International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 4560-4566
http://www.ijcesen.com

ISSN: 2149-9144

Review Article

Adaptive and intelligent security frameworks for SDN-NFV enabled next-generation networks: A Review

Revathi. N[1*], M.Elamparithi[2],V.Anuratha[3]

[1]Research Scholar, Department of Computer Science, Kamalam College of Arts and Science, Udumalpet, Affiliated to Bharathiar University, Coimbatore.
* **Corresponding Author Email:** revsnataraj@gmail.com - **ORCID:** 0000-0002-5247-9950

[2]Associate Professor, Department of Computer Science, Kamalam College of Arts and Science, Udumalpet, Affiliated to Bharathiar University, Coimbator
Email: profelamparithi@gmail.com - **ORCID:** 0000-0002-5247-1150

[3]Associate Professor, Department of Computer Science, Kamalam College of Arts and Science, Udumalpet, Affiliated to Bharathiar University, Coimbatore,
Email: profanuratha@gmail.com - **ORCID:** 0000-0002-5247-2250

Article Info:

DOI: 10.22399/ijcesen.5189
Received : 05 November 2025
Revised : 25 December 2025
Accepted : 27 December 2025

Keywords

Adaptive security,
intelligent security,
SDN-NFV

Abstract:

The rapid evolution of telecommunication technologies towards 5G and 6G has necessitated a paradigm shift from rigid hardware-based infrastructures to flexible, software-defined architectures. This transition is primarily driven by Software-Defined Networking (SDN) and Network Function Virtualization (NFV), which enable dynamic resource management and programmability. However, the centralization of control in SDN and the distributed nature of NFV introduce novel security vulnerabilities, particularly in Zero-Touch Networks (ZTN) and Cloud-Enabled IoT environments. This review paper critically analyzes the current state of adaptive networking protocols, focusing on the integration of Artificial Intelligence (AI) and Machine Learning (ML) for intrusion detection and threat mitigation. We examine recent methodologies, including Deep Learning (DL), Bio-inspired algorithms, and Blockchain-based trust mechanisms, evaluating their efficacy in addressing scalability, latency, and data integrity. The review identifies critical research gaps in real-time adaptivity and computational efficiency, proposing a unified, lightweight framework for intelligent orchestration in next-generation communication systems.

1. Introduction

The telecommunications landscape is undergoing a revolutionary transformation, driven by the exponential growth of the Internet of Things (IoT), the deployment of 5G networks, and the conceptualization of 6G systems. Traditional network architectures, characterized by proprietary hardware and static configurations, are increasingly incapable of meeting the diverse and demanding requirements of modern applications, such as ultra-low latency, massive connectivity, and high bandwidth. To address these challenges, the industry has embraced Network Softwarization, a fundamental shift enabled by two complementary technologies: Software-Defined Networking (SDN) and Network Function Virtualization (NFV).

As illustrated in Figure 1, the progression from 1G to 6G represents not just an increase in speed, but a fundamental change in architectural flexibility. SDN decouples the network control plane from the data forwarding plane, centralizing network intelligence in software-based controllers. This separation allows for direct programmability of network traffic, enabling operators to dynamically adjust policies and routing in real-time. Concurrently, NFV abstracts network functions (e.g., firewalls, load balancers, routers) from dedicated hardware, allowing them to run as virtual machines (VMs) or containers on standard servers. Together, SDN and NFV form the backbone of Cloud-Enabled Networks, offering unprecedented flexibility, scalability, and cost-efficiency.

However, this architectural evolution introduces significant security paradigms. The centralized

SDN controller becomes a single point of failure and a high-value target for Distributed Denial of Service (DDoS) attacks. Furthermore, the expansion of the attack surface in IoT-dense "Smart City" environments necessitates robust, automated security mechanisms. Traditional perimeter defenses are insufficient against sophisticated, multi-vector attacks in these distributed environments. Consequently, there is a critical need for Adaptive Networking Protocols that leverage Artificial Intelligence (AI) to predict, detect, and mitigate threats autonomously—a concept often referred to as Zero-Touch Network Security (ZTNS).

