AI-Based Intrusion Detection Systems for Software-Defined Networking – A Survey

OPEN ACCESS

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
Thiyagarajan, Devasna, et al. "AI-Based Intrusion Detection Systems for Software-Defined Networking – A Survey." *Shanlax International Journal of Arts, Science and Humanities,* vol. 13, no. 3, 2026, pp. 236–45.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i1-Feb.10289

Devasna Thiyagarajan[1&2]
[1] Department of Advance Computing and Analytics School of Computing Sciences Vels Institute of Science Technology and Advanced Studies, Pallavaram, Chennai
[2] Department of Computer Science with Cognitive Systems SDNB Vaishnav College Chromepet, Chennai.

Vidhya Sathish
Department of Advanced Computing and Analytics School of Computing Sciences, Vels Institute of Science Technology and Advanced Studies, Pallavaram

V. Queen Jemila
Department of Computer Application (PG) V.V.Vanniaperumal College for Women. Virudhunagar, India

Abstract

This paper surveys the latest in Software Defined Networking (SDN) security, particularly data, from 2019 to 2025, on strategies to detect and/or mitigate interference. The described literature greatly emphasises machine learning (ML) and deep learning (DL) techniques (e.g., hybrid models related to CNN-LSTM, as well as federated learning frameworks) to resolve challenges such as distributed denial of service (DDoS) detection, privacy-preserving intrusion detection, and dynamic threat response in SDN environments. Recent publications emphasize the importance of high-quality public datasets and standardised benchmarks, identifying gaps in the current research. Gaps that these works provide include a lack of large, realistic SDN datasets, the tendency to use simulations rather than real-world testbeds, and the rise of explainable AI (XAI) methods in security domains. Every investigation specifies research on real-world impact, scale, privacy, and explicability. This survey introduces new requirements based on careful studies, leading to privacy-preserving approaches while enhancing the intrusion detection capabilities using AI-based techniques. Taken together, these results suggest that future SDN security research should focus on precise solutions that are actionable, comprehensible, and adaptable.

Keywords: Software-Defined Networking (SDN), Intrusion Detection System (IDS), Distributed Denial of Service (DDoS), Machine Learning (ML), Deep Learning (DL), Hybrid Models

Introduction

Software-defined networking (SDN) is a groundbreaking paradigm that has transformed the networking landscape by separating the control plane from the data plane, thereby enabling the development of programmable and dynamic network topologies. This separation

enhances the flexibility of network protocol implementation, fosters innovation, and simplifies network management [1]. The ability of SDN to streamline network operations, reduce costs, and accelerate service delivery underscores their significance, making them an attractive option for both academic and commercial applications [2].

Intrusion detection systems (IDS) are vital to network security, as they evaluate and pinpoint potential security vulnerabilities. The integration of IDS with SDN presents a promising approach for enhancing network security, as the centralized control of SDN allows comprehensive network monitoring and management capabilities [3].

The increasing complexity and dynamic nature of network threats necessitate the adoption of AI-based methods in IDS for SDN. AI techniques offer enhanced capabilities for identifying and responding to threats compared with traditional methods. Machine learning algorithms can efficiently manage massive volumes of network data, detect patterns, and predict potential security breaches with high accuracy. In this regard, AI-based intrusion detection systems (IDSs) are highly prized for their capacity to adjust to novel and changing threats, making them essential instruments for guaranteeing network security [4].

This review explores the intersection of SDN and IDS, focusing on AI-based approaches to enhance IDS for SDN environments. This review encompasses an analysis of current methodologies, their effectiveness, challenges faced, and future potential for deploying AI-integrated IDS within SDNs. The scope covers a thorough analysis of current research and advancements in AI-powered IDS models created for SDNs, an assessment of their effectiveness, and the identification of potential areas for further study and development in this area.

Sdn Structure and Traditional Ids Limitations

SDN Architecture and Key Components

Software-Defined Networking (SDN) represents a transformative approach in network management, characterized by the distinct separation of the control and data planes. This separation enables centralized control over the network through a programmable interface, offering a dynamic and flexible approach to network configuration and management.[5]

The SDN architecture comprises several key components (Fig. 1).

