Leveraging AI and Machine Learning to Transform Networking Technologies: Enhancements in Automation and Security

Nikhil Bhagat

Sr. Technical Account Manager – Network Specialist,Independent Scholar, Network Engineering

Abstract

Automation and security are two areas where Artificial Intelligence (AI) and Machine Learning (ML) have revolutionized the landscape of networking and security technologies. As network infrastructures evolve and grow in complexity, traditional management practices are unable to keep up with the ever-increasing demands of scalability, efficiency and security. AI and ML can assist by automating repetitive processes, increasing network efficiency, andidentifying threats. This paper describes the evolution of AI, networking opportunities for AI, and the operating model of machine learning. It describes the use of AI and ML to drive network automation with self-optimizingnetworks, proactive maintenance and zero-touch provisioning. AI and ML also help network security as they provide better anomaly detection, threat prediction and incident response. Not only do these technologies enhance network performance, but they also act as a proactive defense mechanism in a rapidly changing cyberspace environment. As AI and ML mature, their integration into networks will play a critical role in the evolution of more resilient, adaptive, and secure systems.By analyzing the use cases of AI and ML in network automation and network security showcased in this paper, a network and security architect can develop a strategic plan customized to their organization's needs for optimizing the network.

Keywords: Artificial Intelligence, Machine Learning, Network Automation, Security, Anomaly Detection.

I. INTRODUCTION

The rapid expansion of digital transformation in the last several decades has brought a new challenge to network technology. More than ever before, maintaining high performing networks are essential to organizations, governments and individuals. As the amount of data being sent over networks grows, so does the complexity of operating, automating, and securing those networks.Traditionally, network administration is done through manual operations and interventions [1]. However, with the adoption of software-defined networking (SDN) and network function virtualization (NFV), networking has become increasingly fluid, adaptable, and scalable [2].Nonetheless, the sheer complexity of today’s networks demands even greater automation and predictive threat prevention.

To reduce manual intervention and promote streamlined network management, technologies likeArtificial Intelligence (AI) and Machine Learning (ML) can be beneficial [3]. AI consists of technologies that enable machines to simulate human intelligence, while ML, a subset of AI, allows machines to learn from data and improve over time. Innetwork management, AI and ML can automate repetitive work, improve traffic flows, predict network failures and ensure network security by finding abnormalities in traffic.

The paper describes and examines ways in which AI and ML can assist networking technology with automation and security. It covers the history of AI, benefits of AI, how ML works, and gives specifics about how these technologies canimpact network automation and security.

II. Evolution of Artificial Intelligence

The idea of artificial intelligence goes back to antiquity, when myth and legend presented humans as intelligent artificial creatures. However, a formal research into AI took place around the middle of the 20th century with digital computing. The term was first introduced in 1956 by John McCarthy, who is considered to be the father of AI, at a conference held at Dartmouth College [4].Early AI experiments focused on problem-solving and symbolic reasoning, but they were limited by the computer hardware available at the time.Expert systems became one of the most promising uses of AI in the 1980s. These systems simulated the ability to make human-like decisions under the supervision of a human specialist, but were predominantly finite and rule-based [5]. Such limitations of expert systems gave rise to increasingly powerful AI that learnt from data, like machine learning, which gained popularity in the 1990s and 2000s as compute power and data availability increased.

This led to the invention of deep learning in the 21st century — a branch of machine learning that employs artificial neural networks to create patterns from data. It was facilitated by the evolution of big data and the GPU revolution, which accelerated the training of deep learning models. AI began to surpass humans in certain tasks, including image recognition, speech recognition, and gaming, by using techniques such as convolutional neural networks (CNNs)and reinforcement learning [6].

AI is ubiquitous today — in healthcare, banking, mobility, and increasingly, networking. AI is deployed in networking to handle large amounts of data, anticipate network behaviors, optimize resources and shield networks from sophisticated cyberattacks. The move from simple problem-solving logic to machine learning models has helped AI becomean indispensable tool in modern networking.

