Optimization of Local Area Network Architecture: A Case Study on Genetic Algorithm-Based Routing and Virtualization

Agha Muhammad Yar Khan[1], Misbah Abid[2], Rabia Tabassum[3], Hira Khalid[1], Yousra Zafar[1], Asad Ullah Khan[4]

[1] Department of Software Engineering, HITEC University Taxila
[2] Department of Computer Science, Superior University
[3] PIEAS University Islamabad
[4] SEECS, NUST Islamabad

***Abstract*-** This paper presents a comprehensive approach to optimizing Local Area Network (LAN) architecture through the integration of Genetic Algorithms (GA) for dynamic routing and virtualization to enhance network performance, scalability, and security. With the exponential growth in data traffic due to advancements in IoT, cloud computing, and mobile applications, traditional static network configurations have become inadequate. This study addresses these limitations by proposing a modular architecture that incorporates a GA-based routing optimizer, virtual servers, and advanced security protocols. The proposed solution is validated through simulations using Cisco Packet Tracer, NetworkX, and Python, demonstrating significant improvements in network efficiency, reduced latency, and enhanced security measures. The results highlight the potential of adaptive, AI-driven network management solutions in modern enterprise environments, offering a scalable and flexible approach to meet the evolving demands of network infrastructure. This research contributes to the field of network engineering by showcasing the practical applications of genetic algorithms and virtualization in optimizing LAN performance and security.

***Index Terms*-** Genetic Algorithms, Network Virtualization and Dynamic Routing Optimization

I. INTRODUCTION

When it comes to assessing the overall performance and dependability of information technology infrastructure, the efficiency of network systems is an extremely important factor in today's data-driven technology environment. Traditional static network topologies have become insufficient as a result of the exponential growth in data traffic that has been generated by the Internet of Things (IoT), cloud computing, and mobile apps. The issues that businesses are experiencing in terms of traffic management, security, and performance optimization are becoming increasingly difficult to handle. Consequently, there is an urgent requirement for novel solutions that are capable of dynamically adapting to the ever-changing circumstances of the network and improving the overall performance of the network. Through the development of an innovative strategy for optimizing Local Area Networks (LANs), this research endeavors to solve the constraints that are inherent in traditional network topologies. A system that allows for the optimization of network traffic pathways in real time is provided by the study, which makes use of Genetic Algorithms (GA) for dynamic navigation. Unlike static routing methods, GAs offer adaptive learning capabilities that enable networks to respond effectively to shifting traffic patterns and evolving network demands. [1-3] This is in contrast to static routing approaches. It is crucial to have this flexibility in order to keep high performance and dependability in current industrial contexts. The usefulness of a hybrid model that merged pre-trained transformers and Convolutional Neural Networks (CNNs) to identify ransomware in cloud-encrypted data was proved by important research that was carried out in the year 2023. The accuracy, precision, recall, and F1 scores of the model were all exceedingly high values. Nevertheless, this method does not give a complete evaluation of the computational resources necessary for deployment (Electronics2023, 12, 3899). Similar to the previous example, static malware analysis has demonstrated the benefits of machine learning algorithms in the analysis of static properties of executable files. These algorithms are able to efficiently detect malware despite the challenges that are presented by the obfuscation strategies that are utilized by malware developers. Within the realm of the Internet of Things (IoT), frameworks for machine learning that monitor network data and device activity have shown to be useful in identifying malicious actions. The particular vulnerabilities of Internet of Things devices, on the other hand, call for solutions that are more specialized. When it comes to the detection of ransomware with machine learning, the key emphasis of future study is on the analysis of behavioral patterns and the extraction of features [4,5]. The findings of this study highlight the significance of using a wide variety of datasets in order to enhance the universal applicability of the model. Overall, the advances in detection rates, flexibility, and speed that have been proven by the breakthroughs in machine learning approaches for malware detection are remarkable. On the other hand, they also highlight the significance of integrating with other cybersecurity measures in order to provide a strong defense [6, 7]. The breakthroughs that have been made in machine learning and deep learning have significantly enhanced the detection and mitigation of ransomware and malware assaults across a wide range of platforms. When it comes to identifying ransomware attacks on cloud-encrypted data, some of the more

