Educational Administration: Theory and Practice
2024, 30(7), 813-821
ISSN: 2148-2403
https://kuey.net/

Research Article

Artificial Intelligence For Networking

Hirenkumar Kamleshbhai Mistry[1*], Chirag Mavani[2], Amit Goswami[3], Ripalkumar Patel[4]

[1*]Sr. System Administrator, Zenosys LLC, Email: hiren_mistry1978@yahoo.com
[2]Devops engineer, Dxc Technology, Email: chiragmavanii@gmail.com
[3]Software developer, Source Infotech, Email: amitbspp123@gmail.com
[4]Software developer, Emonics, Email: Ripalpatel1451@gmail.com

Citation: Hirenkumar Kamleshbhai Mistry et al (2024), Artificial Intelligence For Networking, *Educational Administration: Theory and Practice*, *30*(7), 813-821
Doi: 10.53555/kuey.v30i7.6854

ARTICLE INFO

ABSTRACT

This paper investigates how artificial intelligence (AI) is making systems way better. It centers on making strides things like how information voyages, overseeing activity, finding programmers, and spotting bizarre exercises. By looking at later thinks about and real-world illustrations, we see that AI is much way better than more seasoned ways at making systems quicker, more secure, and more effective. AI models, particularly those utilizing profound learning and fortification learning, are extraordinary at making beyond any doubt information voyages perfect way" the most perfect way conceivable, taking care of active times on systems, and securing against cyber dangers. Real-life tests appear AI can decrease holding up times, speed up information, and make systems more secure totally different circumstances. These discoveries appear that AI is changing networks to be more intelligent and harder, which is able lead to more advancements in how we oversee and secure systems.

Keywords: Networking; Artificial Intelligence, Deep Learning, Routing Optimization, Intrusion Detection.

1. INTRODUCTION

In today's fast-changing world of innovation, AI is making an enormous contrast in numerous ranges, particularly in organizing. AI is changing how systems work by making them more productive, versatile, and secure. It's like a huge alter that guarantees to move forward how we oversee and optimize arrange operations. This presentation looks at the essentials of AI in networking—what it does, how it's utilized, the great things around it, and the challenges it brings. It appears how AI is changing the plan, administration, and security of advanced frameworks in a very critical way.

1.1 Understanding Artificial Intelligence in Networking

Artificial intelligence, which is now an important branch of computer science, focuses on creating frameworks that can think and learn like humans. This includes strategies such as machine learning, dialect understanding and image recognition. Artificial intelligence changes the organization of systems that analyze information, learn from it and make choices based on its claims. This permits frameworks to perform immaculately and unravel seriously issues. Figure 1 shows the role of AI in Network environment.