III. Advantages of Artificial Intelligence

A. Automation of Routine Tasks

This is one of the major advantages of AI: the capacity to automate repetitive activities. In the case of networking, it could be a matter of automating the configuration of routers and switches, network policies, or even tracking network traffic [7]. Automating them frees network administrators up to deal with more complicated problems and strategic decisions.

B. Predictive Analytics

AI algorithms are able to sort out huge datasets and spot patterns that humans do not immediately notice. This is a particularly powerful tool in networking where AI can anticipate network overages, failures, or downtime based on historical patterns [8]. Predictive analytics helps network administrators identifyand troubleshoot issuesproactively preventing a potential impact.

C. Adaptive Learning

AI machines can also learn and evolve as they ingest data over time. Adaptive learning, especially in networking, can be used to customize the network as the network topology changes [9]. An AI system might re-route traffic in real-time to alleviate traffic jams, or prioritize traffic depending on demand.

D. Enhanced Security

AI can analyze network traffic and identify unusual trends that could indicate a security breach or an attack. AI-powered security systems can process millions of records, and flag anomalies much quicker than

conventional monitoring mechanisms [10]. This allows fasterthreat detection and mitigation, reducing the impact of cyberattacks.

E. Scalability

As the internet continues to expand, the networks are getting increasingly complex. AI systems are network-scalable i.e. they can handle increasingly advanced tasks and large amounts of data with little or no human involvement [11].

These benefits reveal why AI is emerging as a core part of modern networks' administration and security. However, the intelligence within AI is heavily aided by machine learning, which allows AI to learn and adapt to novel situations.

IV. MACHINE LEARNING AND OPERATING MODEL

Machine learning is subset of AI that enables machines to learn from data and make predictions or decisions without being programmed [12]. In contrast to traditional rule systems, ML applies statistical algorithm to discover data patterns and use those patterns to determine appropriate action.

The basis of ML are algorithms that can be trained using varying datasets. Those datasets consist of input data (features) and the correct outputs (labels). The Machine Learning process can be summarized with six major steps.

A. Data Collection

ML models require a large amounts of data to train. In network, data may originate from logs, sensors, traffic and users. The performance of ML models is highly dependent on the quantity and quality of data [9].

B. Data Preprocessing

Before sending to an ML model, the data need to be cleaned, transformed, and normalized. This is done by eliminating missing or irrelevant data, converting categorical variables to numbers and equalizing the features on scale [13].

C. Model Selection

Algorithms like supervised, unsupervised and reinforcement learning are all different kinds of ML algorithms. Supervised learning trains the model on labeled inputs where there is a known correct output. Unsupervised learning is employed when the model is provided with unlabeled data and left to discover patterns on its own [14]. In contrast, reinforcement learning is used to train an agent to make decisions by rewarding correct choices and penalizing incorrect ones.

