iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

INTEGRATING ARTIFICIAL INTELLIGENCE INTO SOFTWARE-DEFINED NETWORKING FOR PROACTIVE SECURITY

Ameya Chaudari
Symbiosis Institute of Technology,
Nagpur Campus, Symbiosis International (Deemed University), Pune, India
Ameya.chaudaru567@gmail.com

ABSTRACT
Centrally Managed Networking decouples the control plane from the data plane, enabling greater programmability and more flexible network management. However, this architectural separation also introduces new security and operational vulnerabilities that can be exploited by malicious actors. Artificial intelligence (AI) offers adaptive detection and intelligent decision-making capabilities that can help mitigate these risks.
This article surveys existing research on the application of AI within SDN to support multi-layer precautionary mechanisms. It discusses key challenges involved in integrating AI with SDN, reviews representative studies in intrusion detection, traffic optimization, and fault management, and compares the performance metrics used to evaluate these approaches. Finally, the paper highlights emerging frameworks and outlines future research directions aimed at building robust and resilient AI-enabled SDN systems.

Keywords:
Artificial Intelligence, Networking, Software-Defined Networking (SDN)

INTRODUCTION

Software-defined networking has its origin as a tool to make network management easier through the separation of the control plane from data forwarding. The SDN controller offers a centralized view and programmatic interface, thus allowing dynamic configuration and monitoring. Nevertheless, the control–data separation of SDN is the reason for new attack surfaces: attackers may focus the controller, take advantage of misconfigurations or exhaust the data plane with malicious flows. As networks become larger and adopt network slicing and virtualized functions, the complexity of threat management also escalates. To identify anomalies, predict traffic patterns and orchestrate policies in real time, a larger number of AI and machine learning algorithms are implemented. The inclusion of AI in SDN is a way to achieve self-learning, adaptive networks with less human intervention and better reliability. Still, this coupling is faced with problems such as data imbalance, latency, and explanability. The challenges discussed here are recognized by the follow-up research, which also gives pointers on how to handle them.

Sources and Challenges in AI–SDN Integration

The AI–SDN systems are confronted with technological and moral issues. The architectural problems arise due to the layered construction of SDN. By centralizing control, the system becomes more flexible but also a single point of failure and a target for DDoS as well as unauthorized-access attacks. The incorporation of AI entails extra computing power and causes latency; hence the models have to operate in real-time without traffic forwarding being put on hold. Challenges related to data come from the fact that AI models rely on training data, which may be biased or incomplete. Inaccurate representation may result in false positives or the models may fail to detect new kinds of attacks. On top of that, privacy issues arise if sharing traffic data with a centralized AI engine. The tasks related to the algorithm aim at achieving fair, transparent, and robust models. Black-box models might produce decisions that are difficult to audit, while adversarial inputs might be misclassified. Last but not least, operational issues concern the compatibility with old systems, absence of standardization and the necessity for constant updates of models to be capable of handling emerging threats and network changes.

Case Studies: Intrusion Detection, Traffic Optimization and Fault Management

Intrusion Detection: Hierarchical AI–SDN Firewall

The 2025 research presented a tiered AI–SDN Security system combining the programmability of SDN with hierarchical AI models for network security with a self-adaptability feature. The system divides the security functions into the layers: The Root layer consists of edge sensors that filter traffic, the Trunk layer applies

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

reinforcement learning to a federated SDN control plane for policy optimization, and the Canopy layer uses the ensemble of convolutional, recurrent, and graph neural networks for zero-day attack detection. This structure not only achieves instant control and anomaly detection but also the root sensors operate at 98.2 % accuracy, the federated control plane has 12 ms response time, and the canopy layer reaches 99.4 % recall with 92 % of the encrypted PMS. The overall precision in threat detection amounts to 99.2 % with a false-alarm rate of 0.8 %, and policy changes are carried out at 5.2× the speed of regular firewalls. The learning component of the firewall is the machine-learning models that allow it to learn from traffic patterns and get used to the new threats while the latency stays at a minimum. Generalized AI–SDN architecture for such intrusion-detection systems is depicted in the figure 1.