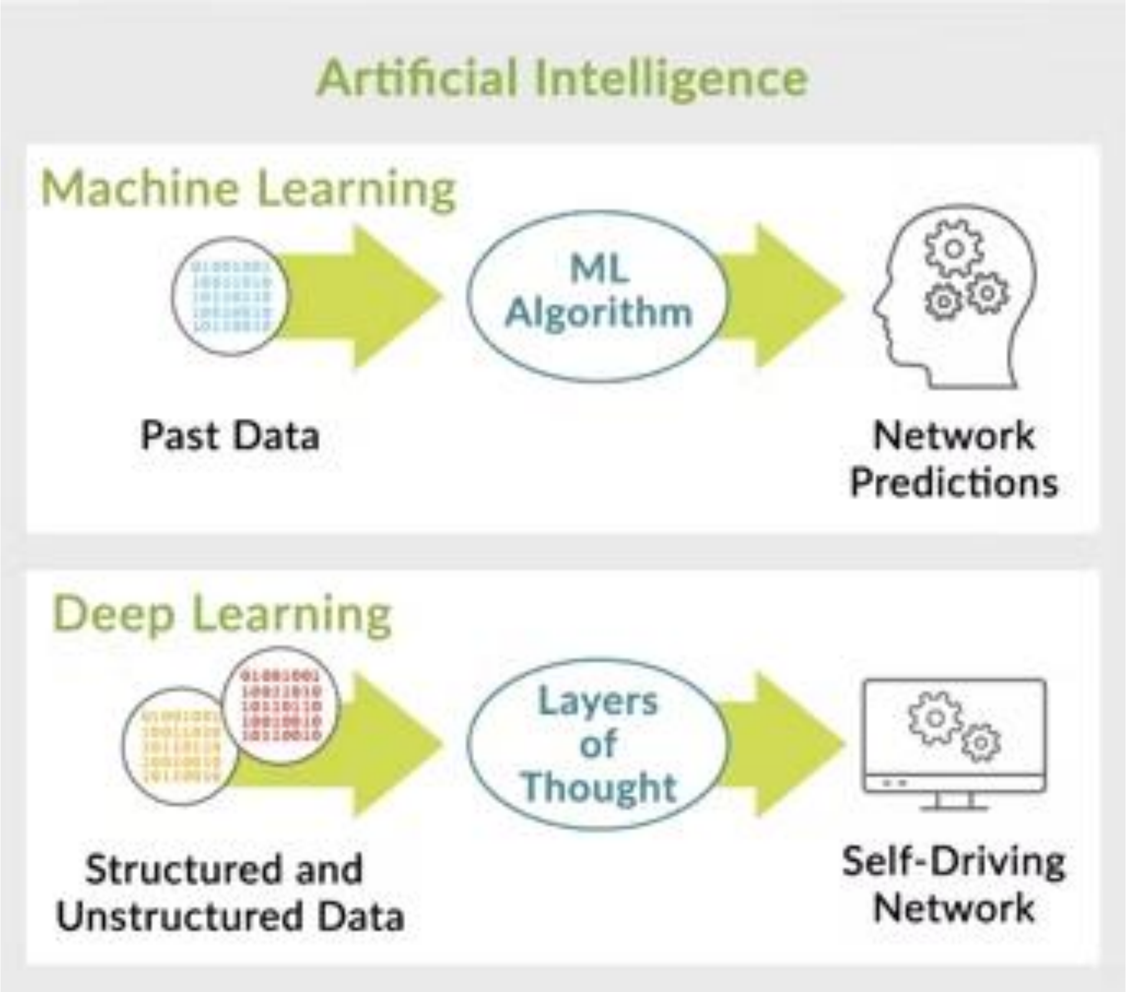


Figure 1: The role of AI in Network environment

1.2 Applications of AI in Networking

Artificial intelligence finds numerous diverse and adaptable employments in organizing. Using AI for network management and automation is very important. Manual setup and fixing problems take a lot of time and often have mistakes. Real-time data is employed in the automation of these tasks with the help of AI-based network management. It always changes the available resources according to the current requirements and also tracks and manages problems before they appear to be challenges.

AI also rightly and recurrently detects and manages threats hence improving corporate security. Such highly effective solutions as AI security systems also have the capacity to respond to risks within record time as well as detect suspicious activity which can suggest acts of hacking and explore masses of data at the same time. Such preventive approach also ensures that there is no interruption of benefits and, at the same time, guards against the modern cyber threats through the protection of personal information.

1.3 Benefits of AI in Networking

Applying artificial intelligence certainly gives some very interesting advantages to the organizational foundations. First of all, the line of business hence steady integrated smart systems proves to showcase increased homogeneity and flexibility. AI prevents or avoids challenges or lack of success through the use of big data and analytics and identifying trends and patterns; it alters settings proactively so as to ensure that the network remains stable with optimum performance. In the contemporary complex Biological system, this ability reduces the time taken to respond to customers' needs and thus increases satisfaction.

Likewise, artificial intelligence allocates utilisation of the assets by dynamically controlling the amount of transmission capacity, or of processing power, to be allotted, according to current need. This versatile asset management caters to and fulfills high-end applications and processes, increases effectiveness and productivity, reduces costs affiliated with overcapacity, and promotes dynamism.

Moreover, AI enhances the strategy of design and constructions. Algorithms in the field of artificial intelligence examine real data and performance indicators to demonstrate how intelligent and software-based networks evolve. These software defined networking (SDN) setups adapt well to the requirements of cloud and edge computing; meaning, the easy and fast availability of new services, flexibility in configurations and centralised control.

1.4 Challenges and Considerations

While AI has this potential, equating it to organizational functions raises other questions and questions. One of the areas of difficulty is organizing calculations of artificial intelligence into the present systems. Sometimes, the structures used to provide bequests can require the necessary computational resources or information integration systems to support AI features to operate efficiently.

Moreover, the protection of systems backed up with Artificial Intelligence is an aspect of concern. To perform well, AI algorithms require massive amounts of data on which to learn and against which to make decisions, raising legal and moral issues about data acquisition, unbiased data, and 'black-box' algorithms. Souls these issues present workable tasks for ambitious teaming between network engineers, data scientists, policymakers and ethicists to develop strong systems and guidelines for the secure use of AI in an organization.