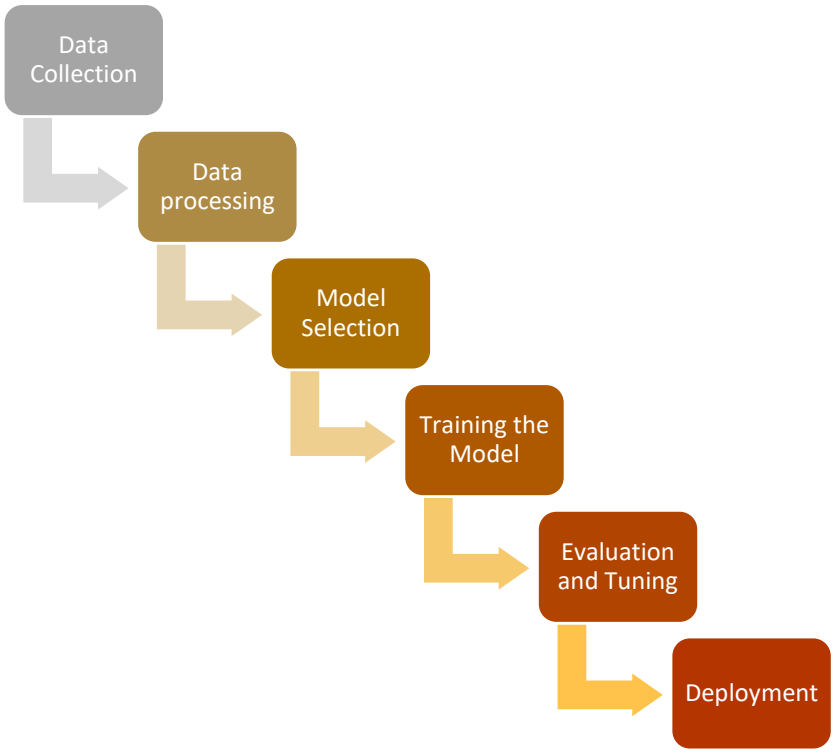

Fig 1. Machine Learning Operating Model

D. Training the Model

Once data is ready and the model is selected, the training process will begin. The model learns the relation between the input and correct output by minimizing an error function in the training process [15]. It involves continuously updating the model's parameters (weights) to obtain as accurate predictions as possible.

E. Evaluation and Tuning

Upon training, the model is run on a different test set to determine if it generalizes to new data. A poor model might be fixed by adjusting hyperparameters or replacing an algorithm with one.

F. Deployment

When it becomes reliable, the model is released to a production environment where it can make real-time predictions. In case of networks, this might be traffic anomaly detection, network failure detection or automatic network configuration [16].

Machine learning can make networks smarter and more responsive over time. With the ability to learn from large datasets, ML models can predict and optimize the network in ways that fixed systems cannot.

V. USE OF AI AND MACHINE LEARNING TO ENHANCE NETWORK AUTOMATION

Network automation is a crucial necessity as networks get increasingly sophisticated and massive. Even legacy network management methods, largely built using manual configuration and rules can no longer meet the rapidly evolving demands of modern organizations. With growing networks, the older approaches are subject to human mistakes, operational inefficiencies and latency, all of which contribute to low-quality performance.

AI and machine learning (ML) provide novel answers to these issues by revolutionizing the management, control and optimization of networks. With the help of AI and ML, network automation can be transformed from a list of functions to an intelligent, self-learning, adaptive algorithm that can dynamically adapt to changing network topologies [17]. AI-enabled network automation does everything from the mundane, like

configuring devices, to advanced network management like traffic optimization and performance optimization.

A. Automated Network Configuration

Automating network configuration is probably one of the major AI/ML network automation capabilities. For traditional network setups, a network administrator will have to manually configure routers, switches and firewalls. However,performing configuration changes manually has its unintended consequences of errors, inefficiencies and misconfigurations, especially when used at scale [1].AI/ML can automate network configuration based on analysis of vast network traffic data and pattern identification in the network. AI algorithms can learn from historical setups, find optimal setups for each machine and update configurations automatically. That avoids human interference, errors, and provides the best conditions for devices to work under [18].

A routing protocol can, for instance, automatically be set by an AI system according to the actual network traffic state so that data flow on the network is optimal. It might also use AI to automatically perform Quality of Service (QoS) to favor certain types of traffic, like applications where latency is critical (video conferencing or real-time gaming).

B. Self-Optimizing Networks

AI/ML helps build self-optimizing networks that automatically tune and optimize based on the current network topology. Performance tuning in a traditional network would typically be performed manually, which is time consuming and prone to human errors [18]. AI enables continuous monitoring of network traffic and device performance, allowing the system to automatically adjust itself without requiring manual intervention.Traffic Management is one area where self-optimization can be very important. AI can track network activity live and identify bottlenecks or areas where congestion may occur. Machine learning algorithms are able to anticipate where traffic is likely to get stuck from historical analysis and automatically change traffic routing to avoid downtime [19]. For example, if one link gets congested, AI can redirect traffic to underutilized links to minimize latency and maximize network efficiency.

