Journal of Cybersecurity Education, Research and Practice

Manuscript 1251

Software-Defined Networking powered by AI-driven Anomaly Detection

Dina Moloja

Vusumuzi Malele Prof

Software-Defined Networking powered by AI-driven Anomaly Detection

Abstract

Software Defined Networking (SDN) revolutionizes network control by separating the control plane from the data plane. Although the latter improves SDN agility and scalability, it creates a security hole, particularly in a central control plane, leading to SDN environments becoming high-profile targets for advanced cybersecurity threats. Due to static and signature-based point-in-time behavior, traditional security methods are unable to keep up with modern attacks that are an anomaly to SDNs. Artificial Intelligence (AI) with its different applications and techniques, has the capability of detecting SDN cyber threats' anomalies. This paper presents the results of a literature scoping exercise that used a total of 54 papers that looked at AI-driven anomaly detection in SDN. The findings showed that control theory, activity theory, and anomaly detection theory are three theoretical aspects that contribute to the topic of AI-driven anomaly detection in SDN. Furthermore, different machine learning algorithms give different results. In this regard, Random Forest (RF), Support Vector Machine (SVM), and Multi-Layer Perceptron would help in detecting threats of a familiar nature, while autoencoders and K-means can detect unfamiliar threats. While deep learning architectures such as Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNN) support low-latency anomaly detection while maintaining throughput and network stability. The findings could be the basis of providing a conceptual framework on how an intelligent, adaptive, and resilient SDN with real-time threat defense mechanisms could be designed, developed, and deployed.

Keywords

Artificial intelligence, Anomaly Detection, SDN, Real-Time Threat Mitigation, Network Security

Software-Defined Networking powered by AI-driven Anomaly Detection

Dina Moloja
Department of Information Technology
Central University of Technology
Welkom, South Africa,
mmoloja@cut.ac.za, 0000-0003-1421-5718

Vusumuzi Malele
School of Computer Science and Information Systems
North-West University,
Vanderbijlpark, South Africa
Vusi.Malele@nwu.ac.za, 0000-0001-6803-9030

I. Introduction

The emergence of Software-Defined Networking (SDN) brings a revolutionary way of network management and control [1]. By separating the control and data planes, SDNs offer a more centralized, manageable system that allows network operators to more efficiently manage and direct network traffic. This novel architecture is an enabler of dynamic reconfiguration caling out, and superior traffic engineering compared to standard networking management architectures [2].

This very centralisation and other advantages which it brings with it, also have a reverse side to the medal. The SDN controller, which is the brain or master node of the network, becomes a potential single point of failure [3][4]. If they are compromised, the entire network architecture may fail or be hijacked by attackers. This single point of failure becomes a significant vulnerability and various attacks, such as Denial-of-Service (DoS) flows and control rule modification, and attacks on controller control planes, have sought to undermine the system security and performance.

Traditional security tools still apply; however, they may not always be efficient in dealing with rapidly evolving and advanced cyber threats we see today [5]. They are usually not agile enough to discover and react to anomalies as they happen, an important factor in avoiding damage, and preserving network integrity. To counteract these drawbacks, Artificial Intelligence (AI), in particular Machine Learning (ML) and Deep Learning (DL), have recently shown as a potential solution [6]. AI-driven solutions can learn from the past and present data and capacity to aid in managing the network, from complex network patterns to anomalies that could alert to malicious activity, even before human analysts can react [7].

The rollout of SDN enables an unprecedented level of network programmability, flexibility, and central control [8]. However, this consolidation results in a central point of attack [9], which is a central weakness that traditional security applications such as firewalls and Access Control Lists (ACL), are not designed to resolve. Existing anomaly detection mechanisms for SDN are static and reactive, unable to identify dynamic zero-day exploits or unknown threats in real time [10]. Furthermore, AI techniques, such as ML and DL, for anomaly detection in SDN are still in the early stages due to certain limitations such as (i) high rates of dependancy and false positives, or negatives, limited to poor generalizability to heterogeneous SDN scenarios, the absence of common datasets, and the lack of real-time response [10][11].