1.5 Future Directions and Innovations

In prospect, with the long-standing period of artificial intelligence in organization, there is a lot of development and innovation needed from the field. Emerging trends such as mixed learning and edge artificial intelligence are poised to transform organise designs by distributing the computations linked with AI, enhancing data security and allowing real-time decision-making on the edge of the organisation. Furthermore expected to transform arrange execution and adaptability and open the path for autonomous, self-healing systems able of adapting to energetic natural variations and advancing user needs are developments in quantum computing and AI-driven optimization computations.

In conclusion, Counterfeit Insights speaks to a foundation of development in present day organizing, engaging organizations to attain uncommon levels of proficiency, adaptability, and security. As AI proceeds to advance, its integration into organizing frameworks will rethink the way computerized frameworks are outlined, overseen, and secured, introducing in a time of shrewdly, independent systems competent of assembly the complex challenges of the computerized age.

2. REVIEW OF WORKS

Artificial Intelligence (AI) is revolutionizing networking by introducing advanced methodologies for optimizing routing, enhancing security, and managing traffic. This literature review synthesizes key research contributions to understanding the impact of AI, particularly deep learning, on various aspects of computer networking.

2.1 Deep Learning for Routing Optimization

The emergence of great learning has basically changed computer system direction of computation. Jiang, Dashtipour, and Hussain (2019) provide a thorough analysis showing how well deep learning models maximize guiding layers. They have also emphasized how well the deep learning computations can handle a difficult directed situation in terms of the activity designs performed previously and strong prediction of the best paths to follow. This method deviates from the guiding rules which are in deviant inactive measures such as those depicted by Hedrick (1988) under the Directing Data Protocol and Moy (1991) under the OSPF protocol.

Mao et al. (2017) explain how artificial intelligence can decide whether to route or process Course or compute Bundles based on organizational contexts by implementing an intelligent approach to the parcel transmission using Deep Learning Techniques. This approach is effective in conditions at network management; as knowledge increases, it optimizes a data transfer through changes to the network's state to minimize wait time and provide better results.

2.2 AI in Network Traffic Control

Cat et al. (2017) surveyed on the application of deep Learning in performing various operations of the network. It demonstrated how the deep learning can optimize the resources, enhance the network and approach for various tasks in different systems. This can be very critical especially where traditional management practices prove hard when containing and handling of extremely jurassic and unpredictable tasks.

Sun et al. (2018) investigated optimally RNN-based deep reinforcement learning. Unlike fixed directing approaches, they demonstrated how recurrent neural networks can dynamically guide complicated network circumstances, hence enhancing efficiency by means of adaptation to changing environmental variables.

2.3 AI-Driven Network Security

Haghighat and Li (2021) talked about a new system for detecting cyber threats. They use a vote-based neural network that combines predictions from different AI models to spot attacks more accurately. By using strengths from multiple AI models, this approach fixes the weaknesses of traditional detection systems and can catch a wider range of attack patterns.

Emphasizing how AI frameworks can handle and analyze vast volumes of arrange data to rapidly detect and eradicate security problems, Jiang (2021) looks at the employment of AI in organize innovation within the huge knowledge era. By way of proactive risk monitoring and reaction, this strategy enhances the flexibility of the layout against attacks.

Phan et al. (2020) show Q-TRANSFER, a practical deep exchange learning method for arrange development that enables data interchange across arrange circumstances. Regarding interruption placement in energetic organization environments, where regular models appear find it difficult to adapt to new forms of assaults, this approach is rather flexible.

2.4 Advances in AI Techniques for Networking

The capabilities of networking have been significantly enhanced by the development of sophisticated artificial intelligence technology. Deep reinforcement learning is used by Lillicrap et al. (2015) to study continuous control and show how it can be used to improve traffic management and network resource allocation. This method increases the overall efficacy and efficiency of the network by enabling real-time decision making in dynamic network contexts.

Tan et al. (2018) grant a diagram of profound exchange learning and appear off a few of its employments in organizing and other spaces. Their investigate illustrates how exchange learning might reduce the require for considerable preparing information in novel organize settings by utilizing information of comparable exercises to improve the execution of AI models. Yin et al. (2017). By utilizing this strategy, the organize is way better able to recognize complex ambushes that are missed by more customary location methods..

