Secure Network Topology Design and Management Using Artificial Intelligence Framework

Vaidheyar Raman Balasubramanian
SASTRA Deemed University
Thanjavur, India
bvram18@gmail.com

Akhil Gupta
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Pune, Maharashtra, India
akhilgupta112001@gmail.c

Nusrat Shaheen
Western Govern University
Salt Lake City, UT
nusratsha92@gmail.com

Srinivasan Jayaraman
Maharishi International University
Fairfield, IA, USA
srinivas1985@gmail.com

Nandish Shivaprasad
Missouri University of Science and Technology
MO, United States
ddatascholar@gmail.com

Neelima Singh
Department of Computer Science and Engineering
Uttaranchal University
Dehradun, India
singh13.neelima@gmail.com

Abstract—Network topology Designing and management of secure networks is designed to protect the confidentiality, integrity and availability of data in a networked environment. Due to the increase in advanced cyber-attacks, traditional network security approaches are no longer enough. In this regard, an AI framework can be used to protect the network structure. It was an AI framework that used algorithms and machine learning techniques to analyze data traffic and detect vulnerabilities in the network. The framework uses these analyses to adapt network configurations and optimize security protocols in real time, thus making it more resilient against threats. In addition, the AI framework not only allows but enables dynamic network management naturally. Its ability to identify and adapt to stray network behaviors, whether they are from malware or denial-of-service attacks, allows it to mitigate those threats and ensure consistent performance and security. Besides, the framework of AI can also help in designing network topology, keeping in view network traffic patterns, user behavior, and possible attack vectors. This creates a stronger and more efficient network topology that is better designed to withstand security threats. The AI Framework for Network Topology Design and Management is a sophisticated approach that combines advanced algorithms, machine learning techniques, and expert knowledge to optimize network performance and ensure cost-effective security.

Keywords— Management, Confidentiality, Framework, Network, Performance.

I. INTRODUCTION

Network topology design is an essential element for managing data and securing communication across the network. The growing technology is making it even more challenging to create and maintain a secure network topology in order to prevent sensitive information from being a victim of cyber-attacks and data breaches [1]. In fact, AI frameworks are changing the game, ushering in innovative approaches to network topology design and management. AI framework for network topology design is also capable of ongoing integration with existing security systems and learning and adapting to new threats [2]. The systematic network topology data gathered is fed into AI models (like machine learning or deep learning), which, due to the vast amount of network data processed in real-time (including anomaly-based detection), uphold the network to its best performance after comparing (for example) the performance of the current and new network topology [3]. This not only enhances network security but also relieves IT professionals from the burden of manual monitoring and analysis. So , in addition to hierarchical configuration, enterprise engineers also provide role-based access and segmentation of resources. It helps prevent unauthorized access or alterations, thereby minimizing the potential for data leaks or tampering. Access control policies help AI frameworks dynamically supervise and manage the users' access rights based on their activities and behaviour patterns [4]. Suppose an employee attempts to access sensitive data outside of their role, for instance. In that case, data access can be restricted, or the attempt can trigger an alert to prevent a security threat. User access management is one thing, and network traffic should be managed, which AI can help with, too [5]. The overflow of packets can be harmful, too, so traffic management is essential for destroying the efficiency of the network, as well as dangerous threats from packet floods [6]. Traffic management systems powered by AI are capable of analyzing real-time data and optimizing network parameters such as bandwidth, routing paths, etc., to alleviate congestion and improve overall network efficiency. Moreover, it can also identify anomalous traffic patterns and take remediation action to avoid potential security breaches [7]. AI frameworks can be used to manage and monitor network devices. Routers, switches, and firewalls are called network devices that are prone to cyber-attacks and need constant monitoring and regular updates to adapt to potential threats [8]. For example, AI can be used to monitor the status of these devices remotely, analyze for any suspicious activity, and automatically update the device settings to reduce any security threat. This lightens the load off of IT professionals and ensures that the network devices are always up-to-date and secure [9]. The absence of visibility and centralized control across the network becomes one of the significant challenges in designing and managing network topology [10]. Different devices, applications, and networks work simultaneously, which makes it challenging to monitor and manage every part of the network. AI frameworks can work together to provide a single view of the network IT professionals can use to gain a comprehensive perspective on the security posture and identify weaknesses [11]. This allows for more efficient and proactive network management, minimizing the response time to mitigate possible security threats. However, we should emphasize that AI is not a silver