1. Controller: The core element of SDN, which acts as the brain of the network. It is located on the control plane and controls the data flow of the network, deciding where to send the traffic. The controller provides a centralized interface for programmatically managing the network. [6]
2. Data Plane (Forwarding Plane): This component is responsible for handling the actual data transmission based on the instructions received from the control plane. It includes networking devices such as switches and routers that forward packets to their destinations. [7]
3. Northbound Interfaces (NBI): These interfaces connect the SDN controller to applications and business logic above the control plane. They enable the integration of various network services and applications that can program network behaviour through open APIs, offering automation and customizability [7].
4. Southbound Interfaces (SBI): These refer to the communication channels that facilitate the connection between the controller and network devices within the data plane. The OpenFlow protocol, which is widely adopted, enables centralized control of data flow rules on networking devices [8].
5. Application Plane: This includes high-level application programs that communicate their network requirements and desired behaviour to the SDN controller, which implements these directives. This plane leverages AI and machine learning in advanced SDN frameworks to enhance decision making processes [9].

Traditional IDS Approaches and their Limitations in SDN Environments

Owing to architectural distinctions, Software-Defined Networking (SDN) environments present challenges for conventional intrusion detection systems (IDS). Traditional IDS rely on centralized machine learning, creating vulnerabilities within SDN environments. Centralization in SDN controllers poses risks if compromised, creating a single point of failure that traditional IDS cannot handle [4]. Traditional IDS struggle with scalability when faced with SDN's dynamic nature of SDNs [2]. They lack data privacy provisions in centralized data-handling models [12]. Based on predefined rules and manual feature extraction, traditional IDS are less effective against emerging attacks in SDN environments [3]. Their integration can impact throughput and latency because of constant monitoring needs [13]. Newer approaches, such as federated learning, enable decentralized data handling and scalable analysis, which aligns with SDN's dynamic nature of SDNs [1]. SDN-based solutions leverage network programmability for responsive IDS/IPS setups that adapt to SDN threat landscapes [3].

AI Techniques Commonly used in Network Security

Artificial intelligence (AI) uses machine learning, deep learning, and natural language processing techniques to improve network security against sophisticated cyber threats.

Machine Learning (ML) Algorithms: ML algorithms detect anomalies, classify malware, and identify network intrusions by recognising malicious activity patterns [14].

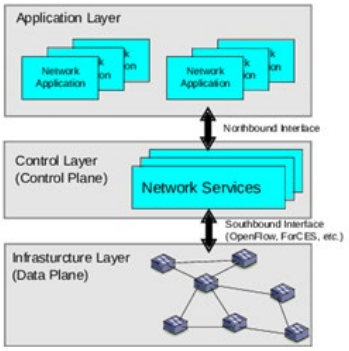

Fig 1 SDN Architecture

1. Deep Learning Models: Deep neural networks process data to detect security breaches, ensuring privacy and information security. [15]
2. Explainable AI (XAI): XAI makes the decisions of AI models transparent, enabling better threat mitigation and trust in AI systems [16].
3. Natural Language Processing (NLP): NLP analyses cybersecurity data to identify threats through textual information processing [17].

AI-based IDS Approaches for SDN

Software-Defined Networking (SDN) architectures, known for their inherent flexibility and adaptability, necessitate the integration of AI-based Intrusion Detection Systems (IDS) to bolster network security. By decoupling the control and data planes, SDN allows for the seamless incorporation of AI techniques, facilitated by centralized management through an SDN controller.

In recent years, various strategies have been explored. For instance, the integration of Support Vector Machines (SVM) with Software-Defined Networking (SDN) for Intrusion Detection Systems (IDS) employs anomaly detection by analyzing traffic flows. This approach identifies malware by utilizing traffic attributes accessible to the SDN controller [4]. A hierarchical IDS

architecture combines flow-based and packet-based IDS, utilizing SVM trained on datasets such as the DARPA Intrusion Detection Dataset to provide high detection rates without degrading network performance [19].