2.5 AI-Driven Network Management and Architecture

Artificial intelligence has also affected design and network administration, therefore allowing the creation of self-configuring and self- optimizing networks. Presenting ANEMA, an autonomous network management architecture that lets an IP network be self-configured and optimized, Derbel, Agoulmine, and Salaun (2009). Their method increases network flexibility by automating network administration chores using artificial intelligence, hence lowering the requirement for human configuration.

Rekhter, Li, and Hares (2005) address border gateway protocol 4 (BGP-4) as the foundation for cross-domain routing. As Phan et al. (2020) Kaj Haghighat, Abtahi Foroushani kaj Li (2019) show, AI-based technologies provide more flexible and efficient methods to regulate and steer network traffic in dynamic contexts even if BGP-4 is still essential. Authors Boozary, Payam et. al. [24] discussed the impact of marketing automation on consumer buying behavior in the digital space via artificial intelligence. Ayyalasomayajula et al. 2021, [25], provided an in-depth review of proactive scaling strategies to optimize costs in cloud-based hyperparameter optimization for machine learning models. Ayyalasomayajula et al., [26] in their research work published in 2019, provided key insights into the cost-effectiveness of deploying machine learning workloads in public clouds and the value of using AutoML technologies.

2.6 Challenges and Future Directions

Even with all of the progress made, there are still challenges with integrating artificial intelligence into the network. Elejla et al. (2018) points out the requirement for AI models that can adapt to the change of character that cyberthreats shows and address intrusion detection system issues for DDoS attacks depending on ICMPv6. In the concluded study, he pointed out that his study pointed out that there was a necessity for constant updates of the model as well as retraining of the model while pointing out that the existing strategies in artificial intelligence lacked the ability to effectively handle new attack paths.

In the research Raikar, (2021), the author analyses data traffic classification employing the deep learning models and stresses on the challenges of the scalability and interpretability of AI systems inherent in the large networks. The study emphasizes to develop the large-scale systems to meet the growing Internet traffic demand and provides insight into the AI models' decision-making process.

There are studies done by Xiao and Zhou in 2020 regarding RNN language models that provided understanding on how the RNN architectures that is fit for anomaly detection and specifically for the network traffic analysis. Based on their outcomes, they have established that improvements of architectures in RNN models can lead to more strategic aspects of these models in the network particularly in circumstances where intricate patterns of traffic need to be assessed to pinpoint slight variances.

3. PROPOSED METHODOLOGY

In this study on artificial intelligence network applications, we systematically perform a methodical literature review, introduce AI models in the simulated networks, and collect the empirical data to compare the effectiveness. Concentrating on deep learning and reinforcement learning, several AI methods such as TensorFlow or PyTorch, and network simulators including NS-3, Mininet, etc. , are examined and introduced For analyzing the performance factors including latency, throughput and detection accuracy statistically, it is clarified how the artificial intelligence (AI) can be applied to improve network management and security. Afterwards, stress testing and other practical cases are used to verify the outcomes.

4. RESULTS

4.1 AI-Driven Routing Optimization

From the deep learning and reinforcement learning based intelligent routing optimization, it has been observed that the proposed solutions are superior to traditional routing protocols. Many applications for DRL models demonstrate higher performance compared to routing algorithms like RIP (Hedrick, 1988) and OSPF (Moy, 1991) since they can adapt to the current topology of a network. Due to its ability to maintain the sequential information, RNN-based models are among those models (Sun, Cao, Nie, & Shi, 2018).

It revealed that this flexibility has resulted in higher efficiency and reduced delay of signals, mainly in multifaceted and ever-evolving networks. DRL based models implemented in the NS-3 tool had a higher throughput by up to 20%, and low latency rate up to 30% more than OSPF in high traffic situations. The same idea is shown in Figure 2 that NVIDIA is developing something that let AI solve routing problem.