bullet for network topology design and management. Organizations differ in their use cases, and there is no one-size-fits-all approach to implementing AI frameworks to meet their requirements. Creating and maintaining an AI-augmented network security architecture demands highly skilled professionals [12][13]. Hence, it is vital for organizations to invest in training and employing experts in this field. To summarise, network topology design and management set to an AI framework can also be helpful in the network security domain. The Cyber Security Solution allows for an innovative, proactive approach to minimizing the effects of a cyber-attack and data breaches, reduces the workload placed on IT professionals, improves overall security posture and builds confidence in the organization. Nonetheless, organizations must define and customize AI technologies to align with their specific needs and must ensure that the framework is trained and managed appropriately [14][15]. As cyber-attacks grow in sophistication, AI-enabled network security is no longer a luxury but rather a requirement for organizations to safeguard sensitive data and ensure communication remains secure within the network. The main contribution of the paper has the following

- It leverages machine learning algorithms and predictive analytics to detect and respond to potential cyber threats, minimizing the risk of data breaches and unauthorized access.
- Artificial intelligence can free up critical human resources by monitoring network infrastructure and determining potential issues in real-time. It improves network performance while lowering the burden on IT teams.
- This AI framework is used in secure network topology design and management, allowing the network to adapt to changing environments and evolving threats.

II. Related Works

The authors [16] have discussed AI and IoT fusion technology, where a rapid increase in network security has drawn attention. Researchers are studying optimization algorithms for factors such as traffic variables, disturbance, etc. The authors [17] have discussed Network AI or artificial intelligence, which refers to advanced machine learning algorithms that can be used to automate and optimize network operations, including actions like traffic routing, resource allocation, and network security. It will improve the effectiveness of the network, depending less on human error, reducing costs and enabling efficient and reliable scaling. AI also allows for self-healing networks, predictive maintenance, and intelligent troubleshooting. The authors [18][19] have discussed it presents a potent model for enhancing the scheduling and routing methods in edge-aided software-defined wireless sensor networks. It utilizes moving target defence and artificial intelligence techniques to manage resources more effectively and securely. It may make WSNs work better, especially finding a specified destination in an environment with changing dynamics. The authors [20] have discussed how these frameworks and use case applications are used to confront some of these challenges and outline potential future research paths. The authors [21][22] have discussed the integration of computer networks and artificial neural networks, an AI-based network operator capable of managing and optimizing computer networks in real-time. This combination substantially enhances network performance and reliability by using machine learning algorithms to analyze network data and make intelligent decisions [23][24].

A. Research Gaps

- The existing network topology designs and management use manual monitoring that requires human interaction to respond to security breaches or cyber threats, they are inefficient in handling security incidents.
- The more connected devices we have, the more complex topology design and management become, especially with decentralized networks. Network complexity quickly adds up, but traditional approaches tend to neglect the gnarly bits of the security problem.
- AI-powered systems can utilize machine learning algorithms to periodically dynamically detect, learn from, and adapt to emerging security threats, enhancing the overall security of the network.
- AI-based frameworks can make dynamic decisions about resource allocation by learning from the current network traffic and demands.
- Most organizations already have security systems, and integrating an AI-based framework can be a complex process.

III. Proposed Model

The topology design leverages AI algorithms to assess multiple network structures and identify the most secure and efficient one based on criteria such as network traffic, devices, and security protocols [25]. As a result, the risk of cyber-attacks should be reduced, and network performance should be improved. The monitoring part uses machine learning to continuously look at network behaviour and pique abnormal behaviour or unusual patterns. This will allow for early noticing of possible threats, which in turn encourages responding to avoid cyber-attacks being successful. The intrusion detection component utilizes deep learning methods to monitor network traffic and detect anomalous behaviour that suggests an attack is currently taking place. It will enable real-time detection and prevention of cyber-attacks that can limit the impact of potential breaches. In this paper, authors integrate AI within network design, which is capable of self-learning and providing ML-based, transparent security for the designed network, which can yield resilient defence against the dynamic nature of threats. It will enable organizations to have a more secure and resilient network infrastructure, where the probability of cyber-attacks is reduced, and the safety, precision and access of their information are guaranteed.