Furthermore, the application of deep learning in IDS shows promise, although susceptibility to adversarial attacks remains a challenge [3]. Studies have highlighted the need for robust datasets compatible with SDN environments to train models effectively [4]. Moreover, leveraging dynamic deployment strategies and load balancing in SDN-enabled environments, such as drone networks, can enhance fault tolerance and network defense in emergency scenarios [20]. The implementation of machine learning approaches, including neural networks, has led to scalable and efficient IDS with lower false-positive rates.

Table 1 Algorithm Performance and Challenges in SDN-Based Intrusion Detection Systems

Category	Algorithms/Models	Performance Highlights	Challenges
ML in SDN-based IDS	SVM, KNN, Decision Trees, RF	SVM demonstrated the highest prediction accuracy of 95.5% for detecting DDoS attacks [9]. Decision Tree achieved 99.81% accuracy in DNS traffic classification [10].	Susceptible to high variance and bias, leading to inaccurate or inconsistent detections [11].
DL in SDN-based IDS	CNN, ANN, LSTM, GRU	CNN achieved 97.80% training accuracy but only 90.08% prediction accuracy [9]. RF-SFS-GRU model reached 87% accuracy [12].	Overfitting issues affecting the robustness of zero-day attacks[13].
Hybrid Models	CNN-RF, RF-SFS	Hybrid DL models, such as RF-SFS-GRU, achieved better detection accuracy (up to 79% with feature selection optimisation) [12]. The SD-Reg regularisation technique addresses overfitting [13].	Complexity in implementing hybrid models and the challenge of effectively combining different algorithms to enhance performance [12].

For example, integrating AI with dynamic routing mechanisms in SDN provides better learning capabilities and traffic management [21]. To enhance the reliability of AI 0models in Intrusion Detection Systems (IDS), Bayesian Deep Learning models, including Bayesian Convolutional Neural Networks, have been introduced. These models aim to improve the accuracy of intrusion detection while minimizing the occurrence of false alarms [7]. The use of ensemble-based detection further enhances performance by relying on multiple models for accurate prediction. The synthesis of ML, DL, and hybrid approaches in SDN based IDS reflects ongoing improvement, with notable advancements in algorithmic performance and hybrid models offering solutions to overcome specific challenges, such as accurate real-time threat detection. However, critical issues such as overfitting, variation, and model bias remain central to ongoing research and development. A comprehensive overview of the current state of machine learning (ML), deep learning (DL), and hybrid models for software-defined networking (SDN)-based intrusion detection systems (IDS) is presented in (Table 1).

Benchmark Datasets Essential for AI-Driven Intrusion Detection in SDN

Various datasets have been used to train and evaluate AI-driven intrusion detection systems (IDS) for software-defined networking (SDN).

The datasets identified in this study are listed in Table II.

NSL-KDD and UNSW-NB15: The NSL-KDD and UNSW-NB15 datasets are widely used to evaluate AI-based IDS. They present a diverse array of attack types and are frequently used alongside advanced methods, such as Bayesian Convolutional Neural Networks, to improve detection precision and minimize false alarm rates [26].

DARPA Intrusion Detection Dataset: This dataset is specifically utilized in hierarchical intrusion detection systems, supporting the training of flow-based IDS using Support Vector Machine-based anomaly detection algorithms that exhibit high detection rates without sacrificing network performance [27].

InSDN Dataset: Known for its applicability to SDN settings, the InSDN dataset includes various attack types that can occur across different components of an SDN platform. It serves as a modern foundation for assessing IDS performance, particularly for researchers focusing on anomaly detection systems customized for SDN networks (Elsayed et al., 2020). [28]

TON_IOT: This dataset was employed for testing deep learning-based approaches within network and IoT systems. It facilitates experimentation on both network-specific and IoT datasets; models such as CNN and DNN have achieved significant accuracy using this data [29]. These datasets are crucial for developing responsive and precise IDS in SDN environments, supporting advancements in machine and deep learning techniques to bolster network security.