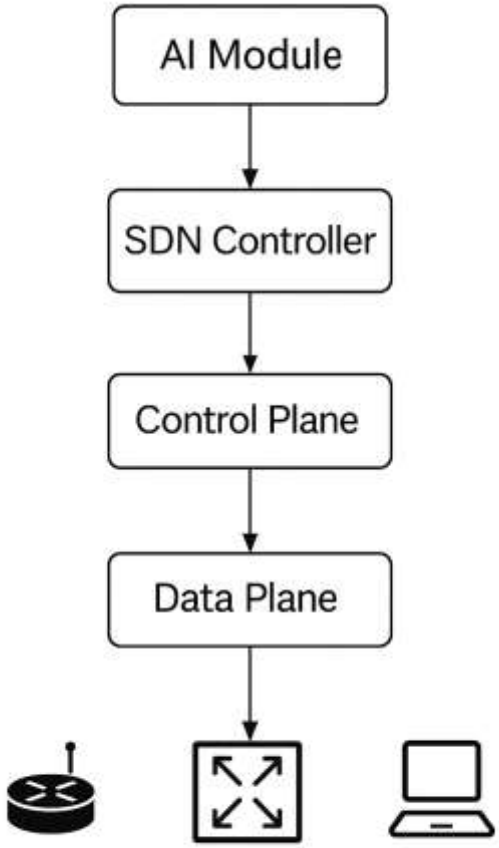

Figure 1. AI-SDN architecture for intrusion detection.

Traffic Optimization: Dynamic Fuzzy Routing with Deep Reinforcement Learning

In software-defined networks, quality-of-service (QoS) depends heavily on the routing of data. The traditional shortest-path routing method is unaware of the network load changes and cannot provide the QoS requirements. To cope with this issue, Wang et al. introduced the Dynamic Fuzzy Routing algorithm based on Deep Reinforcement Learning (DFRDRL) for SDN. DFRDRL combines a deep reinforcement learning (DRL) agent with fuzzy logic to forecast the traffic matrix in real-time and decide on the routes that will ensure latency and bandwidth. The method takes into account the state of the path, uses the network nodes weights based on their significance, and implements a deferral mechanism that temporarily bans high-resource flows during congestion. The results of the simulations demonstrate that DFRDRL is successful in lowering latency and raising throughput as compared to the existing algorithms and thus, it enables 2.5 % more routing requests to be fulfilled. The main steps of the DFRDRL algorithm are represented in Figure 2.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

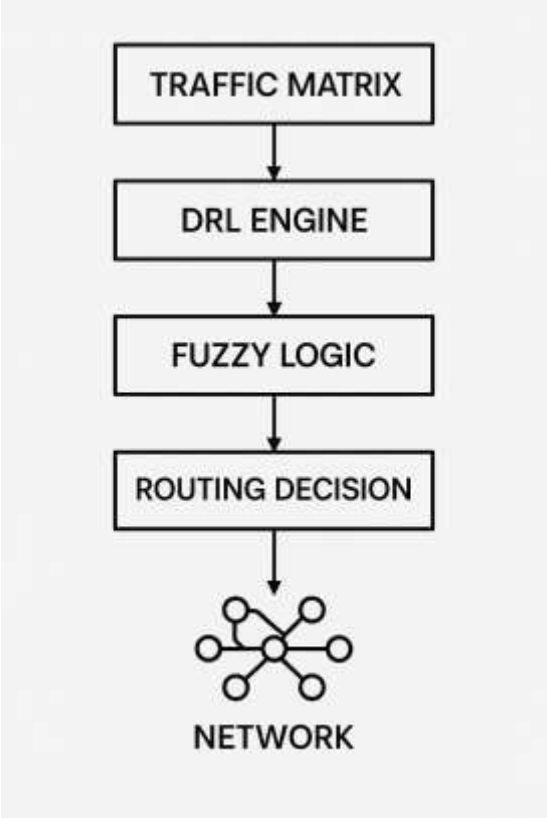

Figure 2. Dynamic fuzzy routing algorithm using deep reinforcement learning.

Fault Management: Game-Based Fault Recovery in Multi-Domain SDN

SDN controllers are the main point of concern when it comes to network stability; hence, a failure of a controller may lead to the collapse of the entire domain. To address this issue, Xu et al. presented a fault recovery algorithm that is autonomous and enhanced by the game concept for the multi-domain SDN controllers. The proposed approach, upon a controller failure, generates a< i> controller game domain using the remaining controller capacities and device transition relations. The problem of mapping out-of-control switches to a target controller is defined as a linear programming model, and it is solved through a multi-population particle swarm optimization algorithm. After that, migration activities are carried out according to the best mapping. The comparative experiments results show that the suggested method can effectively manage the trade-off between migration costs and controller load while decreasing propagation delay and, moreover, fault-recovery time, to a large extent. The main idea of game-based recovery illustrated in Figure 3.

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

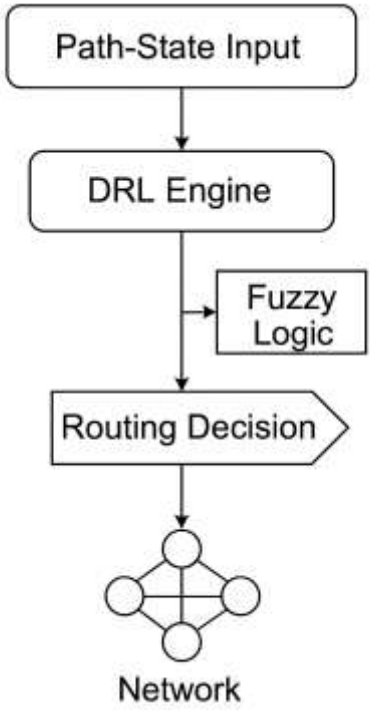

Figure 3. Game-based fault recovery algorithm for multi-domain SDN controllers.