Although there are numerous studies on Anomaly Detection (AD) based on AI, there is no formal framework or theoretical underpinning frame for how AI-based-AD can be successfully done for SDN. The lack of understanding about which models are superior, when and how they should be adopted and what trade-offs between security and performance that one must accept to design an intelligent and self-defending SDN infrastructure are making the task to become even more challenging.

The main aim of this paper is to explore, synthesize, and critically evaluate existing literature on AI-driven-AD techniques within SDN environments. The Introduction, Method, Results and Discussion (IMRAD) format was adopted in paper. In this regard, despite the introduction in Section I, Section II will present the paper's method, followed by Results and Discussion on Section III; then conclusion on Section IV.

II. Material and Methods

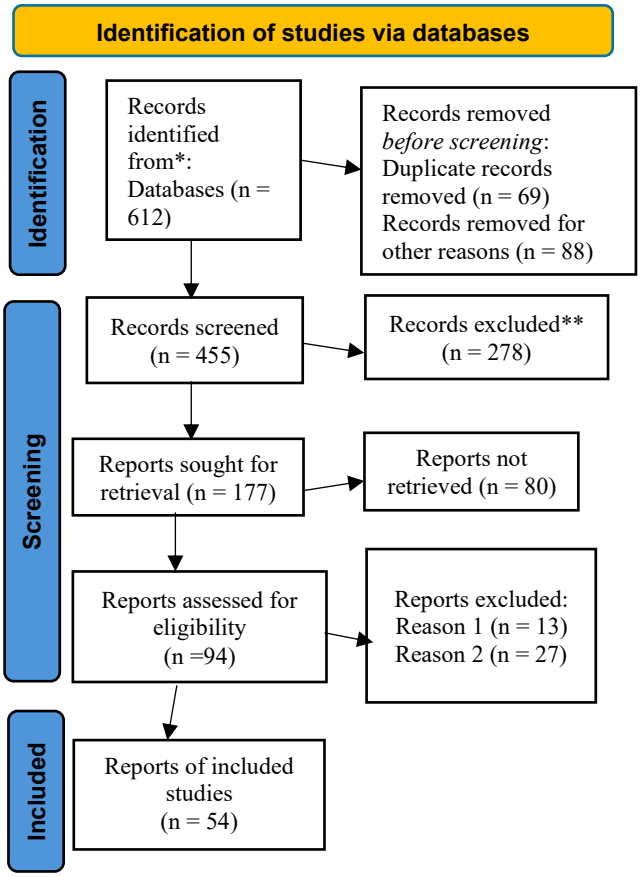

Fig. 1. SLR process using PRISMA (Source: [12])

To ensure methodological rigor and transparency, this paper employed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework for conducting a systematic literature review [12]. Fig. 1 illustrates the PRISMA flow diagram that was adopted to conduct this study. The PRISMA approach allowed for the comprehensive identification, screening, eligibility assessment, and inclusion of relevant scholarly sources focused on AI-powered anomaly detection within SDN environments.

A. Identification

A structured literature search was performed across multiple scholarly databases, namely: IEEE Xplore, ScienceDirect (Elsevier), SpringerLink, ACM Digital Library, and Scopus. The search covered publications from 2018 to 2025, reflecting the period during which SDN and AI-based security methods began gaining traction. A combination of keywords and Boolean operators below were used to initially retrieve a total of 612 records.

- ("Software-Defined Networking" OR "SDN") AND
- ("Anomaly Detection" OR "Intrusion Detection") AND
- ("Artificial Intelligence" OR "Machine Learning" OR "Deep Learning") AND
- ("Security" OR "Threat Mitigation"). A total of 612 records were initially retrieved.

B. Screening

After removing duplicates (n = 157) using Zotero and manual filtering, 455 unique articles were subjected to title and abstract screening. Studies that were clearly irrelevant, non-peer-reviewed, or not related to SDN or AI-based security systems were excluded at this stage.