2: Related work and literature survey

The domain of SDN/NFV security has witnessed a surge in research, particularly focusing on AI-driven Intrusion Detection Systems (IDS). Early approaches relied on statistical analysis and machine learning (ML) algorithms like Support Vector Machines (SVM) and Random Forests. However, the complexity of modern attacks has shifted the focus towards Deep Learning (DL) and hybrid architectures.

One significant trend is the move towards Zero-Touch Networks (ZTN), where networks self-configure and self-heal. Qazi et al. (2024) proposed a ZTNS framework using a multi-layered CNN, achieving 99.8% accuracy on the CICIDS-2018 dataset, demonstrating the viability of DL for high-volume traffic analysis. Similarly, Nayak et al. (2024) introduced a bio-inspired approach, the Binarized Deep Spiking Capsule Fire Hawk Neural Network (BSHNN), combined with blockchain for 5G SDN, addressing both detection accuracy and data integrity.

3: Methods incorporated

The reviewed literature reveals a convergence of three primary methodological pillars in developing adaptive networking protocols: Deep Learning Architectures, Network Softwarization (SDN/NFV), and Trust Technologies (Blockchain).

3.1. SDN/NFV Orchestration:

The methodology for *deployment* relies heavily on the SDN/NFV architecture. The SDN controller acts as the centralized brain, while NFV allows security tools to be deployed instantly as software.

Figure 2 depicts the high-level architecture where the Control Plane interacts with the Data Plane via the Southbound Interface (OpenFlow), and with applications via the Northbound Interface. This separation is crucial for inserting AI-driven modules that can monitor global network states without affecting individual switch performance.

3.2. Deep Learning for Anomaly Detection:

The core method for "adaptive" security is the replacement of static signature-based detection with dynamic Deep Learning models.

- Convolutional Neural Networks (CNN): Used to extract spatial features from network traffic flows.
- Spiking Neural Networks (SNN): Utilized for their energy efficiency and ability to model complex temporal dynamics in 5G traffic.

Figure 3 illustrates a typical Zero-Touch Network Security (ZTNS) workflow. Traffic is ingested from the SDN data plane, pre-processed, and analyzed by the Deep Learning engine. Upon detecting an anomaly (e.g., DDoS), the system automatically pushes mitigation rules back to the SDN controller, closing the loop without human intervention.

3.3. Blockchain for Distributed Trust:

To prevent "Flow Table Poisoning" (where attackers inject malicious rules into the SDN controller), methodologies now incorporate Distributed Ledger Technology (DLT). Flow rules are encrypted and hashed onto a ledger, ensuring that switches can verify the integrity of a rule before execution.

4: Discussion

4.1 Advantages & problems

Advantages: The primary advantage of AI-enhanced SDN/NFV frameworks is agility. Unlike hardware appliances, software-based IDS can be updated instantly across the entire network. AI models provide predictive capabilities, detecting unknown "zero-day" attacks that bypass static firewalls.

Problems: The centralization of the SDN controller creates a bottleneck. If the AI model requires heavy computation, the controller may become overwhelmed during high-traffic volumetric attacks. Additionally, Data Imbalance in training sets leads to biased models.

4.2 Challenges

- Real-Time Latency: 5G and 6G require ultra-low latency (<1ms). Complex AI inference and blockchain consensus can introduce delays of several seconds.

- Adversarial AI: Attackers are now using AI to generate "Adversarial Examples" designed to fool the IDS.
- Scalability: As IoT devices multiply, the volume of flow logs becomes unmanageable for centralized processing.

4.3 Research gap and future directions

A critical gap exists in the development of "Lightweight, Online-Adaptive AI" for SDN. Existing models are accurate but heavy. There is a lack of Hybrid Models (e.g., Quantized Transformers) that can run on the Network Edge.