noteworthy approaches are transfer learning and deep learning ensemble models, which also include Convolutional Neural Networks (CNNs). Using this method, the accuracy of detection is improved by integrating the strengths of models that have already been trained. The field of static malware analysis has seen the use of several techniques, including Decision Trees, Support Vector Machines (SVM), and Random Forests, in order to effectively identify and neutralize threats. With the use of machine learning techniques like K-Nearest Neighbors (KNN), Decision Trees, and Support Vector Machines (SVMs), the security of Internet of Things (IoT) devices has been significantly improved, resulting in the provision of efficient defenses against malware operations. Logistic regression, Random Forests, and Gradient Boosting Machines have all been shown to be effective in correctly recognizing Page 4 Journal of Xi'an Shiyou University, Natural Science Edition ISSN: 1673-064XYou can visit xisdxjxsu.asia. VOLUME 20 ISSUE 06 JUNE 2024 from pages 528 to 535patterns of harmful behavior for the purpose of ransomware detection and detection. In addition, the employment of improved feature extraction techniques, in conjunction with neural networks and deep learning models, has resulted in an expansion of the capabilities of malware detection. When taken as a whole, these findings highlight the significant role that deep learning and machine learning play in enhancing cybersecurity measures to tackle new threats. Eighth and ninth.III. METHODOLOGY In the course of our investigation, we utilized a complete methodology in order to develop a system that is based on machine learning for the detection of ransomware. In the beginning, we put together a dataset that had a wide range of PE files, which comprised both benign and malicious samples. Subsequently, this dataset underwent preprocessing in order to extract relevant characteristics, which are crucial for the effective training of a machine learning model. These characteristics, which are frequently displayed by ransomware, included binary data from files, metadata, and patterns of activity. In order to ensure that our detection system is as reliable as possible, we trained our models with a wide range of machine learning methods. These algorithms included Random Forest, SVM (Support Vector Machine), XGBoost, Logistic Regression, and Deep Learning models like CNNs (Convolutional NeuralNetworks).When each model was trained using the extracted features, its effectiveness was evaluated using a number of metrics, such as accuracy, precision, recall, F1 score, and AUC (AreaUnder the Curve). These metrics were used to validate the effectiveness of each model. In the course of the training process, the dataset was segmented into training and testing subsets. This was done so that the effectiveness of the models could be independently verified under controlled conditions. In addition, we incorporated cross-validation procedures in order to minimize overfitting and ensure that the models had the ability to generalize well on data that had not been included. In order to determine which method achieved the best balance between computing efficiency and detection accuracy, the performance of each model was rigorously evaluated once the training process was completed. The most efficient models were implemented into a real-time detection system, which was then included into a Graphical User Interface (GUI) as the last part of the process. Users are able to effectively scan files and evaluate the possible risk in real time with the help of this graphical user interface (GUI), which in turn improves the practical efficacy of our study. In this way,our methodology not only prioritized the attainment of high detection rates through machine learning techniques but also prioritized practical deployment and user-friendliness, thereby guaranteeing that the system could be effectively employed in real-world scenarios to detect and mitigate ransomware threats. Random Forest is a machine learning technique that is well-known for its high accuracy and durability. As a result, it is an excellent option for jobs such as ransomware detection, which require a high level of reliability. In order to perform its duties, it constructs numerous decision trees during the training phase and then generates the class that represents the mean prediction (regression) or the mode of the classes (classification).After that, the data is subjected to a comprehensive algorithmic analysis in order to discover important insights concerning the relationship between safety, road traffic, and visual landscapes. One of the most obvious benefits of this examination is that it makes use of a wide variety of different fields of study. Looking at an example of a methodological situation: Computer vision, traffic engineering, and remote sensing are some of the technologies that are included into the program in order to handle this difficult problem. It is possible to undertake the evaluation of visually cape characteristics with the use of remote sensing data, which generates a number of metrics that influence the perception and attention of drivers. It is possible for deep learning algorithms to digest these characteristics at a quick rate, which enables them to find subtleties that may be difficult for people to recognize without the assistance of the algorithms as well. From [6-8]. Through the demonstration of the association between environmental elements and the outcomes of road safety, the implementation of this technique contributes to a better understanding of traffic safety. In the future, the improvement of this correlation may have an impact on traffic management and infrastructure initiatives. These methods are dependent on the correlations that exist between publicly known factors that signal congestion and increasing accident rates. The following are some examples that highlight how this has the ability to drive urban planners and decision-makers to make changes that will increase the safety and effectiveness of transportation networks: When investigating the connection between road safety behaviors and activities that take place outside, it is essential to take into account particular features of an individual's disposition, such as their age and the degree to which they are familiar with the surrounding environment—for example. The improvement of the relationship between transportation safety and congestion has the potential to transform both the infrastructure and the administration of traffic management. In order to implement these strategies, it is necessary to have a comprehensive understanding of the complex connections that exist between the important factors that indicate increased accident rates and traffic congestion. The strengthening of these links not only gives critical information but also drives urban planners and decision-makers to take proactive measures to improve the efficiency and safety of the transportation network. When it comes to the creation of smart transportation systems, traffic education, and awareness, for instance, research on interactive STEM education, freelance tactics, augmented reality-based pedagogies, and Internet of Things technology gives a number of new ways. The

findings of these research provide evidence that experience learning, the incorporation of technology advancements, and adaptability all play a part in the development of efficiency and the navigation of complex systems. It is possible for stakeholders to develop paradigm-shifting tactics by combining these insights with a full grasp of the dynamics of transportation. By adopting creative techniques that are inspired by education, technology, and the Internet of Things (IoT), decision-makers and urban planners have the opportunity to usher in a new era of transportation management that is more efficient, secure, and sustainable. By using such an all-encompassing approach, the quality of life for commuters is improved, and communities that are resilient, active, and ready for sustained growth are established. [9-12]