- Articles excluded at this phase: 278
- Remaining for full-text review: 177

C. Eligibility

The full texts of 177 articles were assessed against predefined inclusion and exclusion criteria as indicated below:

- Inclusion Criteria: This paper focused on studies that focused on anomaly or intrusion detection in SDN environments; Articles employing AI, ML, or DL techniques, Peer-reviewed journal and conference papers, and English-language publications.
- Exclusion Criteria: The exclusion criteria focused on non-SDN-based security approaches, Studies focusing solely on hardware or non-network-related security, and articles without available full-text. After applying these criteria, 94 articles were deemed eligible.

Unfortunately, further 40 articles had to be removed because they did not fulfill the reasons for inclusion (i.e. reason 1 = No recommendations or contribution). In this regard, a total of 54 articles adopted and used in this paper. These included foundational studies on SDN security, cutting-edge AI algorithms for anomaly detection, and comparative evaluations of model performance in real-world or simulated SDN environments.

D. Data extraction and analysis

For each included study, key information was extracted and organized using a structured data extraction form, including author(s) and year, research objective and methodology, AI technique used (e.g., SVM, CNN, LSTM), Evaluation metrics (accuracy, false positive rate, etc.), Dataset and experimental setup, and Key findings and limitations. This data was used to identify recurring themes, gaps in literature, and emerging trends, which informed the synthesis presented in the findings and theoretical interpretation sections.

III. Results and Discussion

The literature on SDN and AI-driven security solutions has grown. This section synthesizes key studies across to identify:

- the underlying theories – control theory and activity theory.

A. Theoretical frame: Underlying theories

This paper takes a multi-theoretical perspective based on the Control Theory and Activity Theory to offer an integrated lens for the anomaly detection in SDN.

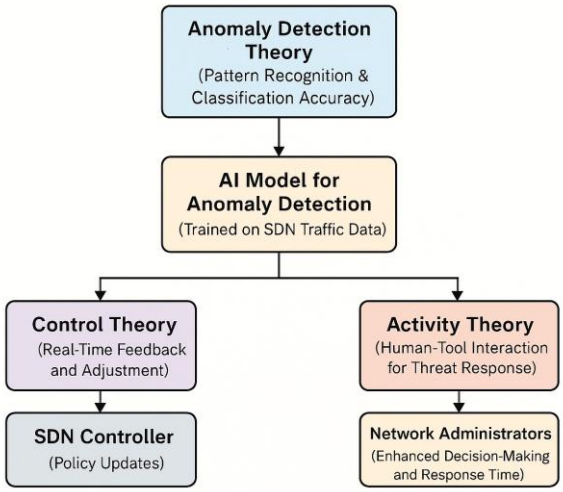

Fig. 2. Theoretical framework for AI-driven Anormaly Detection in SDN

Fig. 2 illustrates the theoretical framework for AI-driven Anomaly Detection in SDN using Control Theory, Activity Theory, and Anomaly Detection Theory. It represents the intersection of control feedback loops, socio-technical interactions and the AI-driven anomalous detection in SDN

DOI: 10.62915/2472-2707.1251

- flow across the network. Furthermore, the AI models serve as adaptive control mechanisms which dynamically respond to disturbances (threats or anomalies) and maintain system stability (network performance). In this regard, Control Activity can provide insights into feedback and regulation that may be required to preserve stability in a network under network attacks and anomalies [14].

- Activity Theory – the studies [18][19] this study applied AT to understand how the AI tool reshapes the relationship between human operators (network administrators) and the goal (secure, stable networks) which frames the network environment as a socio-technical system. In this regard, the Activity theory can frame the relationships and interactions between human and non-human agents (i.e., network administrators, AI systems, and SDN controllers) in the context of a socio-technical system and highlight the roles of tools, rules, and community in shaping outcomes of activities [20].

- Anomaly Detection Theory – allows the identification of alterations in normal networks operation key ingredient to detect in real-time new threats [26]. This theory helps analyze how AI tools interact with human and technical elements in SDN to achieve anomaly detection. AI model is trained to recognize patterns, learn from traffic data, and distinguish anomalies (core technical performance) [21]. It also provides the foundation for identifying statistically significant deviations from normal behavior. In this regard, in real-time AI implementations in SDN anomaly detection theory emphasizes understanding false positives, true positives, concept drift, and noise resilience.