The Network Resource Allocation can also be automatically optimized by AI. The more users and devices access the network, the higher is the need for bandwidth and other resources. AI-driven systems can monitor these demands and allocate resources efficiently, ensuring that critical applications always have the bandwidth they need. This results in the efficient use of the network resources and improves overall user experience.

C. Predictive Maintenance and Failure Prevention

Predictive maintenance is one of the more sophisticated network automation tools provisioned by AI. Predictive maintenance enables machine learning models to analyze performance history and patterns that may indicate a potential hardware or network failure in advance [20]. This predictive algorithm will allow network administrators to address problems early, helping eliminate downtime and improve reliability.For instance, based on device temperature, power consumption and traffic volume, AI is capable identifying system and hardware level failures. This allows the system to prompt network administrators to remove or repair the unit before it leads to a serious network breakdown. Similarly, AI can anticipate software bugs or configuration issues, such as firmware bugs, that could affect performance or security.

Predictive maintenance is especially useful in large, distributed networks where the health of every device cannot be manually monitored. By detecting and avoiding failures, AI-based automation eliminates costly downtime and ensures networks run smoothly without human intervention [21].

D. *Zero-Touch Provisioning*

Another important network automation breakthrough that AI/ML enabled is zero-touch provisioning (ZTP). ZTP allows network devices to automatically configure when initially connected to the network, eliminating manual setup by the administrator [22]. This is a particularly helpful function in enterprise-class deployments such as data centers where manually configuring hundreds or thousands of devices would be time consuming and error-prone.ZTP automatically discovers new devices as they come into the network, and AI systems assign configurations to them based on policies and real-time network conditions [22]. These policies can also be continuously optimized by ML algorithms to make sure the device is always configured optimally for the purpose and network conditions.

When a business connects a new network device to the network, it can download the default configuration, including security policies, routing protocols, and QoS rules. This minimizes potential misconfigurations and allows for the network to scale easily without losing performance or security.

ZTP also proves useful when networks are used in frequently-updated environments, including clouds or enterprise networks. AI automatically manages the provisioning process, saving time and labor in the deployment of new devices, helping networks expand at a faster rate.

E. *Network Slicing and Resource Allocation*

Artificial intelligence driven automation allows for more advanced features such as network slicing and resource sharing in the future networks like 5G. Network slicing enables a single physical network to be broken up into several virtual networks, each with dedicated traffic or applications [23]. This could be a high latency application, for instance, or a high bandwidth application, such as video-streaming.AI and ML are crucial in managing and tuning these network slices dynamically. AI can deploy resources to different slices of the network according to actual network state, and application requirements. This ensures every application delivers optimal performance. ML engines learn over time by analyzing traffic patterns, allowing them to customize bandwidth allocation, latency, and other parameters to meet the specific needs of each network slice [3].

With dynamic resource management, networks can better make use of their scarce resources such as bandwidth and CPU processing power, in real-time. For example, AI can assign additional resources to business critical applications during high-traffic times and associate less amount of resources to less critical traffic. AI makes it possible for performance-critical applications like emergency communications or payments to always have the necessary resources they need.

F. *Reducing Latency and Improving Network Performance*

AI-powered Network automation helps reduces latency and boosts overall network performance. It is vital for current complex networks to handle an array of latency-sensitive applicationssuch as online gaming, live video conferencing and industrial control systems [3].

AI can help minimize latency by intelligently routing traffic down the shortest paths, steering clear of congestion by predicting network congestion. Algorithms can learn from past traffic to determine patterns that cause latency, so that networks can react in real-time to address them [24]. AI ensures real-time adaptation of routing rules and traffic flows, ensuring that data arrives on time, which provides a better quality of service to end-users.

Additionally, AI can optimize the placement and utilization of edge computing resources so that data processing can be performed nearer to the data source. By delegating computation-intensive activities to edge nodes, AI canminimize the amount of data moving around the network, reducing overall latency. This is

especially true in the case of real-time computation-intensive applications such as autonomous vehicles, augmented reality, and IoT devices.