A. Construction

These devices can be switches, routers, firewalls, and servers. Since your network can be accessed and threatened by outside sources, a secure network topology ensures that your inside network is not accessible without proper permissions, helping to protect your areas of vulnerability from cyber-attacks or malicious activity. AI is now a fundamental component of technology in secure network topology. Using this method in real time can help prevent cyber-attacks before they impact an organization. Proper network information and the areas that can fall under a security attack must be known clearly because designing &

managing a safe network topology is not such an easy job. Fig 1: Shows the Construction Model.

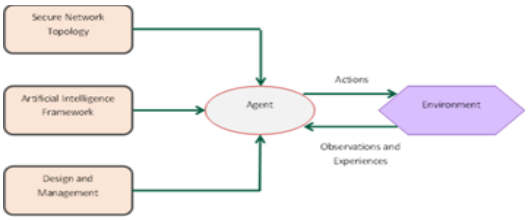

Fig. 1. Construction Model

Risk assessment generally follows from this, at which potential threats and vulnerabilities are identified. Results are used to design and configure network topology for the maximum security. An attack could potentially lead to damaging financial and reputational harm that can have dire consequences for an organization without the correct security measures in place. A secure network topology is only as effective as the context in which it is applied. In the atmosphere of climate change, regularly assessing and updating network security measures and controls are fundamental to recognizing and, most importantly, adjusting and preventing becoming a casualty to possible dangers.

B. *Proposed Algorithm*

Topology as an architecture defines how devices, services, and protocols are organized and programmed on a network. A secure network topology involves several different security measures that are carefully employed. Some of these are firewalls, an intrusion detection system, antivirus software, and access control systems. These factors will be critical in deciding the process and remediation of secure network topology. The first step towards developing a secure network is feature extraction, where we find valuable information and extract different types of features from network flow. Fig 2 Shows the Proposed Algorithm Model.

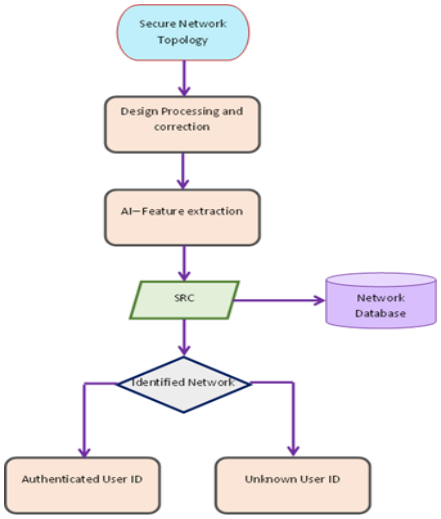

Fig. 2. Proposed Algorithm Model

This culture ensures that all of the people are definitely going to be going within the network and doing it authentically, and in no way can you catch the data if you are not the licensed operator. The identification/label is applied to the source packet and embedded therein to indicate the preferred destination. The infrastructure nodes use it as they follow the route. It contains information about network traffic, security events, and user activities. Knowing the types of devices and components that live on your network is another vital part of a secure network topology. This involves identifying servers and other network devices, as well as end-user devices such as computers and mobile devices.

IV. Results And Discussion

A. *Network Security*

The above four parameters derive the technical performance parameter for the design and management of secure network topology based on artificial intelligence framework, which is the level of network security. It is a way to secure a computer network by connecting an external Internet Protocol address to an internal one. Table.1 shows the comparison of network security.