B. Thematic Areas

- Software-Defined Networking and Its Security Landscape – The emergence of SDN has revolutionized the network architecture entirely. SDN centralizes programmable control of network traffic flowing within the data plane by separating the two [22]. As a result, SDN enables more flexible network architecture and more efficient resource allocation, removing static hardcoded rules from the control. However, since the flow paths of the data plane are dependent on the centralized controller, the vulnerability increases significantly. Attackers can target the controller and have automated and silent fails on the network, creating a low chance that the attacker will get caught [23]. Thus, the SDN controller can be weaponized by the attackers and used as a target for DoS, flooding it with manipulative flow rules or accessing it. As evidenced from studies [24][25], specific SDN vulnerabilities, such as topology poisoning, CC saturation, and FTE exhaustion, make SDN a new attack surface. Therefore, intelligent and real-time detection systems are required.

- Control Theory – various studies, [13-15] applied this theory to interpret how the SDN controller adjusts traffic flows or routing dynamically based on feedback from the anomaly detector. SDN's centralized control architecture aligns with control systems theory, where the controller manages data

- Traditional Approaches to Anomaly Detection in Networks – In the past, network anomaly detection was enabled through signature-based and rule-based systems [26]. Signature-based methods like Snort and Bro, now renamed to Zeek, identify intrusions by correlating incoming patterns with predetermined patterns of differentiated attacks [9] [36]. Signature-based IDSs are strong tools against harmonized attacks, and they are unable to identify the presence of a threat that has previously not been seen, shortly known as a zero-day attack. Rule-based methods, including firewalls and access control solutions, apply static rules to reasoning and do not have the elasticity required to cope with varying threats [13].

Unfortunately, the aforementioned methods have high false positives and cannot scale to the level of dynamic SDN settings [9]. Hence, there was a need for an AI-driven systems for more elasticity, scalability, and autonomous anomaly detection.

- Emergence of AI-Based Anomaly Detection in SDN – More particularly, AI, including Machine Learning (ML) and Deep Learning, has displayed strong potential in AI-based approaches for IDS to highly enhanced SDN [24] [36]. For example, ML tools such as Support Vector Machines (SVM), Random Forest (RF), and k-Nearest Neighbors (k-NN) have been widely employed to classify packages and match malicious patterns with high reliability [23][27]. Additionally, some latest research uses clumping algorithms and unsupervised learning, total as Autoencoders K-Means clumping, to identify unknown anomalies [14][28]—without any previous knowledge. Deep learning methods like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) networks, have further improved the network-traffic based detection performance [27]. SSL has also been considered a hybrid AI plan for IDS potential; these methods, when combined, can form a hybrid AI-based which is what is needed for active secure network.

- Challenges in AI Integration within SDN – while AI offers numerous benefits, integrating these technologies into operational SDN environments presents notable challenges [18][29]. First, unlike old machine learning models and statistical techniques, deep learning models often need significant amounts of processing power and memory [17]. Due to the real-time nature of controlling environments, it will be impossible to deploy many current deep-learning

models. Secondly, the lack of transparency of many AI models has occupied the attention of researchers focusing on AI safety and ethics [23][30]. For network visibility and manageability, the black-box type of an AI model results in leaving it up to the system administrator to figure out why a model predicted something and make appropriate adjustments [30]. Model brittleness, where continual drops in performance occur under conditions or when merely presented noise that has not been encountered during training, is an additional concern [31]. Many AI models also require regular retraining essential maintenance. All these considerations contribute to the exploration of human-in-the-loop systems and the field of explanatory AI. Hybrid approaches combining statistical models with AI techniques are also emerging as a robust alternative for balancing prediction accuracy with interpretability.

- Theoretical Foundations of Anomaly Detection – When it comes to theoretical conceptualization, Anomaly Detection Theory underlies the basic logic of outlier identification in network behavior [28]. Anomaly is defined as an instance that significantly varies from the usual distribution norms of data presents. It lays the theoretical grounds for both the supervised and unsupervised AI models designed to identify deviations in traffic patterns [32]. In contrast, Control Theory describes an AI-facilitated SDN controller as a feedback system responding to input signals [33]. The activity theory focuses on the socio-technical dynamic processes between human users and AI systems. It frames the analysis of AI integration into network operations in the context of tool usability, division of labor and the overarching organizational factors [30].