G. *AI-Based Network Monitoring, Analytics and Troubleshooting*

Network monitoring and troubleshooting are important aspects of network automation. AI and ML help to achieve greater monitoring capabilities by constantly monitoring the network, identifying anomalies and diagnosing problems in real time. Current monitoring tools have largely been based on thresholds and rules that are either fixed or non-adaptive [25]. As these rules are non-adaptive, it is difficult for traditional monitoring tools to detect evolved threats, averts and anomalies.AI-powered monitoring systems apply ML algorithms to historical and live metrics to understand what normal network behavior is, and report any outliers. These systems can look for network irregularities such as spikes of traffic or packet loss or jitter, which could indicate a potential issue [26]. When AI detects these, it prevents issues before they impact end users.

AI can also be used to automate troubleshooting by mapping multiple data sources such as performance logs, error reports, and device statistics [27]. If, for instance, a performance failure occurs on a particular link, AI can look into the logs to identify the root cause of the underlying issue such as hardware failure, configuration failure or something external like a DDoS attack. The AI systems can then recommend or automatically take corrective measures to save time in diagnosing and correcting network problems.

H. *Adaptive and Context-Aware Networking*

Context-awareness is an emerging concept of AI-enabled network automation, where the network adapts dynamically to the requirements of users, applications and devices. AI algorithms can interpret contextual data like application type, geographical location, capabilities of devices, and network conditions to optimize network performance as per the scenario [9].For example, if a user is streaming a video from their mobile device, the AI could serve the low-latency, high-bandwidth connections for that person and allow him to stream the video. On the other hand, if the same user is navigating a page or downloading a file, the network can de-allocate bandwidth for those processes and free up the bandwidth for other latency sensitive applications.

Adaptive networking also extends to security where AI can adapt security policies on real-time context. For instance, AI could increase security for a user browsing highly confidential corporate data via public Wi-Fi and reduce security for the same user browsing less important corporate data via a trusted device on a private network.

VI. USE OF AI AND MACHINE LEARNING TO ENHANCE NETWORK SECURITY

A. *Anomaly Detection and Mitigation*

Anomaly detection is one of the strongest use cases for AI/ML in network security. Traditional security protocols use existing signatures to identify attacks, which can only be used for known attacks. AI-based anomaly detection focuses on finding deviations from network normality regardless of whether the attack has been detected in the past [28].AI systems can learn from vast quantities of network traffic to develop a baseline of "normal" network behavior. This includes factors like average traffic, device behavior, and user behavior. With this baseline established, the AI platform can track the network in real time and detect any deviations or anomalies that might suggest a security issue [29].

For instance, if a specific user starts dumping large amounts of data to an external server unexpectedly, then AI anomaly detection might be able to identify the pattern as suspicious, even if it is different than the signature of a known attack. This enables organizations to identify and attack new threats (such as zero day attacks) that traditional signature-based solutions cannot.Furthermore, ML algorithms become ever more

efficient by continually learning from new data and reacting to changing network behavior. This makes anomaly detection systems resilient as network traffic flows evolve, and it makes AI-based solutions incredibly flexible and scalable for changing networks.

B. Threat Prediction and Threat Intelligence

AI and ML are changing the landscape of threat analysis and intelligence, enabling companies to identify and prevent cyber-attacks before they happen. ML algorithms can also be based on historical attack logs in order to detect patterns and trends that can give you a clue of the potential for future attacks [30]. Based on that information, AI systems can forecast what types of attacks will most likely hit the network and prioritize defenses accordingly.For example, an AI machine can use historical ransomware attacks to identify characteristics of target organizations, including network architectures, vulnerabilities in software, or patterns of users. On the basis of this information, the system will be able to predict the kind of attack the organization can expect in the future and suggests pre-emptive actions to avoid this.