Key Challenges in AI-based IDS for SDN

A. Important issues with AI-based IDS for SDN There are a number of significant obstacles when integrating artificial intelligence (AI) with intrusion detection systems (IDS) for

Table 2 Key Datasets for SDN - IDS and Their Roles

Dataset	Typical Usage in SDN IDS Research	Characteristics & Strengths	Example Methods/ Models Used
NSL-KDD	Benchmark for classical and deep learning-based IDS; evaluates detection, false alarm rates, model robustness	Includes diverse attack types and well-structured normal/attack categories, supporting generalized model training	SVM, Random Forest, CNN, Bayesian CNN
UNSW-NB15	Assesses next-gen IDS and anomaly detectors in SDN and IoT; well-suited for advanced and hybrid models	Extensive feature set, real network traffic, modern attack scenarios; reduces redundancy found in older datasets	CNN, DNN, Hybrid/ ensemble models
DARPA	Used for hierarchical/flow-based IDS; supports anomaly and signature-based evaluations	Historic, widely recognized, with labeled attacks/normal events; useful for statistical and ML-based IDS benchmarking	Support Vector Machines (SVM), anomaly detection
InSDN	SDN-specific; evaluates IDS in realistic, programmable network scenarios	Designed to reflect SDN-plane attacks control /data /management), enabling targeted validation for SDN deployments	AI/ML tailored for SDN threat types

TON_IOT	For cross-domain (IoT and SDN) security and deep learning research	Contains network and IoT telemetry, modern attacks, multi-source data; supports research on smart network/ IoT environments	CNN, DNN, transfer learning

Software-defined networks (SDN). First, because SDN controllers are centralized, they can be a single point of failure and a target for cyber attacks. Therefore, strong IDS solutions are required to defend the SDN architecture against various security risks [19]. Second, the availability of high-quality datasets for model training is crucial for the efficacy of AI-based IDS.

The absence of up-to-date and SDN-compatible datasets presents a significant challenge, as outdated or incompatible datasets can hamper the development of accurate and effective IDS [4]. Another challenge is the opacity of AI models, which can hinder the interpretability of IDS results for human analysts. To address this, frameworks for XAI in IDS are being developed to enhance the understanding of AI decisions, which is crucial for effective threat response [16]. Furthermore, traditional centralized machine learning approaches in IDS have limitations in terms of data privacy and availability.

Federated learning, which enables collaborative training without the necessity of data sharing, presents a viable solution that safeguards privacy while facilitating the effective deployment of intrusion detection systems (IDS) in software-defined networking (SDN) [23]. However, managing the computational overhead required for real-time model execution and addressing the performance variability across different AI models remain challenging tasks [24]. Despite these significant challenges, ongoing research and development efforts are exploring innovative techniques and resources to enhance the security and efficacy of AI-based IDS in SDN systems [25].

Evaluation Metrics and Benchmarks

Performance metrics assess IDS model effectiveness. Key metrics include: Detection Accuracy, measuring correctly identified instances among total instances [26]. False-positive rate (FPR) shows benign activities incorrectly identified as malicious [27].

Precision, Recall, and F1-score evaluate true positive and false negative rates, with F1-score balancing precision and recall [28]. ROC AUC assesses class distinction across thresholds [29].

Following the establishment of the importance of performance indicators in the evaluation of IDS, it is equally crucial to consider the datasets employed for system testing and training. Several datasets are used to train and test IDS models. KDD Cup 99, one of the earliest datasets, contains network intrusion activities simulated in a military network environment [30]. UNSW-NB15 includes nine types of real-world intrusion activities, addressing limitations of earlier datasets [31]. CSE-CIC-IDS 2018 provides comprehensive real-world scenarios. WSN-DS focuses on wireless sensor network intrusion detection [32].

Future Research Directions

An intriguing research avenue that leverages the unique advantages of both domains to enhance network security is the integration of Artificial Intelligence (AI) techniques with Intrusion Detection Systems (IDS) in Software-Defined Networking (SDN) environments. By enabling the system to identify both known and unknown threats through patterns derived from network data, AI methodologies such as machine learning and deep learning significantly augment the detection capabilities of IDS [33]. Emerging AI techniques for IDS in SDN aim to improve both efficiency and reliability. Support Vector Machines (SVM) serve as an example of a machine learning algorithm employed in SDNs for anomaly detection, as they facilitate the focused analysis of specific traffic

flow characteristics, thereby enhancing the detection process. Moreover, frameworks such as Bayesian Deep Learning and ensemble methods have been proposed to address issues of accuracy and confidence in predictions within AI-driven IDS [34]. The integration of these emerging AI techniques with other security measures in SDN can further enhance the robustness of security strategies. This involves combining the advantages of various anomaly detection methods (such as clustering and classification) with AI models, potentially leading to improved detection of complex threat vectors that traditional methods often overlook [16].