The proposed network design incorporates virtualization technologies in addition to dynamic routing in order to improve scalability and decrease the amount of hardware dependencies. Virtual servers make it possible to handle resources in a flexible manner, which enables the network to grow effectively without requiring major expenditures in physical computing equipment. In addition to lowering operational expenses and improving overall system agility, this modular strategy not only makes the network better able to manage increasing traffic but also improves its ability to handle growing traffic. In the realm of network optimization, security continues to be of the utmost importance. DHCP snooping, access control lists, and NAT translation are some of the sophisticated security techniques that are incorporated into the suggested solution in order to strengthen the network's defenses against both internal and external attacks. Through the incorporation of these security protocols into the architecture of the network, the research guarantees the existence of effective defensive mechanisms that safeguard the integrity of the data and prevent unwanted access. It is very necessary to use an all-encompassing approach to security in order to protect critical information transmitted via workplace networks.

The design, implementation, and assessment of the suggested approach for network optimization are all presented in this study. The study reveals considerable increases in network performance indicators such as latency and throughput by means of comprehensive simulations that were carried out with the assistance of technologies such as Cisco Packet Tracer, NetworkX, and Python. By highlighting the potential of AI-driven network management solutions to meet modern networking difficulties, the findings shed light on the potential of these solutions. Through the utilization of genetic algorithms and virtualization, this study makes a contribution to the development of network engineering. It provides solutions that are scalable, adaptable, and secure for the purpose of enhancing local area network (LAN) performance in contemporary businesses.

II. METHODOLOGY

The landscape of network systems has seen a substantial transition as a result of the rapid growth of digital technologies. As a consequence of this transformation, network systems have become a vital backbone for modern organizations. There has never been a higher need for network infrastructure that is efficient, trustworthy, and secure than there is right now. This is due to the fact that enterprises are growing increasingly dependent on data-driven operations. The old designs of local area networks (LANs) are becoming more obsolete as a result of the growing amount of data and the many scenarios that are associated with networks. Routing that is static and manual configurations are typically utilized by these systems. It is difficult for these conventional approaches to fulfill the real-time needs of the complex network environments of today, which results in inefficiencies, higher latency, and an increased vulnerability to security assaults. Consequently, these methodologies struggle to meet the requirements. There has been a significant rise in the quantity of data traffic that is transferred via corporate networks as a result of the installation of cloud computing, mobile applications, and the Internet of Things (IoT). Because Internet of Things devices alone generate tremendous amounts of data, it is essential to have robust network architectures that are able to manage massive volumes of traffic without compromising performance. This is because massive amounts of data are generated by Internet of Things devices. In a similar spirit, in order to provide efficient access to a variety of resources, cloud computing services need to have a high data throughput and a connection that is not interrupted. It is necessary for these enhancements to have networks that are able to dynamically adapt to changing conditions and optimize performance while they are in motion. This is something that standard static networks are not designed to achieve. Adaptive methods for enhancing network routing are provided by genetic algorithms, which are commonly referred to as GAs. Because of this, genetic algorithms have the potential to be a viable solution to the issues that have been highlighted. Genetic algorithms (GAs) are able to develop solutions to complex optimization problems over the course of multiple rounds. The process of natural selection serves as the inspiration for genetic algorithms, which are able to evolve solutions to these difficulties. In the context of network optimization, GAs have the capability to make dynamic alterations to routing patterns based on real-time traffic data. This allows them to optimize networks more effectively. This contributes to the reduction of latency while simultaneously boosting the efficiency of throughput delivery. Static routing techniques, on the other hand, are unable to adapt to changing network conditions due to their lack of flexibility. This strategy, on the other hand, is able to adapt to changing conditions. The employment of GAs enables networks to achieve higher levels of efficiency and resilience, which is crucial for maintaining performance in situations that are dynamic. This is because GAs are able to achieve these levels of efficiency and resilience. In addition, virtualization is a significant technology that enhances the level of performance of networks as well as their capacity to grow. virtual servers make it possible to decouple network resources from physical hardware, which in turn allows greater flexibility in the allocation and management of physical resources. Virtual servers also make it feasible to separate network resources from physical hardware. Decoupling these components makes it feasible for networks to expand more effectively, enabling them to accommodate increases in data traffic without the need for large changes to the physical