Along with making predictions about specific attacks, AI systems can read real-time threat data collected through public databases, social media and security feeds. When AI is combined with data from the external world, and network data within the network, new threats and vulnerabilities can be detected in real time [31]. For instance, if a new threat appears in a popular software, AI-based systems will immediately identify the network's vulnerability and suggest or deploy patch/security measures.

AI prediction is especially useful for preventing advanced and fast-moving threats like zero-day exploits and advanced persistent threats (APTs) which may lack signatures or known attack techniques.

C. Automated Incident Response

The efficiency and accuracy in incident response plays a key role in mitigating the impact of cyberattacks. AI and ML can significantly help the incident response by automating several parts of threat detection, containment, and remediation. Standard incident response is manual, which is slow and error-prone. AI-based systems, meanwhile, are able to react to security incidents real time, reducing the time and amount of impact [32].AI systems can take the necessary actions automatically if attacked, including quarantining compromised devices, blocking malicious IP addresses or closing down compromised users' sessions [32]. This automated responseensures thatsecurity incidents are quickly addressed without the presence of any human security staff.

For instance, AI might detect an unusual increase in outbound network traffic that could indicate a data exfiltration attempt, automatically blocking the malicious IP addresses or restricting access to critical information until the issue is resolved.The same way if a device on the network starts showing signs of malware infection AI can disconnect that device from the network to keep the malware from spreading further.

Apart from containment, AI solutions can provide further information on the security events such as the origin of the attack, the targeted systems and the actions taken to mitigate the impact. These reports offer security teams insight into how they can conduct a more detailed post-incident analysis and optimize future defenses.

D. AI-Based Fraud Detection and Prevention

Fraud prevention is another area where AI and ML have a transformative impact over network security, especially in the banking, e-commerce, and telecom industries. Fraud detection using AI could be able to analyze large amounts of transaction data on the fly and detect trends and patterns of fraud activity [33].AI platforms can monitor credit-card use for trends, for instance, to look for an unexpected increase in purchases

or transactions at faraway locations. AI/ML algorithms can detect subtle patterns that may indicate a fraudulent behavior even if the technique of fraud is new or unfamiliar [34].

Through identifying and blocking fraudulent activity at a time of transaction, AI can protect organizations and their customers from financial losses and reputational damage. AI-based fraud detection systems far outperform existing rules-based fraud detection systems in speed and precision, and are an absolute necessity in the field of network security.

VII. Conclusion

Artificial Intelligence (AI) and Machine Learning (ML) are reshaping the future of networking technologies, providing new enhancementswithin automation and security. As networks and databases grow in complexity, manual network management and security methods no longer deliver the real-time optimization and security that are needed. AI and ML solves these problems by delivering the intelligence and scalability needed for modern networks.

When it comes to automation, AI enables self-optimizing networks that can adapt to changing traffic patterns, predict and prevent faults through proactive maintenance, and manage devices with minimal human intervention. AI algorithms learn continuously from network data and become increasingly accurate at predicting and solving problems. This automated shift reduces human error, increases network efficiency and frees up administrators to focus on strategic tasks.

AI and ML has also revolutionized network security with its advanced capabilities within edge anomaly detection, threat prediction and incident management features. These tools go beyond the traditional security framework by identifying emerging and new threats, enabling networks to rapidly and smartly counter cyber-attacks. AI-based security solutions can process large amounts of data, spot patterns of malware and take immediate action to mitigate threats in real time.

By analyzing the use cases of AI and ML in network automation and network security showcased in this paper, a network and security architect can develop a strategic plan customized to their organization's needs for optimizing the network.

References

[1] S. Lee, T. Wong and H. Kim, "To Automate or Not to Automate: On the Complexity of Network Configuration," in 2008 IEEE International Conference on Communications (ICC), Beijing, China, 2008, pp. 1-5. doi: 10.1109/icc.2008.1072.

[2] D. Kreutz, F. M. V. Ramos, P. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," Cornell University, 2014. doi: 10.48550/arxiv.1406.0440.