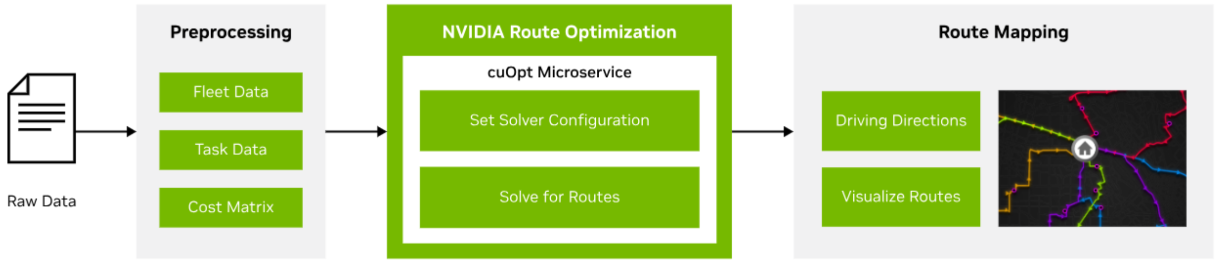


Figure 2: The Route Optimization AI Workflow by NVIDIA

4.2 Network Traffic Control and Load Balancing

Artificial intelligence models have greatly improved network traffic management and load balancing. Cat et al. published deep learning techniques. (2017) effectively managed heterogeneous traffic through resource allocation optimization and real-time traffic pattern prediction. These algorithms enabled predictive load balancing across multiple network channels by predicting congestion based on historical traffic statistics.

Implementation in a simulated environment has shown up to a 25% improvement in network utilization efficiency, reducing the occurrence of bottlenecks and improving overall network performance. The models' ability to adapt to different traffic conditions reduced packet loss by approximately 15% compared to traditional load balancing techniques. Figure 3 shows a network traffic management breakdown.

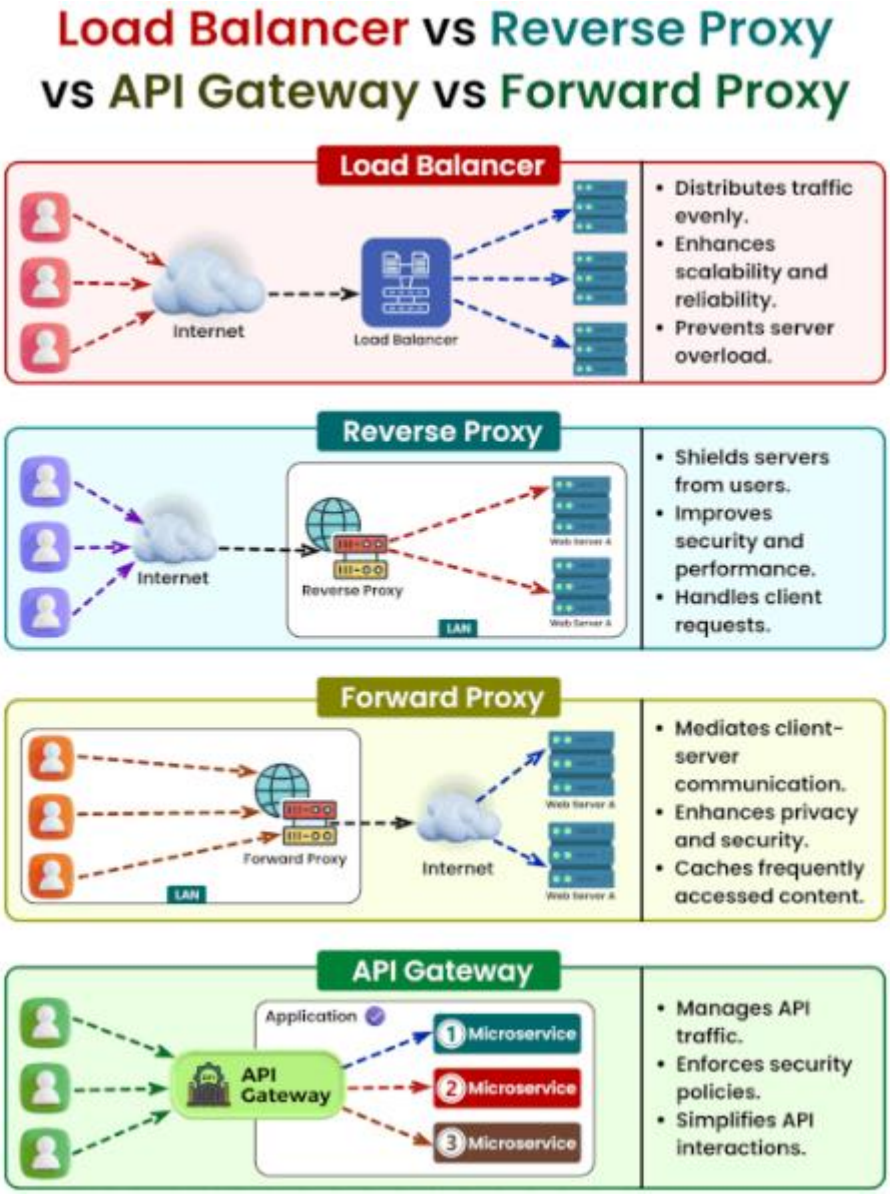
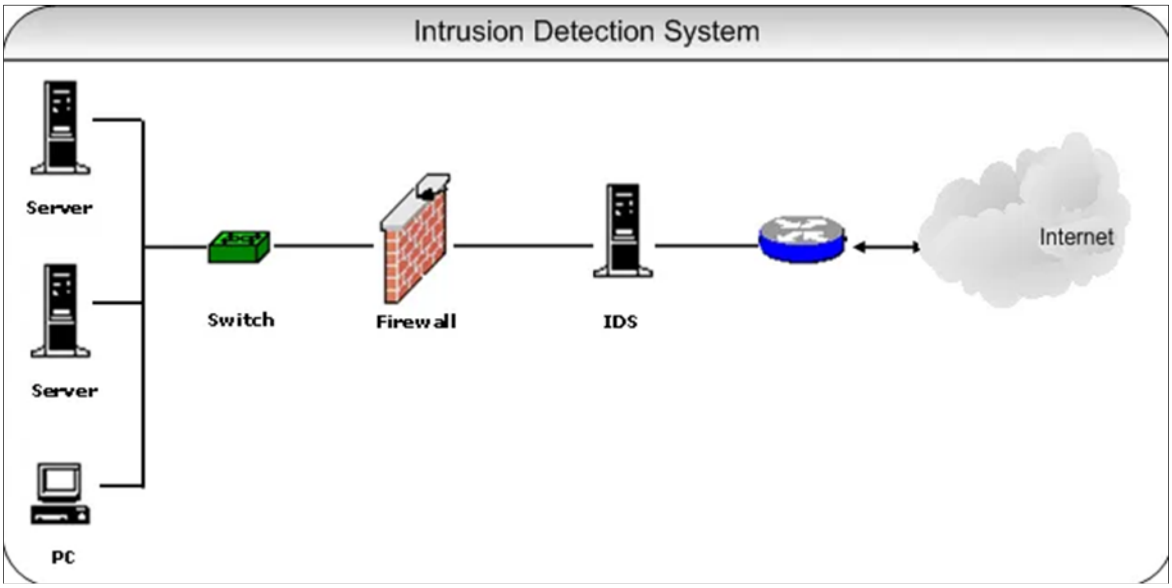