Rigorous Limitations: Adversarial Robustness and Explainability

While many surveyed works report high detection accuracy, several technical limitations constrain operational deployment [14]. First, adversarial robustness has rarely been evaluated systematically: most studies validate models on benign and labelled malicious traffic but do not assess model behaviour under adversarial crafted inputs [10]. Adversarial attacks against network classifiers can cause misclassification while remaining stealthy. Therefore, claims of >90% accuracy is often optimistic unless accompanied by adversarial testing.

Second, explainability (XAI) is underdeveloped in the SDN context [36]. Many high-performing deep models are effectively black boxes; without interpretable rationales, network operators are reluctant to automate mitigation. Explainability is not only a human trust issue but also a compliance requirement [12]. Techniques such as SHAP, Integrated Gradients, or rule extraction from ensembles should be used and reported. Research directions include adversarial evaluation as a standard condition, reporting model calibration and confidence, integrating XAI-by-design, and assessing the trade-off between explainability and detection performance in real SDN deployments [19].

IV. Discussion

This section presents a synthesis of research findings on the application of AI in anomaly detection within SDN environments, specifically focusing on real-time threat mitigation. The analysis draws from peer-reviewed journal articles, conference proceedings, and technical reports published in the past eight years. The findings are categorized thematically to align with the core research objective.

A. High Accurance and Performance of AI-Based Anomaly Detection

According to the literature, AI-driven approaches utilizing ML and DL can attain accuracy levels exceeding 90% in the identification of network anomalies such as DoS attacks [15][20]. Supervised algorithms, including Random Forest (RF), Support Vector Machine (SVM), and Multi-Layer Perceptron (MLP), perform particularly well with labeled datasets. In contrast, unsupervised methods like Autoencoders and K-Means are proficient at detecting unfamiliar threats [17] [36]. This illustrates the effectiveness of AI in reinforcing security within Software-Defined Networking (SDN) frameworks.

B. Real-Time Detection and Threat Mitigation

According to [22], real-time detection and response capabilities are central to the efficacy of AI in SDN security. Several studies report that AI models integrated within the SDN control layer can analyze incoming traffic, detect deviations from normal patterns, and initiate mitigation actions (e.g., updating flow rules or isolating compromised nodes) within milliseconds to a few seconds [30].

For instance, deep learning architectures such as LSTM and CNN have been shown to support low-latency anomaly detection while maintaining throughput and network stability. These findings highlight AI's potential in achieving proactive defense mechanisms, thereby reducing the window of vulnerability.

C. Integration Challenges and System Constraints

Despite promising results, several studies like [10][14] underscore the challenges associated with integrating AI models into operational SDN architectures. Issues include high computational overhead, prolonged model training times, and difficulty in scaling to large or distributed environments.

Moreover, black-box behavior—especially in deep learning models—poses interpretability challenges, limiting administrators' trust in automated decisions [24]. Some works also point to model brittleness, where AI systems underperform when exposed to noisy or adversarial data,

DOI: 10.62915/2472-2707.1251

suggesting a need for robust model validation under dynamic conditions [33].

D. Operational Usability and Human-AI Collaboration

Findings further reveal that operational usability remains a significant concern. For instance, Network administrators often require domain expertise to interpret model outputs or retrain algorithms when traffic patterns shift. Inadequate model explainability and limited user interfaces hinder human-AI collaboration [33] [36].

These challenges are particularly relevant in mission-critical networks where false positives or delayed responses could have serious implications. Consequently, the literature calls for the design of explainable AI (XAI) models and operator-aware systems that facilitate human-in-the-loop control and oversight.

E. Emergence of Hybrid and Ensemble Models

Recent advances suggest that hybrid approaches, combining traditional detection methods with AI algorithms, and ensemble models, which aggregate predictions from multiple classifiers, offer improved robustness [35]. These systems benefit from feature fusion—incorporating temporal, spatial, and behavioral indicators—to enhance detection accuracy and resilience against evolving threats.