Moreover, the implementation of explainable AI (XAI) frameworks enhances the interpretability and transparency of AI-driven decisions within intrusion detection systems (IDS). This advancement aids security analysts in comprehending the rationale behind specific threat detection and corresponding actions [24]. The implementation of AI in IDS necessitates careful consideration of data privacy, particularly given the sensitive nature of network traffic data. Techniques such as federated learning have been proposed to address privacy and security challenges by enabling decentralized model training, thus reducing the need for data centralization and minimizing privacy risks [35].

In conclusion, ongoing research on AI and IDS within SDNs is addressing critical challenges while striving for integrated, secure, and privacy-conscious solutions. Some possible avenues for advancement in this developing subject include the creation of sophisticated detection algorithms, enhanced transparency through XAI, and privacy-preserving techniques like federated learning [22].

Conclusion

Finally, this paper study the improve effect of artificial intelligence (AI) based IDS on software defined networks (SDN) and its important role and future work result. The results indicate the significance of AI-based IDS to strengthening the SDN security architecture for providing proactive mitigation and live threat detection. Employing machine learning, these systems can analyze large amounts of network traffic data to detect anomalies and possible security threats, hence reducing the risk and allowing a secure network [16]. Integrating AI-Powered IDS into SDN gives an opportunity such as improved network visibility, establishing self-healing networks, and minimizing human intervention in threat management. Integration of AI Powered IDS in SDN provides opportunities like network visibility improvement, self-healing networks and reduced human involvement in handling the threats. Continued increase in AI sophistication will continue to increase the capacity and power of adaptive and predicative mechanisms to meet the challenges presented by the complex and dynamic environments of contemporary networks.

However, such obstacles continue to persist, and progress makes such a difference. Key limitations continue to reside in fairness and transparency of AI decision-making processes, ethical issues regarding data protection, and interoperability standards between the AI and SDN components.

Moreover, another significant challenge relates to the scalability of practical artificial intelligence solutions, in particular, in terms of handling the so-called never-ending growing network traffic and maintaining the overall high performance levels. Future research may explore the development of standard AI architectures to facilitate compatibility and ease of implementation for software defined networking platforms. Regulatory mechanisms and ethical reviews of AI implementations in network security could also help enhance stakeholder participation and trust.