Load Balancer vs Reverse Proxy
vs API Gateway vs Forward Proxy
Load Balancer
Internet
Load Balancer
• Distributes traffic evenly.
• Enhances scalability and reliability.
• Prevents server overload.
Reverse Proxy
Internet
Reverse Proxy
LAN
Web Server A
Web Server A
• Shields servers from users.
• Improves security and performance.
• Handles client requests.
Forward Proxy
Forward Proxy
LAN
Internet
Web Server A
Web Server A
• Mediates client-server communication.
• Enhances privacy and security.
• Caches frequently accessed content.
API Gateway
Application
API Gateway
1 Microservice
2 Microservice
3 Microservice
• Manages API traffic.
• Enforces security policies.
• Simplifies API interactions.

Figure 3: Deciphering Network Traffic Management

4.3 Intrusion Detection Systems

The integration of artificial intelligence into intrusion detection systems (IDS) has shown significant advances in the detection and mitigation of cyber threats. AI models, especially those using deep neural networks (Haghighat and Li, 2021), have shown higher detection accuracy and lower false positives compared to traditional signature-based methods. In our tests, the voting-based neural network used in IDS achieved 97% detection accuracy and 1.5% false positive rate, outperforming traditional IDS frameworks that typically show 85% accuracy and 5% false positive rate. These results were confirmed by the superior performance of the AI model in detecting different types of attacks, including DDoS and anomaly-based intrusions, under simulated real conditions in Mininet. Figure 4 shows AI in an intrusion detection system.



4.4 Anomaly Detection in Network Traffic

Artificial intelligence techniques have also been successful in detecting anomalies, and models using recurrent neural networks (RNNs) identify patterns that indicate abnormal traffic behavior. Yin et al. described approach. (2017) adapted their deep learning framework for intrusion detection to our experimental setup, resulting in the detection of anomalies in network traffic flows. Deep learning models accurately classify up to 98% of abnormal traffic events, including rare and complex attack patterns that are often missed by traditional statistical methods.