TABLE I. Comparison Of Network Security (In %)

No. of Inputs	Comparison Models				
	IoTM	AIM	SRM	ICNM	Proposed Model
11	31.2	32.9	33.5	34.8	55.0
12	32.1	34.7	35.4	43.6	57.5
13	36.8	38.1	39.9	41.3	52.4
14	33.2	44.6	38.9	40.2	55.1
15	39.1	36.5	44.2	31.9	57.4

Where, IoTM- Internet of Things Model, AIM- Artificial Intelligence Model, SRM- Secure Routing Model, ICNM- Integration of Computer Networks Model

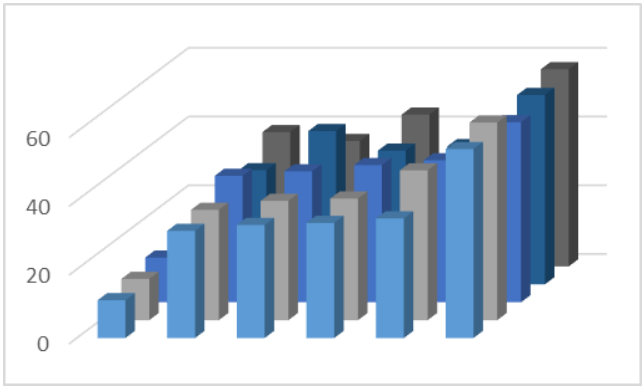

Fig. 3. COMPARISON OF NETWORK SECURITY (IN %)

This can include AI algorithms which monitor, detect, identify, and analyze potential threats, as well as firewalls, intrusion detection systems, and encryption methods as shown in Fig. 3.

B. *Scalability*

The parameters to focus on include the existing network topology, management framework, and scalability. Scalability is defined as the ability of the network to grow and scale with increasing demand while maintaining security and performance. Answer: Scalability, especially as networks connect more devices and more data floods into them. Table.II shows the comparison of scalability.

TABLE II. Comparison Of Scalability (In %)

No. of Inputs	Comparison Models				
	IoTM	AIM	SRM	ICNM	Proposed Model
05	31.6	41.3	32.8	34.1	84.5
08	35.7	36.9	43.1	45.4	83.3
11	39.8	40.6	38.2	42.1	81.7
14	34.3	35.2	44.0	41.4	82.7
17	43.8	45.2	33.9	34.6	86.3

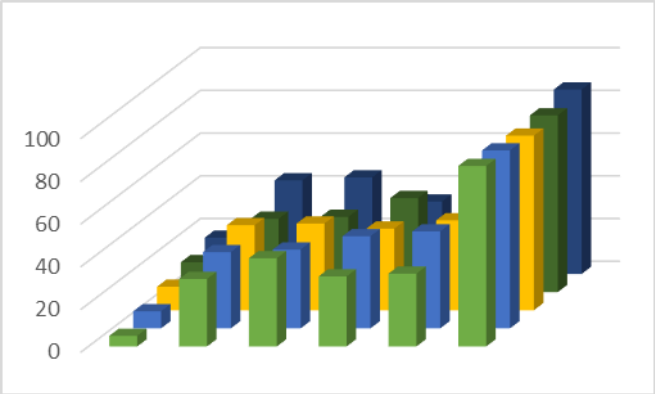

Fig. 4. COMPARISON OF SCALABILITY (IN %)

This challenge can potentially be mitigated by using AI to optimize and dynamically adjust the network topology according to increasing demand and traffic as shown in Fig. 4.

C. Reliability

The Design and Management Framework of Any Trusted Network Topology should also be highly reliable. Trust is the ability of the network to deliver service consistently and dependably despite failures or disruptions. Table.III shows the comparison of reliability

TABLE III. COMPARISON OF RELIABILITY (IN %)

No. of Inputs	Comparison Models				
	IoTM	AIM	SRM	ICNM	Proposed Model
04	37.3	38.7	31.1	32.5	44.9
08	35.0	39.6	42.8	31.4	43.6
12	41.0	31.5	36.2	37.7	45.7
16	40.1	44.9	43.2	45.6	48.3
20	32.3	39.4	31.3	34.4	43.0

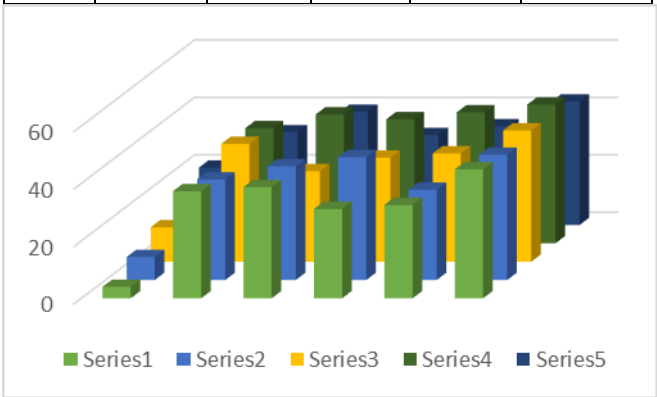

Fig. 5. COMPARISON OF RELIABILITY (IN %)

AI can also help achieve reliability by monitoring the work of network components and promising potential problems. These can include various techniques such as automatic failover, load balancing, and failure tolerance as shown in Fig. 5.