References

1. D. M. Rajan and Dr. D. J. Aravindhar, "Detection and Mitigation of DDOS Attack in SDN Environment Using Hybrid CNN-LSTM," Migration Letters, vol. 20, no. S13, pp. 407–419, Dec. 2023, doi: 10.59670/ml.v20is13.6472.
2. A. Chetouane and K. Karoui, "Risk based intrusion detection system in software defined networking," Concurrency and Computation: Practice and Experience, vol. 36, no. 9, Dec. 2023, doi: 10.1002/cpe.7988.
3. N. Purandhar, M. Sangeetha, A. Ali, M. Mane, M. Rajendrian, and D. Kumar, "Enhancing Cyber-Physical System Security through AI-Driven Intrusion Detection and Blockchain Integration," International Journal of Computational and Experimental Science and Engineering, vol. 11, no. 1, Mar. 2025, doi: 10.22399/ijcesen.1168.
4. H. Y. I. Khalid and N. B. I. Aldabagh, "A Survey on the Latest Intrusion Detection Datasets for Software Defined Networking Environments," Engineering, Technology & Applied Science Research, vol. 14, no. 2, pp. 13190–13200, Apr. 2024, doi: 10.48084/etasr.6756.
5. M. S. Farooq, S. Riaz, and A. Alvi, "Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review," Electronics, vol. 12, no. 14, p. 3077, Jul. 2023, doi: 10.3390/electronics12143077.
6. G. Li, Z. Zhang, and X. Wang, "SDN-Based Load Balancing Scheme for Multi-Controller Deployment," IEEE Access, vol. 7, pp. 39612–39622, Jan. 2019, doi: 10.1109/access.2019.2906683.
7. B. Isyaku, K. Abu Bakar, M. S. Mohd Zahid, F. A. Ghaleb, and M. Bte Kamat, "Software Defined Networking Flow Table Management of OpenFlow Switches Performance and Security Challenges: A Survey," Future Internet, vol. 12, no. 9, p. 147, Aug. 2020, doi: 10.3390/fi12090147.
8. S. Ali, M. K. Alvi, A. Alshanqiti, M. A. Khan, S. Faizullah, and I. Khan, "Detecting DDoS Attack on SDN Due to Vulnerabilities in OpenFlow," Feb. 2020, vol. 10, pp. 1–6. doi: 10.1109/aect47998.2020.9194211.
9. M. Blose, M. Faheem, A. L. Imoize, L. A. Akinyemi, A. A. Khan, and S. Ojo, "Scalable Hybrid Switching-Driven Software Defined Networking Issue: From the Perspective of Reinforcement Learning Standpoint," IEEE Access, vol. 12, pp. 63334–63350, Jan. 2024, doi: 10.1109/access.2024.3387273.
10. M. Adnan et al., "Towards the Design of Efficient and Secure Architecture for Software-Defined Vehicular Networks.," Sensors (Basel, Switzerland), vol. 21, no. 11, p. 3902, Jun. 2021, doi: 10.3390/s21113902.
11. L. Boukraa, S. Essahraui, K. El Makkaoui, I. Ouahbi, Y. Maleh, and R. Esbai, "Enhancing DDoS attack detection in software-defined networking: a comparative study of machine learning algorithms using benchmark datasets," EDPACS, vol. ahead-of-print, no. ahead-of-print, pp. 1–20, Mar. 2025, doi: 10.1080/07366981.2025.2478706.
12. M. Raza, M. Awais Sattar, M. B. Riaz, and M. Jasim Saeed, "Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks," IEEE Access, vol. 12, pp. 69551–69567, Jan. 2024, doi: 10.1109/access.2024.3395997.
13. G. Rampone, S. Rampone, and T. Ivaniv, "A Hybrid Federated Learning Framework for Privacy-Preserving Near-Real-Time Intrusion Detection in IoT Environments," Electronics, vol. 14, no. 7, p. 1430, Apr. 2025, doi: 10.3390/electronics14071430.
14. D. N. Katiyar, M. P. Kumar, D. A. K. Sahu, M. S. Verma, M. S. Tripathi, and D. S. Saxena, "AI and Cyber-Security: Enhancing threat detection and response with machine learning.," Educational Administration Theory and Practices, Apr. 2024, doi: 10.53555/kuey.v30i4.2377.