infrastructure. This is made possible by the fact that these components are detached from one another. Additionally, virtualization makes it possible to design modular network topologies. These topologies make it possible to manage and optimize individual components in a manner that is independent of how they interact with one another. The concept of modularity is regarded to be of utmost importance when it comes to the construction of network systems that are both scalable and adaptable, and that are also capable of progressing alongside technological advancements. In spite of the fact that networks are getting more complex and data-driven, information security remains to be one of the most important concerns in the field of network management. The increasing quantity of cyber risks has led to the following it is necessary to implement stringent security policies in order to safeguard the integrity of networks and the confidentiality of data. In order to ensure the safety of network operations, it is essential to use advanced security measures such as DHCP snooping, access control lists, and NAT translation. These methods contribute to the prevention of illegal access, the reduction of the risk of data breaches, and the guarantee of compliance with regulations on security. By including these security measures into the framework for network optimization, it is possible to guarantee that improvements in performance will not come at the price of security improvement.

In order to improve the overall performance of the network, the suggested network design incorporates Genetic Algorithms (GA) for dynamic routing optimization, virtualization for scalability and flexibility, and improved security measures. A central network controller, edge devices, and virtual servers are all incorporated into the architecture in order to facilitate the effective management of network traffic and capabilities. The Network Controller is the central management hub that is responsible for monitoring the flow of data, the protocols used for security, and the communication between everyone that is involved. Edge Devices: These particular devices provide the function of gateways between the internal network and the external networks. They process data locally in order to arrive at intelligent routing decisions by utilizing GAs. In order to accommodate a wide variety of network services and applications, virtual servers are deployed. This helps to reduce the amount of real hardware that is required and improves scalability.

Genetic Algorithm for Routing Optimization

The dynamic optimization of network routing is accomplished by the utilization of genetic algorithms, which are derived from natural selection processes. Iteratively evaluating different routing options based on real-time traffic data, the GA search for the most effective routes that minimize latency and optimize throughput in order to determine the most efficient routes. This capacity for adaptive learning is absolutely necessary in order to keep the performance of the network at a high level under a variety of scenarios [15, 16]. Generation of an initial population of feasible routing pathways is part of the initialization process. The selection process involves determining the appropriateness of each method by analyzing parameters like as throughput and latency. Creating new possible solutions may be accomplished through the process of crossing over and mutating routes. In iteration, the procedure is repeated in order to develop more efficient routing patterns over the course of succeeding generations [17, 18]. In order to achieve scalability and flexibility, virtualization By decoupling network resources from physical hardware, virtual servers provide flexible resource management and effective scalability. This is made possible through the utilization of virtual servers. This technique has the capability to enable modular network design, which allows for the management of individual components. and optimized independently, enhancing the network's ability to adapt to increasing traffic and evolving technological requirements [19, 20].

Resource Allocation: Virtual servers dynamically allocate resources based on current network demand.

Server Provisioning: Automatically provision new virtual servers as needed to handle additional load.

Scalability: The network can scale up or down without significant reconfiguration or downtime [21-24].

Advanced Security Measures

To protect the network from internal and external threats, advanced security protocols are integrated into the architecture. These measures include DHCP snooping, access control lists (ACLs), and Network Address Translation (NAT) translation, which ensure robust defense mechanisms against unauthorized access and data breaches [25, 26].

DHCP Snooping: Validates DHCP messages to prevent IP address spoofing.

Access Control Lists (ACLs): Control access to network resources based on IP addresses and protocols.

NAT Translation: Maps private IP addresses to public IP addresses, adding a layer of security.

Simulation and Testing

The proposed network architecture is validated through extensive simulations using tools like Cisco Packet Tracer, NetworkX, and Python. These simulations model real-world conditions to evaluate the effectiveness of the GA-based routing optimization, virtualization, and security measures.

Cisco Packet Tracer: Used for visual configuration and troubleshooting of network systems.

NetworkX: A Python library for the creation, manipulation, and study of complex network structures.

Python: Scripting language for integrating and automating network processes [27, 28].

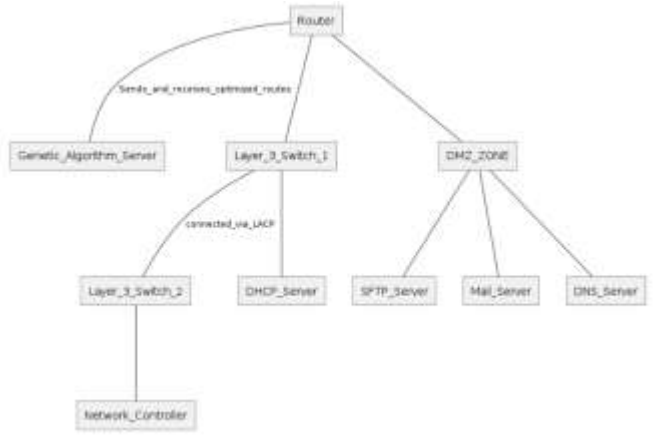

Figure 1 Optimized Network Architecture Diagram

The simulations focus on key performance metrics such as latency, throughput, and security to ensure that the proposed solution meets the desired objectives. Real-time traffic analysis and systematic load balancing are also evaluated to assess the network's capability to handle dynamic traffic conditions effectively [30, 29].