For example, hybrid models that integrate statistical profiling with LSTM or SVM exhibit lower false positive rates and improved adaptability compared to standalone models. Such architectures are considered promising for future implementation in real-time SDN security frameworks.

F. Practical Deployment Scenarios and Examples

To illustrate the immediate practical value of AI-driven anomaly detection in SDN, we outline representative deployment scenarios across industry and critical infrastructure:

• Telecommunications (Mobile & Fixed Networks): SDN controllers that manage traffic slices for 5G network slicing can host lightweight LSTM or RF-based anomaly detectors to spot traffic anomalies that indicate DDoS attempts on a particular slice.

• Data Centre / Cloud Providers: CNNs or autoencoder ensembles can detect unusual lateral movement or unusually bursty flows associated with VM compromise.

• Industrial Control Systems (ICS) and SCADA networks: SDN-enabled industrial networks benefit from supervised classifiers (SVM, RF) trained on protocol-specific telemetry to detect unusual command patterns.

• Smart Grid / Energy Distribution: In SDN-managed substations, hybrid detectors (statistical profiling + LSTM) can detect abnormal command and telemetry patterns preceding equipment misoperation.

• Intelligent Transport Systems / Connected Vehicles: SDN-based roadside units can host ensemble models to detect spoofing or DDoS attacks targeting vehicular communication channels.

• Financial Infrastructure: SDN in financial data centers can integrate supervised ML to detect exfiltration or anomalous query patterns on market data feeds.

• Healthcare Networks: AI-based detectors can identify anomalous access or telemetry for medical devices.

The examples emphasise two recurring constraints: the need for lightweight or optimized models for low latency and finite edge compute, and the operational requirement for explainability before blocking traffic in mission-critical environments.

These findings collectively reinforce the transformative potential of AI in enhancing the security posture of SDN networks, particularly when detection models are designed for scalability, interpretability, and human-in-the-loop integration.

V. Conclusion

In conclusion, anomaly detection based on AI is a revolutionary approach to enabling real-time threat defense in SDN. When supervised, unsupervised, hybrid, and ensemble models are combined within AI systems, the ability to accurately detect both known and zero-day threats is multiplied whilst also providing better flexibility and scale. Feature fusion and false positive reduction also make them effective in a dynamic SDN environment. Based in Control Theory, these systems support active responses to feedback; Activity Theory emphasises collaboration between people and AI; and Anomaly Detection Theory underpins the concept of recognising anomalous patterns.

Future work should include: (1) Enhancing the interpretability of AI models (2) Incorporating human-in-the-loop system for better transparency in decision making (3) Designing lean, real time detection architectures for large-scale deployment. Also, AI-driven security to be more closely aligned with emerging SDN standards and an increasingly disruptive cyber threat landscape.

References

[1] L. M. Halman and M. J. Alenazi, "MCAD: A Machine learning based cyberattacks detector in Software-Defined Networking (SDN) for healthcare systems," IEEE Access, vol. 11, pp. 37052–37067, 2023. DOI: 10.1109/ACCESS.2023.3266826

[2] Y. Cao et al., "Detecting and mitigating DDoS attacks in SDN using spatial-temporal graph convolutional network," IEEE Trans. Dependable Secure Comput., vol. 19, no. 6, pp. 3855–3872, 2021. DOI: 10.1038/s41598-024-66907

[3] A. H. Abdi et al., "Security control and data planes of SDN: a comprehensive review of traditional, AI and MTD approaches to security solutions," IEEE Access, 2024. DOI: 10.1109/ACCESS.2024.3486825

[4] R. Nanda, "AI-Augmented Software-Defined Networking (SDN) in Cloud Environments," Int. J. Artif. Intell. Data Sci. Mach. Learn., vol. 4, no. 4, pp. 1–9, 2023. DOI: 10.63282/3050-9262.IJAIDSML-V4I4P101

