST.2015.2494502
[18] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," Cybersecurity, vol. 2, Art. no. 20, 2019. [Online]. Available: https://doi.org/10.1186/s42400-019-0038-7
[19] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security and Privacy, 2010, pp. 305–316. [Online]. Available: https://doi.org/10.1109/SP.2010.25
[20] J. Gama, I. Žliobaitė, A. Bifet, M. Pechenizkiy, and A. Bouchachia, "A survey on concept drift adaptation," ACM Computing Surveys, vol. 46, no. 4, Art. no. 44, 2014. [Online]. Available: https://doi.org/10.1145/2523813
[21] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognition, vol. 84, pp. 317–331, 2018. [Online]. Available: https://doi.org/10.1016/j.patcog.2018.07.023
[22] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in Proc. Int. Conf. Learning Representations (ICLR), 2015. [Online]. Available: https://arxiv.org/abs/1412.6572
[23] R. Vinayakumar et al., "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525–41550, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2895334
[24] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018. [Online]. Available: https://doi.org/10.1109/TETCI.2017.2772792
[25] N. Moustafa and J. Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset," Information Security Journal: A Global Perspective, 2016. [Online]. Available: https://doi.org/10.1080/19393555.2015.1125974
[26] A. H. Lashkari, G. Draper-Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of Tor traffic using time based features," in Proc. Int. Conf. Information Systems Security and Privacy (ICISSP), 2017. [Online]. Available: https://doi.org/10.5220/0006105602530262
[27] M. Varol and A. Karakaya, "Explainable AI-based intrusion detection systems for IoT environments: A systematic literature review," Sensors, vol. 26, no. 18, Art. no. 5744, 2026. [Online]. Available: https://doi.org/10.3390/s26185744
[28] G. P. Oise et al., "Attention-based intrusion detection using transformer networks on UNSW-NB15," Scientific Reports, vol. 16, Art. no. 33862, 2026. [Online]. Available: https://doi.org/10.1038/s41598-026-65710-2
[29] M. Alauthman et al., "Generative adversarial networks for intrusion detection systems: A comprehensive survey of applications, challenges, and research directions," Arabian Journal for Science and Engineering, vol. 51, pp. 179–203, 2026. [Online]. Available: https://doi.org/10.1007/s13369-026-11103-6
[30] M. Moustafa, N. Slay, and others, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset," Information Security Journal: A Global Perspective, 2016. [Online]. Available: https://doi.org/10.1080/19393555.2015.1125974.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)