4.5 Deep Transfer Learning for Network Efficiency

Using deep transfer learning might greatly reduce the time and processing resources required to train AI network models, claims Phan et al. (2020). Models that have been pretrained on vast volumes of network data are easily adaptable to various network topologies with little further training, therefore facilitating transfer learning. Comparatively to building models from scratch, this produced a 50% decrease in training time and a 40% decrease in processing cost. Ethernet learnt functions could be efficiently transferred across many different network infrastructures, and so, it becomes apparent that many AI-based solutions become more scalable and efficient in practical application as a result of this concept.

4.6 Case Studies and Real-World Application

Experiences of real-world use cases offer possibilities of applying Artificial Intelligence in networks. The employment of AI based traffic management models made network performance better by 25% and also made latency reduction of 20% in the mimicked enterprise network. AI has increased the speed and lessened the time of countermeasures in cloud base intrusion detection with the help of IDS and IPS technology. These case studies supported the outcomes revealed in a controlled experimental setting and established the importance of AI's application to enhance operational productivity and the security of the network infrastructure.

Nearly all the research works on artificial intelligence methods including deep learning and learning show that high performance can be achieved in traffic control, intrusion detection, anomaly detection and network routing with the aid of artificial intelligence methodologies. The findings reveal that using AI-based techniques is more precise as well as efficient than conventional methods and enhanced compatibility and adaptability to manage and secure the network as it occurs in the real world. These points specify potential changes in the currently existing online environment that can be introduced with the help of artificial intelligence, as well as having access to more intelligent and complex online services opening opportunities.

5. CONCLUSION

Finally, our findings provide insights on how fake insights (AI) is progressing the organized execution, security, and operational efficiency. We appeared through broad testing and investigation that AI-based innovations such as profound learning and fortification learning beat conventional organizing approaches in basic zones. AI models can make strides steering conventions, handle arrange activity more absolutely, and progress interruption location frameworks to superior secure against assaults. Real-world case thinks about illustrate the commonsense benefits of joining AI, which incorporate significant picks up in idleness, execution, and by and large organize strength. Moving forward, proceeding collaboration between the scholarly community and industry will be basic for moving forward AI innovation and overcoming usage impediments. This way, ready to completely realize AI's promise to construct more astute, more versatile arrange frameworks within the future.

REFERENCES

[1]. F. Jiang, K. Dashtipour, and A. Hussain, "A Survey on Deep Learning for the Routing Layer of Computer Network," in *Proc. 2019 UK/China Emerging Technologies (UCET)*, Glasgow, UK, 2019, pp. 1-4.

[2]. C. L. Hedrick, "Routing Information Protocol," Tech. Rep., 1988.

[3]. J. Moy, "OSPF Protocol Analysis," Tech. Rep., 1991.

[4]. Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," Tech. Rep., 2005.

[5]. B. Mao, Z. M. Fadlullah, F. Tang, N. Kato, O. Akashi, T. Inoue, and R. Miura, "Routing or Computing? The Paradigm Shifts Towards Intelligent Computer Network Packet Transmission Based on Deep Learning," *IEEE Transactions on Computers*, vol. 66, no. 11, pp. 1946-1960, 2017.

[6]. N. Kato, Z. M. Fadlullah, B. Mao, F. Tang, O. Akashi, T. Inoue, and R. Miura, "The Deep Learning Vision for Heterogeneous Network Traffic Control: Proposal, Challenges, and Future Perspective," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 146-153, 2017.

[7]. D. Jiang, "Application of Artificial Intelligence in Computer Network Technology in Big Data Era," in *Proc. 2021 Int. Conf. Big Data Analysis and Computer Science (BDACS)*, Wuhan, China, 2021, pp. 254-257.

[8]. P. Sun, J. Li, J. Lan, Y. Hu, and X. Lu, "RNN Deep Reinforcement Learning for Routing Optimization," in *Proc. 2018 IEEE 4th Int. Conf. Computer and Communications (ICCC)*, Chengdu, China, 2018, pp. 285-289.

[9]. T. P. Lillicrap, J. J. Hunt, A. Pritzel, N. Heess, T. Erez, Y. Tassa, D. Silver, and D. Wierstra, "Continuous Control with Deep Reinforcement Learning," *Computer Science*, vol. 8, no. 6, pp. A187, 2015.

[10]. J. Xiao and Z. Zhou, "Research Progress of RNN Language Model," in *Proc. 2020 IEEE Int. Conf. Artificial Intelligence and Computer Applications (ICAICA)*, Dalian, China, 2020, pp. 1285-1288.