Future Directions:

- Federated Learning (FL): Moving training to the edge to preserve privacy.
- Lightweight Trust: Replacing Proof-of-Work blockchains with DAG-based ledgers.

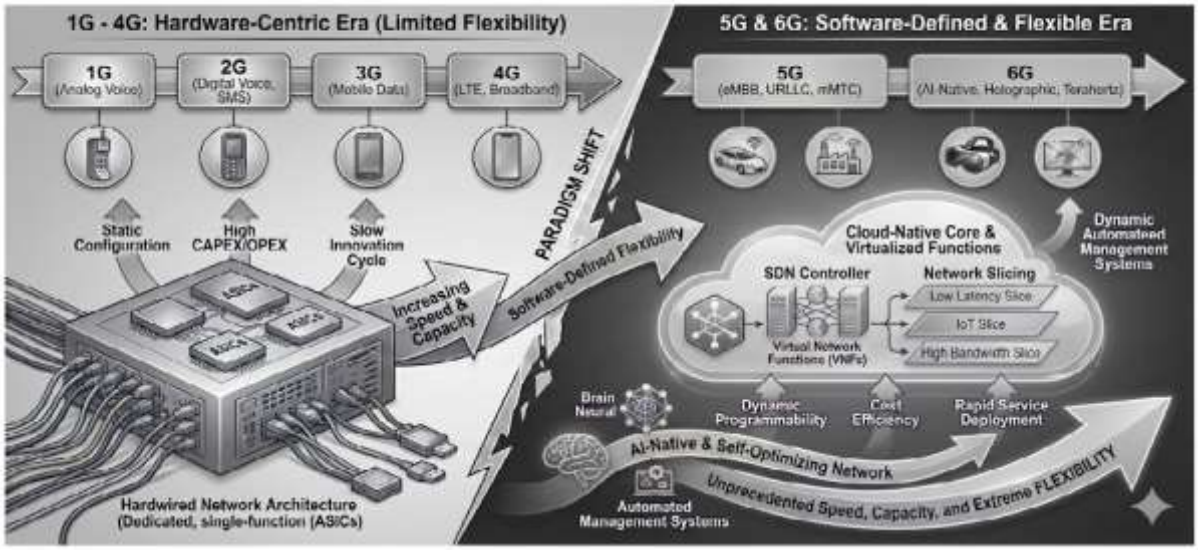

Figure 1: *The Architectural Paradigm Shift from 1 G to 6G*

Table 1: *Literature Survey of Recent Adaptive Security Frameworks (2020–2026)*

Author & Year	Methodology / Technique	Dataset Used	Key Focus / Contribution	Limitations / Gaps
Lorincz et al. (2026)	SDN/NFV Softwarization & AI-driven Energy Optimization	N/A (Review/ Architecture)	Analyzed the impact of softwarization on energy efficiency in 5G/6G; proposed AI for dynamic resource scaling.	Lack of experimental validation for specific AI energy models in real-world B5G scenarios.
Qazi et al. (2024)	Zero-Touch Network Security (ZTNS) using **CNN**	CICIDS-2018	Proposed a 5-layer CNN for autonomous intrusion detection in Smart City ZTNs. Achieved 99.8% accuracy.	Focused primarily on detection; lacked a proactive mitigation or "response" mechanism for zero-day attacks.
Nayak et al. (2024)	**BSHNN** (Binarized Deep Spiking Capsule Fire Hawk Network) + **Blockchain**	Real-time traffic / Simulation	Integrated bio-inspired AI for classification and Blockchain for securing flow rules in 5G SDN.	High authentication time (16.2s) due to blockchain consensus is a bottleneck for URLLC applications.
Janabi et al. (2024)	Survey of IDS in SDN (ML/DL approaches)	Review of KDD'99, NSL-KDD, CICIDS2017	Comprehensive taxonomy of SDN attacks (DDoS, U2R, Probe) and evaluation of ML/DL efficacy.	Identified that many studies still use outdated datasets and lack scalability analysis for distributed controllers.
Kumar et al. (2025)	AI-driven Security for **6G** (Survey)	N/A (Survey)	Explored AI's role in 6G enablers (THz, VLC, Quantum). Proposed a roadmap for AI-centric 6G security.	Theoretical framework; lacks specific implementation details for the proposed "AI-enabled security layer."
Chatzimiltis et al. (2024)	**SDN-IDS** with Ensemble Learning	Custom SDN Dataset	Used feature selection and data resampling (SMOTE)	Relied on traditional ML (Random Forest/XGBoost)