15. K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," IEEE Access, vol. 12, pp. 173127–173136, Jan. 2024, doi: 10.1109/access.2024.3493957.
16. S. C. Emerald and T. Vengattaraman, "Explainable Artificial Intelligence with Single Layer Feedforward Neural Network and Improved Crowned Porcupine Optimization Algorithm for Classification Problems," Engineering, Technology & Applied Science Research, vol. 15, no. 2, pp. 21593–21598, Apr. 2025, doi: 10.48084/etasr.10070.
17. D. N. Katiyar, M. P. Kumar, D. A. K. Sahu, M. S. Verma, M. S. Tripathi, and D. S. Saxena, "AI and Cyber-Security: Enhancing threat detection and response with machine learning.," Educational Administration Theory and Practices, Apr. 2024, doi: 10.53555/kuey.v30i4.2377.
18. J. D. Haltigan, "Review of Martin et al. (2024)," Journal of Open Inquiry in the Behavioral Sciences, vol. 3, no. 5, Dec. 2024, doi: 10.58408/issn.2992-9253.2024.02.03.0003.
19. A. O. Alzahrani and M. J. F. Alenazi, "ML-IDSDN: Machine learning based intrusion detection system for software-defined network," Concurrency and Computation: Practice and Experience, vol. 35, no. 1, Nov. 2022, doi: 10.1002/cpe.7438.
20. B. Nugraha, N. Kulkarni, and A. Gopikrishnan, "Detecting Adversarial DDoS Attacks in Software- Defined Networking Using Deep Learning Techniques and Adversarial Training," Jul. 2021, vol. 15, pp. 448–454. doi: 10.1109/csr51186.2021.9527967.
21. M. Tropea, M. G. Spina, and F. De Rango, "Supporting Dynamic IDS Deployment with Load Balancing Strategy for SDN-enabled Drones in Emergency Scenarios," Oct. 2023, pp. 297–300. doi: 10.1145/3616388.3617549.
22. G. Agarwal, "Explainable AI (XAI) for Cyber Defense: Enhancing Transparency and Trust in AI-Driven Security Solutions," International Journal of Advanced Research in Science, Communication and Technology, pp. 132–138, Mar. 2025, doi: 10.48175/ijarsct-23624.
23. O. Aouedi and K. Piamrat, "F-BIDS: Federated-Blending based Intrusion Detection System," Pervasive and Mobile Computing, vol. 89, p. 101750, Jan. 2023, doi: 10.1016/j.pmcj.2023.101750.
24. O. Arreche, T. Guntur, and M. Abdallah, "XAI-IDS: Toward Proposing an Explainable Artificial Intelligence Framework for Enhancing Network Intrusion Detection Systems," Applied Sciences, vol. 14, no. 10, p. 4170, May 2024, doi: 10.3390/app14104170.
25. N. Maheswaran, S. Bose, and B. Natarajan, "An adaptive multistage intrusion detection and prevention system in software defined networking environment," Automatika, vol. 65, no. 4, pp. 1364–1378, Jul. 2024, doi: 10.1080/00051144.2024.2372749.
26. A. A. Abubakar, E. Gilliard, and J. Liu, "An efficient blockchain-based approach to improve the accuracy of intrusion detection systems," Electronics Letters, vol. 59, no. 18, Sep. 2023, doi: 10.1049/ell2.12888.
27. V. Hnamte and J. Hussain, "Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach," Telematics and Informatics Reports, vol. 11, p. 100077, Jul. 2023, doi: 10.1016/j.teler.2023.100077.
28. X. Jiao et al., "Comparing discriminating abilities of evaluation metrics in link prediction," Journal of Physics: Complexity, vol. 5, no. 2, p. 025014, May 2024, doi: 10.1088/2632-072x/ad46be.
29. N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. Aboras, and N. Gowtham, "An optimized LSTM-based deep learning model for anomaly network intrusion detection," Scientific Reports, vol. 15, no. 1, Jan. 2025, doi: 10.1038/s41598-025-85248-z.
30. A. A. E.-B. Donkol, M. M. Mabrook, A. I. Hussein, and A. G. Hafez, "Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in

Communication Networks," IEEE Access, vol. 11, pp. 9469–9482, Jan. 2023, doi: 10.1109/access.2023.3240109.

31. R. Mohammad, F. Saeed, A. A. Almazroi, F. S. Alsubaei, and A. A. Almazroi, "Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach," Systems, vol. 12, no. 3, p. 79, Mar. 2024, doi: 10.3390/systems12030079.
32. S. Songma, T. Pamutha, and T. Sathuphan, "Optimizing Intrusion Detection Systems in Three Phases on the CSE-CIC-IDS-2018 Dataset," Computers, vol. 12, no. 12, p. 245, Nov. 2023, doi: 10.3390/computers12120245.
33. S. K. R. Mallidi and R. R. Ramisetty, "Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: a systematic literature review," Discover Internet of Things, vol. 5, no. 1, Jan. 2025, doi: 10.1007/s43926-025-00099-4.
34. M. Sankaram, M. Roopesh, S. Rasetti, and N. Nishat, "A Comprehensive Review of Artificial Intelligence Applications in Enhancing Cybersecurity Threat Detection and Response Mechanisms," Global Mainstream Journal, vol. 3, no. 5, pp. 1–14, Jul. 2024, doi: 10.62304/jbedpm.v3i05.180.
35. A. Karunamurthy, K. Vijayan, P. R. Kshirsagar, and K. T. Tan, "An optimal federated learning-based intrusion detection for IoT environment," Scientific Reports, vol. 15, no. 1, Mar. 2025, doi: 10.1038/s41598-025-93501-8.