[5] A. Rahoma, S. Imtiaz, S. Ahmed, and F. Khan, "Detection and diagnosis of process fault using unsupervised learning methods and unlabeled data," Int. J. Adv. Eng. Sci. Appl. Math., vol. 15, no. 1, pp. 24–36, 2023.DOI: 10.1007/s12572-023-00327-6

[6] V. Ravi, R. Chaganti, and M. Alazab, "Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system," Comput. Electr. Eng., vol. 102, p. 108156, 2022. DOI:10.1016/j.compeleceng.2022.108156

[7] A. Hirsi, L. Audah, A. Salh, M. A. Alhartomi, and S. Ahmed, "Detecting DDoS threats using supervised machine learning for traffic classification in software defined networking," IEEE Access, 2024. DOI:10.1109/ACCESS.2024.3486034

[8] R. Olaniyi, H. Olugbile, and O. Okwuobi, "The role of artificial intelligence in networking—A review," GEN-Multidisciplinary Journal of Sustainable Development, vol. 3, no. 1, pp. 15–45, 2025. http://genjournals.com/index.php/GEN-Multidiscipline/article/view/45

[9] Z. Mustafa, R. Amin, H. Aldabbas, and N. Ahmed, "Intrusion detection systems for software-defined networks: a comprehensive study on machine learning-based techniques," Cluster Computing, vol. 27, no. 7, pp. 9635–9661, 2024. DOI: 10.1007/s10586-024-04430-

[10] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 393–430, 2019, DOI: 10.1109/COMST.2018.2866942.

[11] N. Bilal, S. Askar, and K. Muheden, "Challenges and Outcomes of Combining Machine Learning with Software-Defined Networking for Network Security and Management Purpose: A Review," Indones. J. Comput. Sci., vol. 13, no. 2, 2024. DOI: doi.org/10.33022/ijcs.v13i2.3845

[12] M. J. Page, et al. BMJ 2021;372:n71. doi: 10.1136/bmj.n71.

[13] R. Malavika and M. L. Valarmathi, "Load Balancing Based on Closed Loop Control Theory (LBBCLCT): A Software Defined Networking (SDN) powered server load balancing system based on closed loop control theory," Concurrency Computat.: Pract. Exper., vol. 34, no. 11, p. e6854, 2022. DOI: **10.1002/cpe.6854**

[14] A. Shukla and T. Kashni, "Bibliometric analysis of banking frauds and scams literature," J. Financial Crime, vol. 32, no. 3, pp. 729–750, 2024. DOI: 10.1108/JFC-08-2024-0252

[15] A. Hirsi et al., "Comprehensive Analysis of DDoS Anomaly Detection in Software-Defined Networks," IEEE Access, 2025. DOI: 10.1109/ACCESS.2025.3535943

[16] R. Dhaya and R. Kanthavel, "An extensive analysis of artificial intelligence-based network management in software-defined networking (SDN)," in AI for Large Scale Communication Networks, IGI Global, 2025, pp. 83–106. DOI: 10.4018/979-8-3693-6552-6.ch005

[17] C. N. Bodea, M. I. Dascalu, and M. Cazacu, "Increasing the effectiveness of the cybersecurity teaching and learning by applying activity theory and narrative research," Issues Inf. Syst., vol. 20, no. 3, 2019. DOI: 10.48009/3_iis_2019_186-193

[18] S. Zheng and J. Zhao, "A new unsupervised data mining method based on the stacked autoencoder for chemical process fault diagnosis," Computers & Chemical Engineering, vol. 135, p. 106755, 2020, DOI: 10.1016/j.compchemeng.2020.106755.

[19] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "MetaWatch: Trends, Challenges, and Future of Network Intrusion Detection in the Metaverse," IEEE Internet Things J., 2025. DOI: DOI: 10.1109/JIOT.2025.3568477

[20] S. Ayoubi et al., "Machine Learning for Cognitive Network Management," in IEEE Communications Magazine, vol. 56, no. 1, pp. 158-165, Jan. 2018, DOI: 10.1109/MCOM.2018.1700560.