	(XGBoost, RF)		to handle imbalanced traffic in SDN.	which may struggle with complex, high-dimensional 6G data compared to DL.
Attou et al. (2023)	Intelligent IDS for Cloud Computing	N/A	Focused on detecting malicious activities in cloud environments using intelligent systems.	Specific architectural details for SDN integration were limited.
Awajan (2023)	Deep Learning-based IDS for IoT	CSE-CIC-IDS2018	Designed a DL model specifically for heterogeneous IoT networks.	Detection rate for rare attack classes needs improvement; limited focus on "zero-touch" automation.
Al-Qatf et al. (2018)	Sparse Autoencoder + SVM	NSL-KDD	Combined deep feature extraction (Autoencoder) with efficient classification (SVM).	Used an older dataset (NSL-KDD) which does not reflect modern SDN/5G traffic patterns.
Tang et al. (2016)	Deep Neural Network (DNN) for SDN	NSL-KDD	Early application of Deep Learning specifically for SDN-based flow analysis.	High false alarm rates compared to modern hybrid models; lacked real-time processing capabilities.

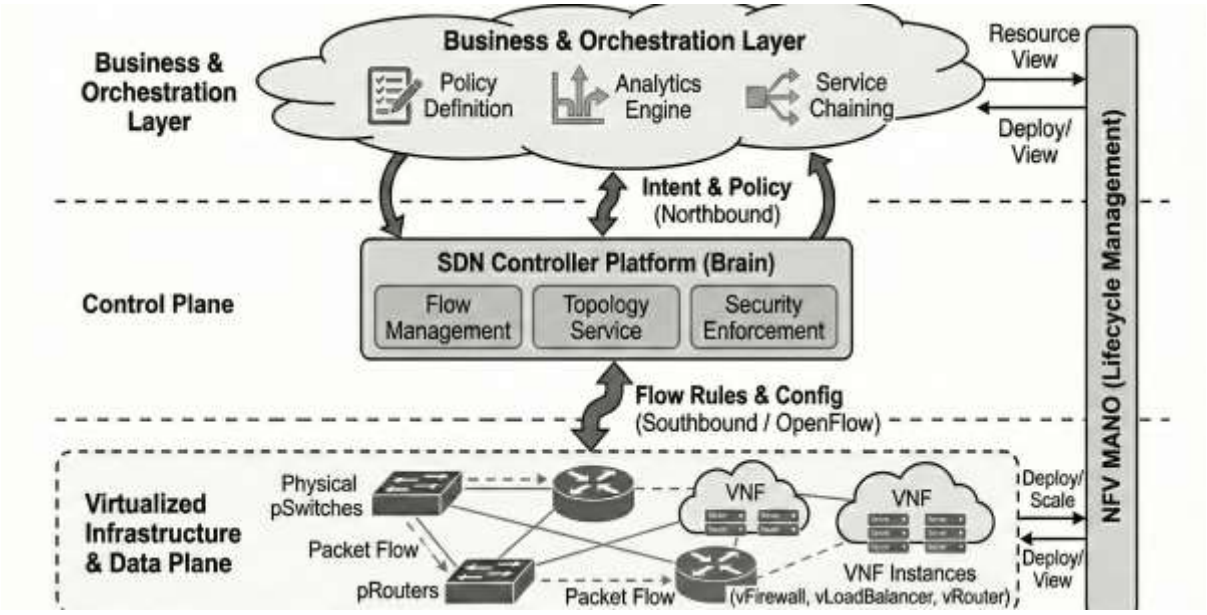

Figure 2: *Functional View of SDN/NFV interaction Flow*

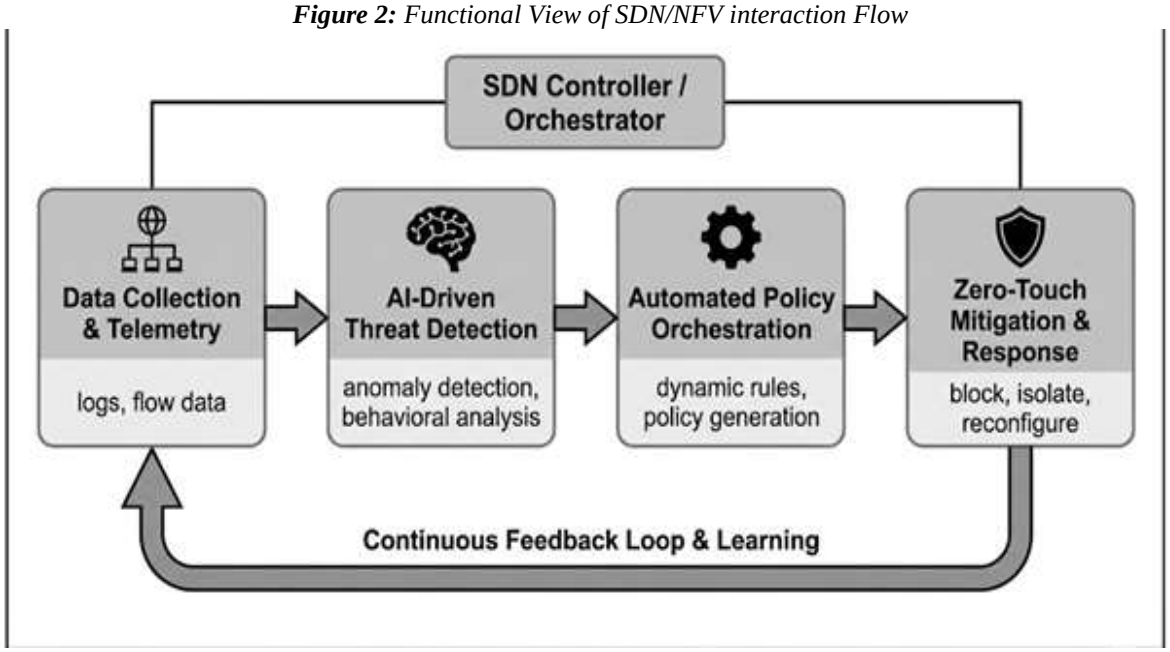

Figure 3: *Zero-Touch Network Security (ZTNS) Workflow*

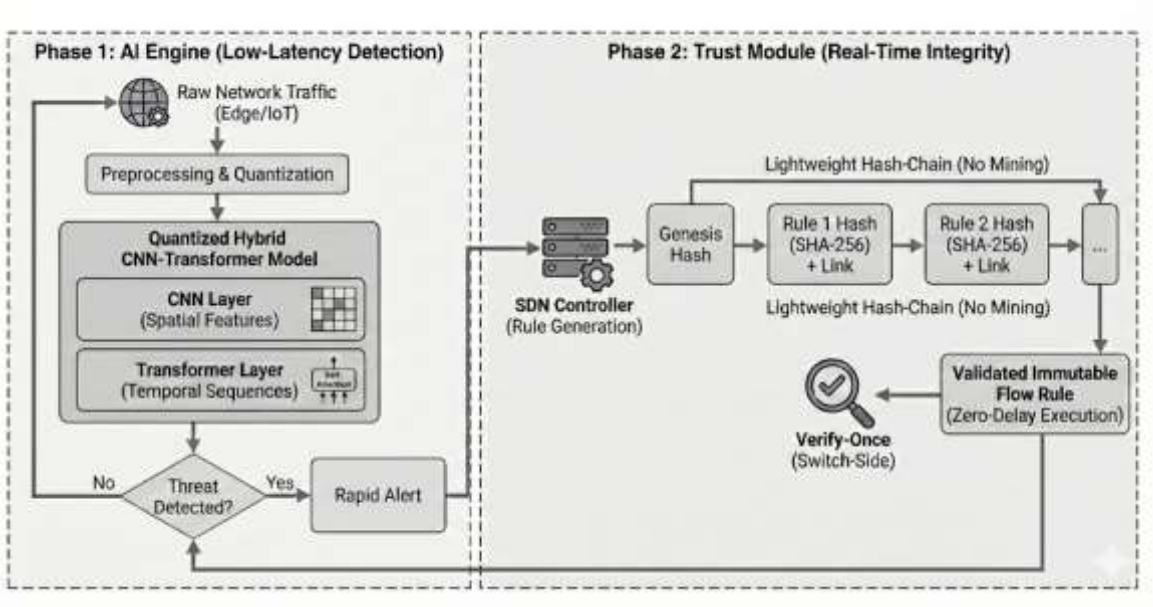

Figure 4 : *Proposed Lightweight Hybrid AI & Trust Model (Solution Architecture)*

4.4 Recommendations

Based on the review, the following research phases are recommended for further study, as visualized below:
Figure 4 represents the proposed Lightweight Hybrid AI & Trust Model.

- Phase 1: Development of a Quantized CNN-Transformer model (shown in the AI Engine block) to combine spatial and temporal analysis with low latency.
- Phase 2: Integration of a "Verify-Once" Hash-Chain (shown in the Trust Module) to replace heavy blockchain consensus, enabling millisecond-level rule verification.

5. Conclusions

The transition to 6G requires network security that is as dynamic as the network itself. This review established that while SDN provides flexibility, it introduces centralized vulnerabilities. The integration of Artificial Intelligence has proven effective in Zero-Touch Networks, but current solutions suffer from high computational overhead and latency. To realize the vision of "Intelligent, Scalable, and Secure" networking, future research must pivot towards decentralized intelligence and lightweight cryptographic primitives, as proposed in the hybrid framework.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

1. Lorincz, J., Kukuruzović, A., & Begušić, D. (2026). Mobile Network Softwarization: Technological Foundations and Impact on Improving Network Energy Efficiency. *Sensors*, 26(2), 503.
2. Qazi, E. U. H., Zia, T., Faheem, M. H., Shahzad, K., Imran, M., & Ahmed, Z. (2024). Zero-Touch Network Security (ZTNS): A Network Intrusion Detection System Based on Deep Learning. *IEEE Access*, 12, 141625-141638.
3. Nayak, N. K., & Bhattacharyya, B. (2024). An Intrusion Detection System for 5G SDN Network Utilizing Binarized Deep Spiking Capsule Fire Hawk Neural Networks and Blockchain Technology. *Future Internet*, 16(10), 359.