Impact on Network Reliability, Security and Trust

The incorporation of AI in SDN makes the latter more reliable as it performs proactive detection and autonomous response. The Forest Tree AI–SDN Firewall is characterized by high precision and low false-alarm rate, which, in turn, reduce the chances of the attackers being missed and also minimize the unnecessary disruptions. The capability of the system to learn from traffic patterns and to update policies fast helps the system to become more resilient against the ever-changing threats. DFRDRL takes QoS to the next level by intelligently balancing latency and bandwidth requirements and thus, keeping resource utilization efficient during traffic peaks. The game-based fault-recovery algorithm can thus be compared to a battery that can be recharged quickly while at the same time alleviating the load on the rest of the system. These reliability enhancements also have an impact on user trust: systems that are capable of self-intrusion detection, optimization of traffic and fault recovery, thus, users can rely more on the service availability and data security. Nevertheless, the black-box nature of AI decisions might result in trust erosion; hence, explainable AI and transparent logging are the main factors responsible for keeping the network accountable.

Mitigation Frameworks and Intelligent Control Strategies

The examples of research presented in this article have confirmed the existence of various ways of mitigation. Fully integrated security architectures from the physical to the application level, combining SDN, network function virtualization (NFV), and AI, provide intrusion detection advantages through synergistic analysis of heterogeneous data sources. Hence, these frameworks can handle threats that cut across physical, control, and application planes, plus they can deploy different AI models for intrusion detection, traffic forecasting, and policy enforcement. The hierarchical AI–SDN firewall features illustrate that accuracy in detection and promptness of reaction can be attained through the combination of light and simple sensors at the edge, reinforcement learning, and deep learning ensembles. The DFRDRL algorithm provides an example of how DRL and fuzzy logic can jointly bring about optimization in routing decisions so as to facilitate real-time QoS provisioning. The game-based recovery method shows that optimization techniques in concert with intelligence can not only accomplish the task of recovering from the fault but also maintain the system's stability. The discussed strategies collectively stress the necessity for adaptable, multi-layered, and explainable AI frameworks. Among the ethical stipulations is the provision of fairness in detection (i.e., not discriminating certain traffic patterns), ensuring the privacy of encrypted traffic while performing the analysis, and offering the audit trails for the AI-powered

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

decision-making. Open and standardized interfaces, as well as interoperable protocols, will make it easier for the integration to work across various network domains.

Comparative Table: Performance Metrics in AI–SDN Systems

Metric	**Intrusion Detection** (AI–SDN Firewall)	**Traffic Optimization** (DFRDRL Algorithm)	**Fault** Recovery (Game-Based)
Detection/Accuracy	The edge sensors operate at 98.2 % accuracy; the canopy layer achieves 99.4 % recall with 92 % coverage; overall detection precision is 99.2 % with false alarms at 0.8 %.	Non-applicable (focus on routing efficiency).	Fault detection is at the core of optimization; it achieves high detection accuracy and rapid recovery.
ResponseLatency	The federated reinforcement learning control is quick to respond in 12 ms; the overall firewall latency can be as low as 0.2 ms.	Routes were selected to ensure both latency and bandwidth were satisfied; the simulations show lower latency than the baseline algorithms.	Propagation delay and fault-recovery time are shortened to a great extent compared to the existing schemes.
Throughput/Efficiency	TLS 1.3 inspection is able to handle 40 Gbps; the policy updates are 5.2× faster than the conventional firewalls.	Throughput is enhanced and 2.5 % more routing requests can be fulfilled.	Mobilization expenses are efficiently managed and the loading of controllers is evenly distributed; the service continuity is ensured during the occurrence of faults.
AdditionalNotes	An ensemble of CNN, LSTM and GNN models is used to detect zero-day threats; supervised learning achieves ≥96.79 % accuracy.	The work involves a combination of DRL with fuzzy logic to forecast traffic matrix and perform deferral during congestion.	Creates a controller game domain; particle swarm optimization is used for mapping and migration.