V. CONCLUSION

With the increasing reliance on transmitting information and digital communication, the discussion surrounding the field of network security has also significantly expanded. For organizations to protect themselves from cyber threats and ensure the confidentiality integrity, and availability of their network infrastructure, secure network topology design and management has become one of the most important disciplines. The article reports on a novel technique based on protocol optimization through artificial intelligence towards providing an approach to performance enhancement and security in network topologies. The paper will provide technical closure on the domain of Secure Network Topology Design and Management Using Artificial Intelligence Framework. With AI, the network needs flexible and robust topologies; the architecture needs intelligent threat monitoring and automatic/corrective actions. AI systems use machine learning algorithms to monitor large volumes of network data, identify patterns and anomalies, and initiate automated responses, which can help prevent a potential security breach. Ultimately, this improves the speed with which the system can detect threats and reduces the burden placed upon the network administrator. AI enables the management of network topologies by resource optimization and vulnerability pinpointing. It does this by using predictive analytics to detect meiotic threats and then prioritize security based on those predictions. Integrating AI solutions with virtual assistants can enable organizations to have real-time monitoring and alerting capabilities, minimizing the time from detection to response when security incidents occur. AI streamlines the use of zero-trust architecture in network security, ensuring that every packet of network traffic is monitored and authenticated by the AI system, thus prohibiting unauthorized access. This method adds another level of security and lowers the chances of internal endings.

REFERENCES

[1] W. Fei, "Research on optimization algorithms for artificial intelligence network security management based on All IP Internet of Things fusion technology," Comput. Electr. Eng., vol. 115, p. 109105, 2024.

[2] D. S. S. Satyanarayana and K. M. V. V. Prasad, "Multilayered antenna design for smart city applications," in Proc. 2nd Smart Cities Symp. (SCS), Bahrain, 2019, pp. 1–7, doi: 10.1049/cp.2019.0229.

[3] R. Dhull, D. Chava, D. V. Kumar, K. M. Prasad, G. Samudrala, and M. V. Bhargav, "Pandemic stabilizer using smartwatch," in Proc. Int. Conf. Decision Aid Sci. Appl. (DASA), Sakheer, Bahrain, 2020, pp. 860–866, doi: 10.1109/DASA51403.2020.9317056.

[4] M. V. V. P. Kantipudi, S. Vemuri, S. S. Kashyap, R. Aluvalu, and Y. S. Kumar, "Modeling of microstrip patch antenna using artificial neural network algorithms," in Commun. Comput. Inf. Sci., 2021, pp. 27–36, doi: 10.1007/978-981-16-3653-0_3.

[5] M. P. Kantipudi, S. Rani, and S. Kumar, "IoT-based solar monitoring system for smart city: An investigational study," in Proc. 4th Smart Cities Symp. (SCS), Bahrain, 2021, pp. 25–30, doi: 10.1049/icp.2022.0307.

[6] A. Bagwari et al., "Intelligent computational model for energy efficiency and AI automation of network devices in 5G communication environment," Tsinghua Sci. Technol., vol. 29, no. 6, pp. 1728–1751, 2024.

[7] S. Chamoli, P. K. Singh, S. S. Chauhan, and S. P. Yadav, "Web user access path prediction using recognition with recurrent neural network," in A Practitioner's Approach to Problem-Solving Using AI, Bentham Science Publishers, 2024, pp. 104–116.

[8] H. Alsaif et al., "Design and optimization of a MXene-based terahertz surface plasmon resonance sensor for malaria detection," Plasmonics, pp. 1–11, 2024.

[9] K. Purohit et al., "News event detection methods based on big data processing techniques," in A Practitioner's Approach to Problem-Solving Using AI, Bentham Science Publishers, 2024, pp. 117–129.