4. Janabi, A. H., et al. (2024). Survey: Intrusion Detection System in Software-Defined Networking. *IEEE Access*, 12, 164103.
5. Kumar, R., Dutta, J., Vamsi, N., Varri, U. S., & Puthal, D. (2025). Next-Generation Security in the 6G Era: The Role of AI in Safeguarding Future Networks. *IEEE Access*. (Early Access).
6. Chatzimiltis, S., Shojafar, M., Mashhadi, M. B., & Tafazolli, R. (2024). A Collaborative Software Defined Network-Based Smart Grid Intrusion Detection System. *IEEE Open Journal of the Communications Society*, 5, 700-711.
7. Attou, H., Mohy-Eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., & Almusallam, N. (2023). Towards an intelligent intrusion detection system to detect malicious activities in cloud computing. *Applied Sciences*, 13(17), 9588.
8. Awajan, A. (2023). A novel deep learning-based intrusion detection system for IoT networks. *Computers*, 12(2), 34.
9. Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. *IEEE Access*, 6, 52843-52856.
10. Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2016). Deep learning approach for Network Intrusion Detection in Software Defined Networking. *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 258-263.
11. Brik, B., et al. (2024). Federated Learning for 6G Security: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*.
12. Yang, Y., Gu, Y., & Yan, Y. (2023). Machine learning-based intrusion detection for rare-class network attacks. *Electronics*, 12(18), 3911.
13. Li, S., Cao, Y., Liu, S., Lai, Y., Zhu, Y., & Ahmad, N. (2024). HDA-IDS: A hybrid DoS attacks intrusion detection system for IoT by using semi-supervised CL-GAN. *Expert Systems with Applications*, 238, 122198.
14. Kumar, R., Aljuhani, A., Javeed, D., Kumar, P., Islam, S., & Islam, A. K. M. N. (2024). Digital twins-enabled zero touch network: A smart contract and explainable AI integrated cybersecurity framework. *Future Generation Computer Systems*, 156, 191-205.
15. Smys, D. S., Basar, D. A., & Wang, D. H. (2020). Hybrid intrusion detection system for Internet of Things (IoT). *Journal of ISMAC*, 2(4), 190-199.
16. Kim, J., Kim, J., Kim, H., Shim, M., & Choi, E. (2020). CNN-based network intrusion detection against denial-of-service attacks. *Electronics*, 9(6), 916.
17. Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions. *Electronics*, 9(7), 1177.
18. Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, 111(4), 2287-2310.
19. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150.
20. Tama, B. A., Nkenyereye, L., Islam, S. M. R., & Kwak, K.-S. (2020). An enhanced anomaly detection in web traffic using a stack of classifier ensemble. *IEEE Access*, 8, 24120-24134.
21. Souhail, M., Rachidi, T., & Assem, N. (2019). Network based intrusion detection using the UNSW-NB15 dataset. *International Journal of Computing and Digital Systems*, 8(5), 477-487.
22. Leghris, C., Elaeraj, O., & Renault, E. (2019). Improved security intrusion detection using intelligent techniques. *Proceedings of International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 1-5.
23. Khater, B. S., Wahab, A. W. B. A., Idris, M. Y. I. B., Hussain, M. A., & Ibrahim, A. A. (2019). A lightweight perceptron-based intrusion detection system for fog computing. *Applied Sciences*, 9(1), 178.
24. Chafika, B., Taleb, T., Phan, C.-T., Tselios, C., & Tsolis, G. (2021). Distributed AI-based security for massive numbers of network slices in 5G & beyond mobile systems. *Proceedings of Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 401-406.
25. Kumar, R., Kumar, P., Aloqaily, M., & Aljuhani, A. (2023). Deep-learning-based blockchain for secure zero touch networks. *IEEE Communications Magazine*, 61(2), 96-102.
26. Khan, N. W., Alshehri, M. S., Khan, M. A., Almakdi, S., Moradpoor, N., Alazeb, A., Ullah, S., Naz, N., & Ahmad, J. (2023). A hybrid deep learning-based intrusion detection system for IoT networks. *Mathematical Biosciences and Engineering*, 20(8), 13491-13520.
27. Yang, X., Peng, G., Zhang, D., & Lv, Y. (2022). An enhanced intrusion detection system for IoT networks based on deep learning and knowledge graph. *Security and Communication Networks*, 2022, 1-21.
28. Gallego-Madrid, J., Sanchez-Iborra, R., Ruiz, P. M., & Skarmeta, A. F. (2022). Machine learning-based zero-touch network and service management: A survey. *Digital Communications and Networks*, 8(2), 105-123.
29. El Houda, Z. A., Brik, B., & Khoukhi, L. (2022). Ensemble learning for intrusion detection in SDN-based zero touch smart grid systems. *Proceedings of IEEE 47th Conference on Local Computer Networks (LCN)*, 149-156.
30. Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IoT: A survey. *Wireless Personal Communications*, 115(2), 1667-1693.