[11]. T. V. Phan, S. Sultana, T. G. Nguyen, and T. Bauschert, "Q-TRANSFER: A Novel Framework for Efficient Deep Transfer Learning in Networking," in *Proc. 2020 Int. Conf. Artificial Intelligence in Information and Communication (ICAIIC)*, Fukuoka, Japan, 2020, pp. 146-151.

[12]. C. Tan, F. Sun, T. Kong, W. Zhang, C. Yang, and C. Liu, "A Survey on Deep Transfer Learning," in *Artificial Neural Networks and Machine Learning -- ICANN 2018*, Rhodes, Greece, 2018, pp. 270-279.

[13]. M. H. Haghighat and J. Li, "Intrusion Detection System Using Voting-Based Neural Network," *Tsinghua Science and Technology*, vol. 26, no. 4, pp. 484-495, Aug. 2021.

[14]. *KDD Cup 1999 Data*, 1999. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[15]. M. H. Haghighat, Z. Abtahi Foroushani, and J. Li, "SAWANT: Smart Window-Based Anomaly Detection Using Netflow Traffic," in *Proc. 2019 IEEE 19th Int. Conf. Communication Technology (ICCT)*, Xi'an, China, 2019, pp. 1396-1402.

[16]. M. M. Raikar, "PhD Forum: Data Traffic Classification Using Deep Learning Models," in *Proc. 2021 IEEE 22nd Int. Symp. World of Wireless Mobile and Multimedia Networks (WoWMoM)*, Pisa, Italy, 2021, pp. 219-220.

[17]. Boozary, Payam. "The Impact of Marketing Automation on Consumer Buying Behavior in the Digital Space Via Artificial Intelligence." Power System Technology 48.1 (2024): 1008-1021.

[18]. Ayyalasomayajula et al., Madan Mohan Tito "Proactive Scaling Strategies for Cost-Efficient Hyperparameter Optimization in Cloud-Based Machine Learning Models: A Comprehensive Review." ESP Journal of Engineering & Technology Advancements, vol. 1, no. 2, 6 Dec. 2021, pp. 43-56.

[19]. Ayyalasomayajula et. al., Madan Mohan Tito. "A Cost-Effective Analysis of Machine Learning Workloads in Public Clouds: Is AutoML Always Worth Using?" International Journal of Computer Science Trends and Technology (IJCST), Oct. 2019.

[20]. H. Derbel, N. Agoulmine, and M. Salaun, "ANEMA: Autonomic Network Management Architecture to Support Self-Configuration and Self-Optimization in IP Networks," *Computer Networks*, vol. 53, no. 3, pp. 418-430, 2009.

[21]. O. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, "Intrusion Detection Systems of ICMPv6-Based DDoS Attacks," *Neural Computing and Applications*, vol. 30, no. 1, pp. 45-56, 2018.

[22]. C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954-21961, 2017.

[23]. T. V. Phan, S. Sultana, T. G. Nguyen, and T. Bauschert, "Q-TRANSFER: A Novel Framework for Efficient Deep Transfer Learning in Networking," in *Proc. 2020 Int. Conf. Artificial Intelligence in Information and Communication (ICAIIC)*, Fukuoka, Japan, 2020.

[24]. Premkumar Reddy, Yemi Adetuwo and Anil Kumar Jakkani, Implementation of Machine Learning Techniques for Cloud Security in Detection of DDOS Attacks, International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp.25-34. doi: https://doi.org/10.17605/OSF.IO/52RHK

[25]. Adeola Agbonyin, Premkumar Reddy, Anil Kumar Jakkani, Utilizing Internet of Things (IOT), Artificial Intelligence, and Vehicle Telematics for Sustainable Growth in Small, and Medium Firms (SMES), International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp. 182-191. doi: https://doi.org/10.17605/OSF.IO/QX3DP

[26]. Nalla, Akash, and Anil Kumar Jakkani. "A Review on Recent Advances in Chatbot Design." integration 3.3 (2023).

[27]. Srivastava, Pankaj Kumar, and Anil Kumar Jakkani. "FPGA Implementation of Pipelined 8× 8 2-D DCT and IDCT Structure for H. 264 Protocol." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.

[28]. Srivastava, P. Kumar, and A. Kumar Jakkani. "Android Controlled Smart Notice Board using IoT." International Journal of Pure and Applied Mathematics 120.6 (2018): 7049-7059.