Future Directions for Resilient AI–SDN Ecosystems

The integration of AI and SDN is at its nascent stage and has not yet reached perfection. Explainable AI should be the main focus of the future work where the models not only provide interpretation but also keep transparent logs of decisions. Federated and distributed learning can be used to train models across multiple controllers without the need for sharing raw data, thus, privacy will be ensured. The availability of digital twins and simulation environments will make it possible to test AI policies safely before they go live. Besides that, the implementation of zero-trust architectures and blockchain might be the keys to better authentication and accountability in SDN domains. The arrival of 6G networks will require cross-layer frameworks to consider various aspects such as terahertz communications, quantum-safe cryptography and AI-driven orchestration. On the other hand, energy-saving AI models and eco-friendly networking techniques will be essential for the continued operation to be in line with the principles of sustainability. Last but not least, the development of standards and open platforms will pave the way for the AI–SDN ecosystems to be interoperable and facilitate the collaboration among the researchers and the industry.

Conclusion

The integration of artificial intelligence into software-defined networking opens the way for the successful implementation of the multi-precautionary measures in modern networks. AI empowers SDN's programmability

iJETRM
International Journal of Engineering Technology Research & Management
(IJETRM)
https://ijetrm.com/

with features such as adaptive intrusion detection, intelligent traffic engineering, and autonomous fault management. The case studies provide evidence for achieving high detection accuracies, low latencies, and improved reliabilities. Nevertheless, AI incorporation in SDN poses challenges concerning the quality of data, latency, transparency of algorithms, and interoperability. The solution to these problems lies in cross-layer security frameworks, hybrid learning algorithms, and taking into account the ethical aspects. Moreover, with further research on explainable and energy-efficient AI models, federated learning, and standardized interfaces, AI-SDN systems could be seen as the core of secure and resilient 5G/6G networks.

REFERENCES

1) Fnu, H., Soni, V., Asundi, S., Thummarakoti, S., Kaushik, K., & Soni, M. (2025, May). Design and Deployment of AI-Driven Fraud Detection Models in Cloud-Based Banking Ecosystems. In *2025 International Conference on Networks and Cryptology (NETCRYPT)* (pp. 223-228). IEEE.
2) Narasimha Rao Vanaparthi. Why digital transformation in fintech requires mainframe modernization: A cost-benefit analysis. International Journal of Science and Research Archive, 2025, 14(01), 1052-1062. Article DOI: https://doi.org/10.30574/ijsra.2025.14.1.0161.
3) Cheekati, S., Borra, C. R., Kumar, S., Rayala, R. V., Sangula, S. K., & Kulkarni, V. (2025, May). Intelligent Cybersecurity for IoT: A Hybrid QRIME-SDPN Approach for Network Attack Detection on CIC-IoT-2023. In *2025 13th International Conference on Smart Grid (icSmartGrid)* (pp. 774-781). IEEE**.**
4) Ande, B.R. (2025). AI-Driven Continuous Authentication: Integrating Deep Learning with Multimodal Biometrics for Enhanced Identity Verification. In: Mishra, D., Yang, X.S., Unal, A., Jat, D.S. (eds) Data Science and Big Data Analytics. IDBA 2025. Learning and Analytics in Intelligent Systems, vol 56. Springer, Cham. https://doi.org/10.1007/978-3-032-05373-2_42
5) Kabade, S., Sharma, A., & Kagalkar, A. (2025). Cloud-Native AI Solutions for Sustainable Pension Investment Strategies. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 6(1). https://doi.org/10.63282/3050-9262.IJAIDSML-V6I1P121
6) Gopal Varma, S. C.; Chaudhari, B. Federated Learning in Financial Data Privacy: A Secure AI Framework for Banking Applications. *IJETCSIT* **2025**, 101-110. https://doi.org/10.56472/ICCSAIML25-112
7) Borra, C. R., Cheekati, S., Pareek, P. K., Rayala, R. V., Kothuri, S. R., & Kumar, S. V. (2025, May). An Intelligent IoT Attack Detection Model Using Weighted ELM and Educational Achievement Guided Optimization. In *2025 13th International Conference on Smart Grid (icSmartGrid)* (pp. 789-796). IEEE.
8) Kagalkar, A., Kabade, S., Chaudhri, B., & Sharma, A. (2023). AI-Driven Automation for Death Claim Processing In Pension Systems: Enhancing Accuracy and Reducing Cycle Time. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(4), 105-110. https://doi.org/10.63282/3050-9262.IJAIDSML-V4I4P112
9) Rayala, R. V., Borra, C. R., Pareek, P. K., & Cheekati, S. (2024, November). Hybrid Optimized Intrusion Detection System Using Auto-Encoder and Extreme Learning Machine for Enhanced Network Security. In 2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET) (pp. 1-7). IEEE.
10) Narasimha Rao Vanaparthi. (2025). The Roadmap to Mainframe Modernization: Bridging Legacy Systems with the Cloud. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *11*(1), 125-133. https://doi.org/10.32628/CSEIT25111214