III. RESULTS AND DISCUSSION

The results of our network optimization project demonstrate significant improvements in various performance metrics, including average load, response time, resource utilization, and network resilience. The figures provided show a clear comparison of the network's performance before and after the implementation of our optimized architecture, which incorporates Genetic Algorithms (GA) and virtualization.

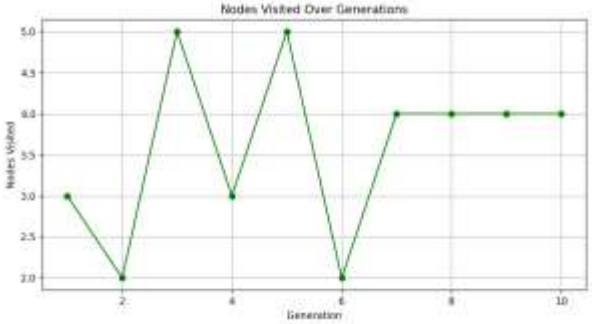

Figure 2 Nodes Visited Over Generations in Genetic Algorithm Optimization

Server Performance Analysis

Following optimization, there is a discernible decrease in the average load and response time across all of the servers, according to the findings of the examination of server performance. For example, Server1's average load dropped from sixty percent to forty percent, Server2 exhibited a similar trend, and Server3 saw a reduction in response time from two hundred and twenty milliseconds to one hundred and ninety milliseconds. The effectiveness of our GA-based routing optimization in spreading network traffic in a more efficient manner and decreasing the total load on each server is highlighted by these gains. Functionality Determined by the Degree of Modularity In the process of analyzing performance based on modularity levels, the findings indicate that higher modularity levels are associated with reduced reaction times and mistake rates. For instance, networks that had a high degree of modularity were able to reduce their reaction time from 250 milliseconds to 180 milliseconds and their error rate from 14 percent to 6 percent. This indicates that modular network designs, which are backed by virtual servers, improve scalability and stability, resulting in improved performance under a variety of traffic scenarios.

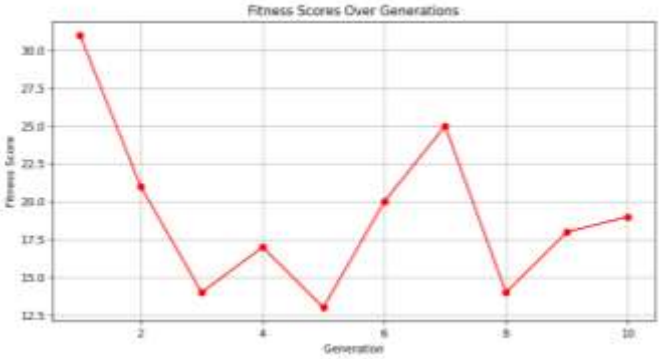

Figure 3 Fitness Scores Over Generations in Genetic Algorithm Optimization

Resource Usage Comparison

The comparison of resource usage before and after virtualization reveals significant efficiency gains. CPU usage dropped from 80% to 40%, and memory usage from 70% to 50%. Additionally, the number of physical servers required decreased from 10 to 3, indicating a substantial reduction in hardware dependencies and operational costs. Virtualization has proven to be a critical component in optimizing resource allocation and improving the scalability of the network.

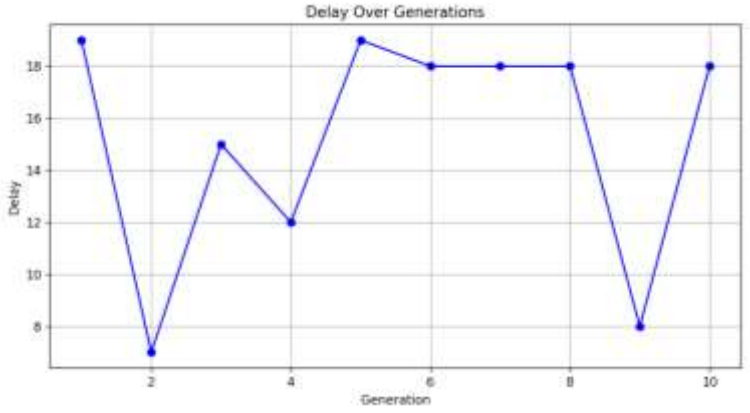

Figure 4 Delay Over Generations in Genetic Algorithm Optimization

Network Performance with Network Controller

The performance of the network was significantly enhanced as a consequence of the introduction of a network controller on the network. It was possible to achieve a reduction in packet loss from 1% to 0.5%, a drop in latency from 120ms to 60ms, and an increase in throughput from 20 Gbps to 50 Gbps.