31. ElKashlan, M., Elsayed, M. S., Jurcut, A. D., & Azer, M. (2023). A machine learning-based intrusion detection system for IoT electric vehicle charging stations (EVCSs). *Electronics*, 12(4), 1044.
32. Bugshan, N., Khalil, I., Kalapaaking, A. P., & Atiquzzaman, M. (2023). Intrusion detection-based ensemble learning and microservices for zero touch networks. *IEEE Communications Magazine*, 61(6), 86-92.
33. Alkahtani, H., & Aldhyani, T. H. H. (2021). Botnet attack detection by using CNN-LSTM model for Internet of Things applications. *Security and Communication Networks*, 2021, 1-23.
34. Alkahtani, H., & Aldhyani, T. H. H. (2021). Intrusion detection system to advance Internet of Things infrastructure-based deep learning algorithms. *Complexity*, 2021(1), 1-18.
35. Potnurwar, A. V., Bongirwar, V. K., Ajani, S., Shelke, N., Dhone, M., & Parati, N. (2023). Deep learning-based rule-based feature selection for intrusion detection in industrial Internet of Things networks. *International Journal of Intelligent Systems and Applications in Engineering*, 11(10), 23-35.
36. Chawla, S. (2017). *Deep learning based intrusion detection system for Internet of Things*. M.S. thesis, University of Washington.
37. Hussain, J., & Hnamte, V. (2021). Deep learning based intrusion detection system: Software defined network. *Proceedings of Asian Conference on Innovation in Technology (ASIANCON)*, 1-6.
38. Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks detection in IoT-based smart city applications using machine learning techniques. *International Journal of Environmental Research and Public Health*, 17(24), 9347.
39. Gupta, S. K., Tripathi, M., & Grover, J. (2022). Hybrid optimization and deep learning based intrusion detection system. *Computers and Electrical Engineering*, 100, 107876.
40. Elsaeidy, A. A., Jagannath, N., Sanchis, A. G., Jamalipour, A., & Munasinghe, K. S. (2020). Replay attack detection in smart cities using deep learning. *IEEE Access*, 8, 137825-137837.
41. Reddy, D. K., Behera, H. S., Nayak, J., Vijayakumar, P., Naik, B., & Singh, P. K. (2021). Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications of future smart cities. *Transactions on Emerging Telecommunications Technologies*, 32(7), e4121.
42. Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of effective machine learning algorithm and bot-IoT attacks traffic identification for Internet of Things in smart city. *Future Generation Computer Systems*, 107, 433-442.
43. Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q.-V., Padannayil, S. K., & Simran, K. (2020). A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities. *IEEE Transactions on Industry Applications*, 56(4), 4436-4456.
44. Wang, M., et al. (2020). 6G Security: Challenges and Opportunities. *IEEE Network*.
45. Nguyen, V., et al. (2021). Security and Privacy for 6G: A Survey. *IEEE Communications Surveys & Tutorials*.
46. Porambage, P., et al. (2021). Roadmap to 6G Security and Privacy. *IEEE Open Journal of the Communications Society*.
47. Mucchi, L., et al. (2021). Physical Layer Security in 6G Networks. *IEEE Access*.
48. Mao, B., et al. (2023). AI for 6G Security: A Comprehensive Review. *IEEE Internet of Things Journal*.
49. Zuo, Y., et al. (2023). Blockchain for 6G Security. *Future Generation Computer Systems*.
50. Kazmi, S., et al. (2024). AI-Driven Security for 6G. *IEEE Wireless Communications*.