[3] K. M. Sivalingam, "Applications of Artificial Intelligence, Machine Learning and Related Techniques for Computer Networking Systems," Cornell University, 2021. doi: 10.48550/arxiv.2105.15103.

[4] J. E. McCarthy, "What Is Artificial Intelligence?" in Artificial Intelligence: Foundations and Applications, 2020, pp. 37-49. doi: 10.1002/9781119601906.ch3.

[5] M. W. Hurley and W. A. Wallace, "Expert Systems as Decision Aids for Public Managers: An Assessment of the Technology and Prototyping as a Design Strategy," Public Adm. Rev., vol. 46, no. 6, p. 563, Nov. 1986. doi: 10.2307/975578.

[6] M. Langer, Z. He, W. Rahayu and Y. Xue, "Distributed Training of Deep Learning Models: A Taxonomic Perspective," IEEE Trans. Parallel Distrib. Syst., vol. 31, no. 12, pp. 2802-2818, Jun. 2020. doi: 10.1109/tpds.2020.3003307.

[7] G. P. Kumar and P. Venkataram, "Artificial Intelligence Approaches to Network Management: Recent Advances and a Survey," Artificial Intelligence, vol. 20, no. 15, pp. 1313-1322, Dec. 1997. doi: 10.1016/s0140-3664(97)00094-7.

[8] G. Luo, Q. Yuan, J. Li, S. Wang and F. Yang, "Artificial Intelligence Powered Mobile Networks: From Cognition to Decision," IEEE Network, vol. 36, no. 3, pp. 136-144, May 2022. doi: 10.1109/mnet.013.2100087.

[9] M. Wang, Y. Cui, X. Wang, S. Xiao and J. Jiang, "Machine Learning for Networking: Workflow, Advances and Opportunities," IEEE Network, vol. 32, no. 2, pp. 92-99, Nov. 2017. doi: 10.1109/mnet.2017.1700200.

[10] N. T. Lam, "Detecting Unauthorized Network Intrusion Based on Network Traffic Using Behavior Analysis Techniques," Int. J. Appl. Comput. Sci., vol. 12, no. 4, 2021. doi: 10.14569/ijacsa.2021.0120407.

[11] L. Zhang, Z. Chen and S. Yang, "Application of Artificial Intelligence in Computer Network Security," J. Phys. Conf. Ser., vol. 1865, no. 4, p. 042039, Apr. 2021. doi: 10.1088/1742-6596/1865/4/042039.

[12] K. G. Srinivasa, S. G. Matt and H. Srinidhi, "Basics of Machine Learning," in Machine Learning, 2018, pp. 127-138. doi: 10.1007/978-3-319-77800-6_8.

[13] M. Kang and J. Tian, "Machine Learning: Data Pre-processing," in Machine Learning, Wiley, 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/9781119515326.ch5.

[14] S. Sah, "Machine Learning: A Review of Learning Types," Preprints, Jul. 2020. doi: 10.20944/preprints202007.0230.v1.

[15] R. P. Dixit, R. Kushwah and S. Pashine, "Handwritten Digit Recognition Using Machine and Deep Learning Algorithms," Int. J. Comput. Appl., vol. 176, no. 42, pp. 27-33, Jul. 2020. doi: 10.5120/ijca2020920550.

[16] M. Usama et al., "Unsupervised Machine Learning for Networking: Techniques, Applications and Research Challenges," IEEE Access, vol. 7, pp. 65579-65615, 2019. doi: 10.1109/access.2019.2916648.

[17] S. Vassilaras et al., "Problem-Adapted Artificial Intelligence for Online Network Optimization," Cornell University, 2018. [Online]. Available: https://arxiv.org/abs/1805.12090.

[18] G. Ai-peng and C. Yuan, "Network Intelligent Control and Traffic Optimization Based on SDN and Artificial Intelligence," Electronics, vol. 10, no. 6, p. 700, Mar. 2021. doi: 10.3390/electronics10060700.

[19] Z. M. Fadlullah et al., "State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems," IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2432-2455, 2017. doi: 10.1109/comst.2017.2707140.