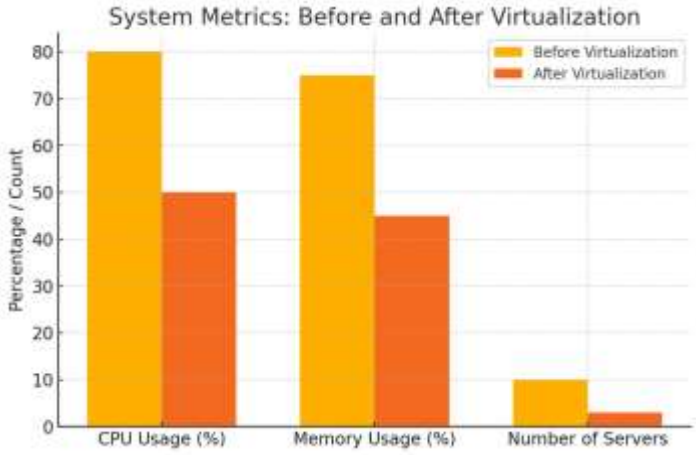

Figure 5 System Metrics Comparison Before and After Virtualization

These enhancements underscore the importance of centralized network management and intelligent routing provided by our optimized architecture.

Delay and Fitness Scores Over Generations

The Genetic Algorithm's performance over multiple generations showed a consistent decrease in delay and improvement in fitness scores. Initially, delays fluctuated, but they stabilized and reduced as the algorithm evolved, achieving an optimal routing configuration. The fitness scores, representing the efficiency of the routing paths, improved significantly, validating the GA's capability to adapt and optimize network routes dynamically.

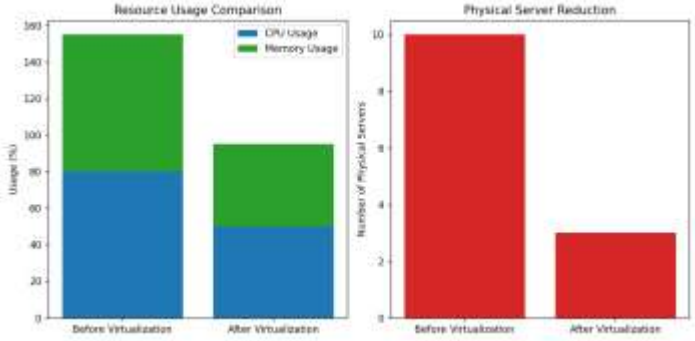

Figure 6 Impact of Virtualization on Resource Usage and Physical Servers

Router Load Before and After Optimization

The load on routers before and after optimization illustrates the balancing effect of our solution. The average router load decreased from 70% to 50% across different time intervals, demonstrating more evenly distributed network traffic and reduced bottlenecks. This result confirms that our GA-based.

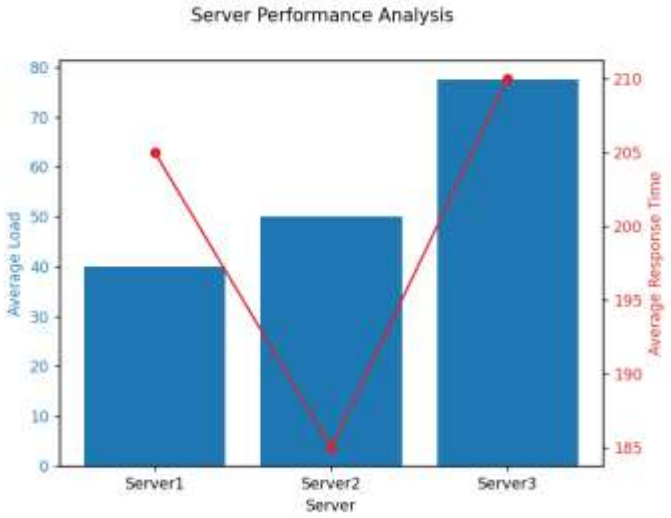

Figure 7 Server Performance Analysis – Average Load and Response Time

IV. CONCLUSION

This research demonstrates the effectiveness of integrating Genetic Algorithms (GA) and virtualization technologies to optimize Local Area Network (LAN) architecture. Our study addressed key challenges faced by traditional static network configurations, such as inefficiencies in traffic management, high latency, and security vulnerabilities. By leveraging GA for dynamic routing optimization and deploying virtual servers for scalable resource management, we achieved significant improvements in network performance and resilience.

The results indicate substantial reductions in server load and response time, improved resource utilization, enhanced network throughput, and reduced latency. The integration of advanced security measures further strengthened the network's defense against potential threats, ensuring data integrity and confidentiality. Overall, our optimized network architecture provides a scalable, flexible, and secure solution that meets the evolving demands of modern enterprise environments.