[21] A. Mishra, "AI-Powered Cybersecurity Framework for Secure Data Transmission in IoT Network," Int. J. Adv. Eng. Manag., vol. 7, no. 3, pp. 05–13, 2025. DOI: 10.35629/5252-07030513

[22] F. Mahmood, M. Shehroz, Z. Ansari, and F. Rauf, "A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques," Spectrum Eng. Sci., vol. 2, no. 4, pp. 232–257, 2024. [Online]. Available: https://sesjournal.org/index.php/1/article/view/73

[23] W. Desalegn, J. Shaikh, and B. Taye, Methodology to Improve Control Plane Security in SDN Environments. CRC Press, 2024. DOI: 10.1201/9788770042123

[24] N. Bilal, S. Askar, and K. Muheden, "Challenges and Outcomes of Combining Machine Learning with Software-Defined Networking for Network Security and Management Purpose: A Review," Indones. J. Comput. Sci., vol. 13, no. 2, 2024. DOI: 10.33022/ijcs.v13i2.3845

[25] R. Olaniyi, H. Olugbile, and O. Okwuobi, "The role of artificial intelligence in networking—A review," GEN-Multidisciplinary Journal of Sustainable Development, vol. 3, no. 1, pp. 15–45, 2025. https://gmjsd.org/journal/index.php/gmjsd/article/view/75

[26] G. Kumar and H. Alqahtani, "Machine learning techniques for intrusion detection systems in SDN—Recent advances, challenges and future directions," Computer Modeling in Engineering & Sciences (CMES), vol. 134, no. 1, pp. 1–30, 2023, DOI: 10.32604/cmes.2022.020724.

[27] R. K. Gupta et al., "AI-Based Cognitive Twin Models for Software-Defined IoT Security and Analytics," in 2024 4th Int. Conf. Mobile Netw. Wireless Commun. (ICMNWC), IEEE, 2024, pp. 1–7. DOI: 10.1109/ICMNWC63764.2024.10872194

[28] M. Ma, L. Han, and C. Zhou, "Research and application of Transformer based anomaly detection model: A literature review," arXiv preprint arXiv:2402.08975, 2024.DOI: 10.48550/arXiv.2402.08975

[29] A. H. Abdi et al., "Security control and data planes of SDN: a comprehensive review of traditional, AI and MTD approaches to security solutions," IEEE Access, 2024. DOI: 10.1109/ACCESS.2024.3393548

[30] K. Zdrojewski, "Impact of Artificial Intelligence on Computer Networks," Advances in IT and Electrical Engineering, vol. 30, pp. 49–59, 2024. DOI: 10.7862/re.2023.x

[31] M. Aminu, A. Akinsanya, D. A. Dako, and O. Oyedokun, "Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms," Int. J. Comput. Appl. Technol. Res., vol. 13, no. 8, pp. 11–27, 2024. DOI:10.7753/IJCATR1308.1002

[32] T. Das, V. Sridharan, and M. Gurusamy, "A survey on controller placement in SDN," IEEE Commun. Surv. Tutor., vol. 22, no. 1, pp. 472–503, 2019. DOI: 10.1109/COMST.2019.2935453

[33] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," Information, vol. 14, no. 1, p. 41, 2023. DOI: **10.3390/info14010041**

[34] G. Yi and Y. Pan, "Advanced computer science and applications for soft computing of converged IT environments," Soft Comput., vol. 22, pp. 6617–6619, 2018. DOI: 10.1007/s00500-018-3522-1

[35] T. V. Phan, S. T. Islam, T. G. Nguyen, and T. Bauschert, "Q-DATA: Enhanced traffic flow monitoring in software-defined networks applying Q-learning," in Proc. 2019 15th Int. Conf. Network and Service Management (CNSM), Halifax, NS, Canada, Oct. 2019, pp. 1–9. DOI: 10.23919/CNSM46954.2019.9012727

[36] O. Polat et al., "Hybrid AI-Powered Real-Time Distributed Denial of Service Detection and Traffic Monitoring for Software-Defined-Based

Vehicular Ad Hoc Networks: A New Paradigm for Securing Intelligent Transportation Networks," Appl. Sci., vol. 14, no. 22, p. 10501, 2024. 10.3390/app142210501