[20] Y. Ran, X. Zhou, P. Lin, Y. Wen and R. Deng, "A Survey of Predictive Maintenance: Systems, Purposes and Approaches," Cornell University, 2019. doi: 10.48550/arXiv.1912.07383.

[21] M. Bidollahkhani and J. Kunkel, "Revolutionizing System Reliability: The Role of AI in Predictive Maintenance Strategies," Cornell University, Apr. 20, 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2404.

[22] I. Boškov, H. Yetgin, M. Vučnik, C. Fortuna and M. Mohorčič, "Time-to-Provision Evaluation of IoT Devices Using Automated Zero-Touch Provisioning," IEEE Globecom 2020, pp. 1-6, Dec. 2020. doi: 10.1109/globecom42002.2020.9348119.

[23] M. A. Habibi, B. Han and H. D. Schotten, "Network Slicing in 5G Mobile Communication Architecture, Profit Modeling, and Challenges," Cornell University, 2017. doi: 10.48550/arxiv.1707.00852.

[24] Z. Xu et al., "Experience-Driven Networking: A Deep Reinforcement Learning Based Approach," in 2018 IEEE INFOCOM - IEEE Conference on Computer Communications, 2018, pp. 1-9. doi: 10.1109/infocom.2018.8485853.

[25] S. Ayoubi et al., "Machine Learning for Cognitive Network Management," IEEE Commun. Mag., vol. 56, no. 1, pp. 158-165, Jan. 2018. doi: 10.1109/mcom.2018.1700560.

[26] R. Mijumbi, A. Asthana, M. Koivunen, F. Haiyong and Q. Zhu, "Design, Implementation, and Evaluation of Learning Algorithms for Dynamic Real-Time Network Monitoring," Netw. Model., vol. 31, no. 4, 2020. doi: 10.1002/nem.2108.

[27] Y. Lai, C. Kao, J. Jhan, F. Kuo, C. Chang and T. Shih, "Quality of Service Measurement and Prediction Through AI Technology," 2020 1st International Conference on Electronics and Communication (ICEC), pp. 1-6, Oct. 2020. doi: 10.1109/ecice50847.2020.9302008.

[28] J. Sen and S. Mehtab, "Machine Learning Applications in Misuse and Anomaly Detection," IntechOpen, Jun. 2020. doi: 10.5772/intechopen.92653.

[29] M. Zou, C. Wang, F. Li and W. Song, "Network Phenotyping for Network Traffic Classification and Anomaly Detection," 2020 IEEE International Conference on Telecommunications (ICT), pp. 1-6, Oct. 2018. doi: 10.1109/ths.2018.8574178.

[30] R. Jones, M. Omar, D. Mohammed, C. Nobles and M. Dawson, "Harnessing the Speed and Accuracy of Machine Learning to Advance Cybersecurity," 2023 IEEE 5th International Conference on Cybersecurity (CSCE), pp. 1-6, Jul. 2023. doi: 10.1109/csce58395.2023.10123820.

[31] K. Hartmann and C. Steup, "Hacking the AI - the Next Generation of Hijacked Systems," IEEE Access, vol. 10, pp. 17440-17454, 2022. doi: 10.1109/access.2022.3141617.

[32] B. Geluvaraj, P. Satwik and T. A. Kumar, "The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace," IEEE Access, vol. 8, pp. 167012-167021, 2020. doi: 10.1109/access.2020.3023011.

[33] G. S. Sowmya and H. K. Sathisha, "Detecting Financial Fraud in the Digital Age: The AI and ML Revolution," International Journal of Computer Applications, vol. 975, no. 8887, pp. 7-12, 2020. doi: 10.5120/ijca2020920542.

[34] B. Mytnyk, O. Tkachyk, N. Shakhovska, C. Федушко and Y. Syerov, "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition," International Journal of Advanced Computer Science and Applications, vol. 11, no. 7, pp. 260-267, 2020. doi: 10.14569/ijacsa.2020.0110738.