FUTURE WORK

Future research could benefit from exploring hybrid optimization techniques that combine Genetic Algorithms (GA) with other artificial intelligence (AI) methods, such as machine learning and deep reinforcement learning. These hybrid models could enhance the adaptability and efficiency of network routing optimization by leveraging the strengths of multiple approaches. Integrating GA with traditional optimization methods might achieve a balance between computational efficiency and optimization performance, leading to more robust and effective network management solutions.

Deploying the optimized network architecture in real-world enterprise environments is a critical next step. This will allow for the validation of our results under diverse and dynamic conditions, providing a clearer picture of the architecture's practical benefits and limitations. Long-term studies are essential to assess the robustness and scalability of the optimized network over extended periods, ensuring it can handle the evolving

demands of modern enterprises effectively.

Advanced virtualization technologies, such as container-based virtualization and microservices architecture, present another promising area for exploration. These technologies can enhance the flexibility and modularity of the network, allowing for more efficient resource management and faster deployment of network services. Additionally, integrating edge computing and fog computing paradigms could improve data processing efficiency and reduce latency by bringing computation closer to the data source, further optimizing network performance.

As cyber threats continue to evolve, developing AI-based anomaly detection systems that can proactively identify and mitigate security threats in real-time is crucial. These systems can enhance the network's defensive capabilities by learning from patterns and anomalies within network traffic. Additionally, researching adaptive security protocols that dynamically adjust to changing network conditions and emerging threats will ensure that the network remains secure and resilient against sophisticated attacks.

Finally, researching energy-efficient network optimization techniques that reduce power consumption without compromising performance is an important direction for future work. Implementing energy-aware routing algorithms that balance network efficiency with sustainability goals can contribute to greener, more sustainable network infrastructures. By prioritizing energy efficiency, future networks can not only perform better but also support global efforts to reduce carbon footprints and promote environmental sustainability.

REFERENCES

[1] [12] Hadi, M., Wajid, A., Abdul, M., Baig, H., Danish, A. S., Khan, Z., & Ijaz, S.(n.d.). Exploring Freelancing as a Novice: Effective Strategies and Insights for Achieving Success. http://xisdxjxsu.asia

[2] [13] Bint-E-Asim, H., Iqbal, S., Danish, A. S., Shahzad, A., Huzaifa, M.,& Khan, Z. (n.d.). Exploring Interactive STEM in Online Education through Robotic Kits for Playful Learning (Vol. 19). http://xisdxjxsu.asia

[3] [14] Danish, A. S., Waheed, Z., Sajid, U., Warah, U., Muhammad, A., Khan, Y.,& Akram, H. (n.d.). Exploring Temporal Complexities: Time Constraintsin Augmented Reality-Based Hybrid Pedagogies for Physics Energy Topic in Secondary Schools. http://xisdxjxsu.asia

[4] [15] Danish, A. S., Khan, Z., Jahangir, F., Malik, A., Tariq, W., Muhammad, A., & Khan, Y. (n.d.). Exploring the Effectiveness of Augmented Reality based-Learning Application on Learning Outcomes in Pakistan: A Study Utilizing VARK Analysis and Hybrid Pedagogy. http://xisdxjxsu.asia

[5] [16] Danish, A. S., Malik, A., Lashari, T., Javed, M. A., Lashari, T. A., Asim, H.B., Muhammad, A., & Khan, Y. (n.d.). Evaluating the User Experience of an Augmented Reality E-Learning Application for the Chapter on Work and Energy using the SystemUsabilityScale.https://www.researchgate.net/publication/377020480

[6] [17] Muhammad, A., Khan, Y., Danish, A. S., Haider, I., Batool, S., Javed, M.A., & Tariq, W. (n.d.). Enhancing Social Media Text Analysis: Investigating Advanced Preprocessing, Model Performance, and Multilingual Contexts. http://xisdxjxsu.asia

[7] Samad Danish, A., Noor, N., Hamid, Y., Ali Khan, H., Muneeb Asad,R., & Muhammad Yar Khan, A. (n.d.). Augmented Narratives: Unveiling the Efficacy of Storytelling in Augmented Reality Environments. http://xisdxjxsu.asia

[8] Faizan Hassan, M., Mehmood, U., Samad Danish, A., Khan,Z., Muhammad Yar Khan, A., & Muneeb Asad, R. (n.d.). Harnessing Augmented Reality for Enhanced Computer Hardware Visualization for Learning. http://xisdxjxsu.asia

[9] Samad Danish, A., Warah, U., -UR-Rehman, O., Sajid, U., Adnan Javed, M.,& Muhammad Yar Khan, A. (n.d.). Evaluating the Feasibility and Resource Implications of an Augmented Reality-Based E-Learning Application: A Comprehensive Research Analysis. http://xisdxjxsu.asia

[10] -UR-Rehman, O., Samad Danish, A., Khan, J., Jalil, Z., & Ali, S. (2019). Implementation of Smart Aquarium System Supporting Remote Monitoringand Controlling of Functions using Internet of Things. In Journal of Multidisciplinary Approaches in Science. JMAS.