[10] A. Baz, J. Logeshwaran, Y. Natarajan, and S. K. Patel, "Deep fuzzy nets approach for energy efficiency optimization in smart grids," Appl. Soft Comput., vol. 161, p. 111724, 2024.

[11] S. Bansal et al., "Optoelectronic performance prediction of HgCdTe homojunction photodetector in long wave infrared spectral region using traditional simulations and machine learning models," Sci. Rep., vol. 14, no. 1, p. 28230, 2024, doi: 10.1038/s41598-024-79727-y.

[12] S. Singh, M. K. Maurya, N. P. Singh, and R. Kumar, "Survey of AI-driven techniques for ovarian cancer detection: State-of-the-art

methods and open challenges," Netw. Model. Anal. Health Inform. Bioinform., vol. 13, no. 1, p. 56, 2024, doi: 10.1007/s13721-024-00491-0.

[13] P. K. Verma, J. Kaur, and N. P. Singh, "An intelligent approach for retinal vessels extraction based on transfer learning," SN Comput. Sci., vol. 5, no. 8, p. 1072, 2024, doi: 10.1007/s42979-024-03403-1.

[14] S. Kumar, C. Verma, M. S. Raboaca, Z. Illés, and B. C. Neagu, "Face spoofing, age, gender, and facial expression recognition using advanced neural network architecture-based biometric system," Sensor J., vol. 22, no. 14, pp. 5160–5184, 2022.

[15] A. Pal et al., "Oral cancer detection at an earlier stage," in Proc. Int. Conf. Comput. Electron. Wireless Commun. (ICCWC), Singapore, Dec. 2023, pp. 375–384, doi: 10.1007/978-981-97-1946-4_34.

[16] A. Jain, S. Rani, H. Alshazly, S. A. Idris, and S. Bourouis, "Deep neural network-based vehicle detection and classification of aerial images," Intell. Autom. Soft Comput., vol. 34, no. 1, pp. 119–131, 2022.

[17] S. Kumar et al., "A comparative analysis of machine learning algorithms for detection of organic and non-organic cotton diseases," Math. Probl. Eng., vol. 21, no. 1, pp. 1–18, 2021.

[18] B. Shah, P. Singh, A. Raman, and N. P. Singh, "Design and investigation of junction-less TFET (JL-TFET) for the realization of logic gates," Nano, p. 2450160, 2024, doi: 10.1142/S1793292024501601.

[19] N. S. Ujgare et al., "Non-invasive blood group prediction using optimized EfficientNet architecture: A systematic approach," Int. J. Inf. Gen. Signal Process., 2024, doi: 10.5815/ijigsp.2024.01.06.

[20] R. Saklani et al., "A neural network study of face recognition," in A Practitioner's Approach to Problem-Solving Using AI, Bentham Science Publishers, 2024, pp. 142–157.

[21] R. C. Poonia et al., "Finding real-time crime detections during video surveillance by live CCTV streaming using deep learning models," in Proc. 10th Int. Conf. Comput. Artif. Intell., 2024, pp. 272–277.

[22] N. K. Agrawal et al., "Enhancing data aggregation efficiency: Dynamic energy-aware strategies in wireless sensor networks," in Proc. Int. Conf. Smart Devices (ICSD), Dehradun, India, 2024, pp. 1–5, doi: 10.1109/ICSD60021.2024.10750980.

[23] S. Kumar et al., "Automatic face mask detection using deep learning-based MobileNet architecture," in Proc. 6th Int. Conf. Contemporary Comput. Informat. (IC3I), Gautam Buddha Nagar, India, 2023, pp. 1075–1080, doi: 10.1109/IC3I59117.2023.10397772.

[24] R. Verma et al., "Deep neural network model for improved DDoS attack detection in cloud environments," in Proc. 5th Int. Conf. Emerging Technol. (INCET), Belgaum, India, 2024, pp. 1–6, doi: 10.1109/INCET61516.2024.10593561.

[25] H. A. Al-Alshaikh et al., "Comprehensive evaluation and performance analysis of machine learning in heart disease prediction," Sci. Rep., vol. 14, no. 1, p. 7819, 2024.