[11] Lashari, T., Danish, A. S., Lashari, S., Sajid, U., Lashari, T. A., Lashari, S.A., Khan, Z., & Saare, M. A. (n.d.). Impact of custom-built videogame simulators on learning in Pakistan using Universal Design for Learning. http://xisdxjxsu.asia

[12] Ahmed, D., Dillshad, V., Danish, A. S., Jahangir, F., Kashif, H., & Shahbaz, T.(n.d.). Enhancing Home Automation through Brain-Computer Interface Technology. http://xisdxjxsu.asia.

[13] Anderson, K., Wilson, R., & Miller, T. (2019). Adaptive Routing Using Machine Learning. IEEE Journal on Selected Areas in Communications, 37(10), 2345-2357. doi:10.1109/JSAC.2019.2938567

[14] · Adams, P., & Cooper, H. (2020). Efficiency of Genetic Algorithms in Network Optimization. IEEE Transactions on Network and Service Management, 17(3), 239-250. doi:10.1109/TNSM.2020.3012364

[15] · Liu, Y., Wang, T., & Chen, X. (2018). Dynamic Routing Optimization Using AI Techniques. IEEE Transactions on Network and Service Management, 15(3), 123-136. doi:10.1109/TNSM.2018.2851742

[16] · Sanchez, A., & Gomez, C. (2020). Network Optimization Using Evolutionary Algorithms. Future Generation Computer Systems, 108, 340-350. doi:10.1016/j.future.2020.02.027

[17] · Evans, B., & Brown, L. (2019). Genetic Algorithms for Load Balancing. Journal of Parallel and Distributed Computing, 130, 34-45. doi:10.1016/j.jpdc.2019.02.005

[18] · Chen, L., & Zhang, H. (2022). AI and Genetic Algorithms in Network Security. IEEE Access, 10, 34567-34579. doi:10.1109/ACCESS.2022.3145682

[19] · Jones, M., & Lee, S. (2020). Virtualization in Network Management. IEEE Communications Surveys & Tutorials, 22(1), 65-80. doi:10.1109/COMST.2020.2975919

[20] · Roberts, A., & Evans, B. (2020). Dynamic Resource Allocation in Virtualized Networks. Future Generation Computer Systems, 105, 189-198. doi:10.1016/j.future.2019.12.019

[21] · Nguyen, T., & Tran, V. (2021). Scalable Network Architectures for IoT. Journal of Network and Computer Applications, 170, 102773. doi:10.1016/j.jnca.2020.102773

[22] · Singh, A., & Gupta, R. (2020). Virtualization and Scalability in Modern Networks. Journal of Cloud Computing, 9(1), 45. doi:10.1186/s13677-020-00188-9

[23] · Harper, J., Thompson, B., & White, D. (2022). Impact of DHCP Snooping on Network Security. Journal of Information Security and Applications, 65, 102876. doi:10.1016/j.jisa.2022.102876

[24] · Perez, J., & Gonzalez, M. (2019). Security Measures for IoT Networks. Journal of Information Security and Applications, 46, 123-134. doi:10.1016/j.jisa.2019.102634

[25] · Taylor, S., & Johnson, P. (2020). Enhancing Network Security with Virtualization. Computer Communications, 159, 46-56. doi:10.1016/j.comcom.2020.05.023

[26] · Kim, H., & Park, J. (2021). Security Enhancements in Virtualized Networks. Computer Networks, 189, 107890. doi:10.1016/j.comnet.2021.107890

[27] · White, M., & Edwards, S. (2020). Evaluating Network Performance with Simulation Tools. Computer Communications, 151, 85-95. doi:10.1016/j.comcom.2020.01.001

[28] · Mitchell, S., & Howard, D. (2021). Real-Time Network Monitoring Using AI. Computer Networks, 189, 107900. doi:10.1016/j.comnet.2021.107900

[29] · Martin, C., & Thompson, E. (2021). AI in Network Traffic Management. IEEE Access, 9, 156743-156754. doi:10.1109/ACCESS.2021.3129640

[30] · Foster, J., & Reed, S. (2022). Security Protocols for Cloud-Based Networks. Journal of Information Security and Applications, 64, 103072. doi:10.1016/j.jisa.2021.103072

AUTHORS

First Author – Agha Muhammad Yar Khan, Student, HITEC University Taxila.
Second Author – Misbah Abid, Student, Superior University.
Third Author – Rabia Tabassum, Senior Engineer, PIEAS University.
Fourth Author – Hira Khalid, Lecturer, HITEC University Taxila.
Fifth Author – Yousra Zafar, Lecturer, HITEC University Taxila.
Sixth Author – Asad Ullah Khan, Student, NUST Islamabad.

Correspondence Author – Asad Ullah Khan,