ISSN 2349-7815

International Journal of Recent Research in Electrical and Electronics Engineering (IJRREEE)
Vol. 13, Issue 1, pp: (1-14), Month: January - March 2026, Available at: www.paperpublications.org

OPTIMIZATION OF NETWORK RESILIENCE AND RELIABILITY USING ARTIFICIAL INTELLIGENCE AND MULTI-LAYERED ARCHITECTURE

PRINCEWILL CHINOMSO OKEKE

School of Computing & AI, Malaysia University of Science and Technology, Malaysia.

DOI: https://doi.org/10.5281/zenodo.18518629

Published Date: 07-February-2026

Abstract: **This study assesses various AI methodologies, such as reinforcement learning and deep neural networks, and their applicability in network optimization for network infrastructures. This study examines how artificial intelligence (AI) can improve a number of network-related tasks, including fault detection, resource allocation, and traffic management. AI-driven models that utilize machine learning (ML) algorithms to predict network behavior, manage traffic in real-time, and optimize resource utilization are gradually replacing traditional network management systems, which frequently rely on static configurations. This study focuses on optimizing resilient and dependable computer networks using a multi-layered architecture, network protocols, network components and elements. This study offers a comparative framework of analysis for network protocols, network components, and the OSI model layered architecture which consists of seven layers. This study uses layered architecture technology to explain the fundamentals of computer networking and offers a structured method of organizing networks and enhances scalability and flexibility.**

Keywords: **Artificial Intelligence, architecture, computer, components, layers, model, network optimization, protocols, machine learning.**

1. INTRODUCTION

1.1 An Overview of Network Optimization

Networks are the foundation for the seamless flow of data, voice, and multimedia communication throughout the worldwide digital landscape. As the demand for dependable, high-performance connectivity grows, network optimization has emerged as a top concern for telecommunications service providers. Network optimization is the entire process of improving the performance, efficiency, and resilience of networks to satisfy the dynamic and ever-changing needs of users and applications.

The fundamental goals of network optimization in the network industry are varied, including improving network performance by lowering latency, increasing throughput, and ensuring consistent connectivity. Network providers can deliver greater user experiences, lower operational costs, and preserve a competitive advantage in the quick expanding digital environment by improving network resource allocation and utilization.

1.2 An Introduction to Artificial Intelligence (AI) in Network Optimization

Rapid advances in Artificial Intelligence (AI) have fundamentally altered the landscape of the network business, providing new prospects for network optimization. AI, with its tremendous capabilities in machine learning, deep learning, and neural networks, has transformed the network industry, allowing providers to achieve new levels of network efficiency, responsiveness, and intelligence.

AI-powered solutions are progressively being integrated into many aspects of network operations, from traffic management and resource allocation to predictive maintenance and anomaly detection. Using AI's predictive and adaptive capabilities, telecommunication networks may dynamically adapt to changing conditions, maximize resource use, and proactively resolve future faults, thereby improving overall network performance and user experience.

1.3 An Introduction to Layered Architectures in Network Optimization

Any organization's success depends on designing resilient and dependable computer networks. One of the most popular methods for preserving network security and functionality is a layered architecture. Routing, switching, storage, and other services are just a few of the many components and protocols that can be used with this kind of architecture. Different layers enable each system component to be isolated from the others and operated independently, enhancing the overall system's reliability. Layered architectures can be constructed using a variety of protocols and technologies, including Ethernet, TCP/IP, and the Open System Interconnection (OSI) model. The most widely used protocol for tying together devices on the same network is Ethernet. It provides quick communication between devices using a token-passing system. The system requires that each device send only one request at a time and complete that request.

Additionally popular, TCP/IP enables dependable device-to-device communication across a range of networks. Each of these technologies and protocols has its own advantages and features and can be used to create dependable and secure computer networks. It's critical to compare these protocols while taking into account aspects like performance, cost, scalability, and security. In addition, the network's size and related services must be considered when determining each system's requirements. By carefully examining each protocol and technology, designers can develop efficient multi-tier architectures that provide the required level of reliability and security. The elements and protocols required to construct a dependable and secure computer network are provided by a multi-tiered architecture. The designer can create an architecture that is specifically suited to the requirements of the system by carefully examining the protocols and technologies that are currently in use. To ensure that the system offers the necessary level of reliability and security, factors such as performance, cost, scalability, and security are taken into account. A computer network is a group of hardware and software elements that enable two or more devices to communicate with one another. Computer networks are designed using a layered architecture with the physical layer, data link layer, network layer, transport layer, and application layer in order to ensure efficient, secure, and reliable data transfer.

2. BACKGROUND AND REVIEW OF RELATED WORK

Computer networks are a rapidly growing and evolving field. Effective use of computer networks requires an understanding of the various technologies used in layered architecture. Understanding the protocols and technologies that interact to enhance network performance is essential for designing layered architectures that result in resilient and dependable computer networks. Implementing link-layer error control to ensure reliability, as described in [1], provides a framework for architectural resilience. Network security should also be considered in the framework, as stated in [2]. Secure network architectures and protocols must be used at every layer to provide layer-by-layer security. Protocols for the physical and MAC layers are also specified by wireless network standards. Additionally, the SDN architecture can be separated into three layers, as described in [3]. For resilient protocols, the network layer can independently protect metadata. Increasing the effectiveness, dependability, and resilience of conventional power grids also requires the use of hierarchical, multi-layered architectures [4]. In order to achieve highly available and reliable network performance, SDN architecture using the Open-flow protocol has made significant advancements in terms of network resilience and flexibility [5]. Link-level encryption with shared network keys can be used to build secure networks, and network-wide replication of the state is a crucial step in creating a resilient network. [6]. Layering is a useful technique when creating computer networks. However, it is not always appropriate in all situations and should be implemented with caution, as stated in [7]. It takes in-depth knowledge of networking protocols and technologies to build resilient and dependable computer networks, and these protocols and technologies must be implemented carefully for better results.

Objective and Scope of the Study: This study seeks to investigate the revolutionary artificial intelligence AI-driven computer network resilience and reliability optimization using multi-layered architecture, network protocols, and network components. It will look at the various AI techniques and technologies using multi-layered architecture, network protocols, and network components,that are generating significant gains in network performance, such as lower latency, more throughput, and greater reliability.

The study will also look into the advantages and disadvantages of implementing AI-driven optimization methodologies in modern networks. This research will provide a thorough knowledge of how network service providers may employ AI to promote innovation, increase operational efficiency, and deliver excellent user experiences in an ever-changing digital context.

Research questions:

1. Is there any correlation between the network layers and the network components?

2. Does layering of computer network components enables efficient communication and ensuring security and reliability?

3. How does layers communicate with each other in a network with OSI architecture?

By addressing these research questions, this study will add to the growing body of knowledge in AI-Driven computer network resilience and reliability optimization using multi-layered architecture, network protocols, and network components, allowing network service providers to make informed decisions and fully utilize the potential of AI-driven technologies using multi-layered architecture, network protocols, and network components to improve network operations and maintain a competitive edge in the dynamic network market.

3. THE TRANSITION TO AI-DRIVEN OPTIMIZATION

The limits of traditional network optimization approaches have made way for the widespread use of Artificial Intelligence (AI) in the network industry. This shift has been fueled by the awareness that AI-powered technologies may handle the inherent constraints of manual optimization while unlocking new levels of network efficiency, responsiveness, and intelligence.

AI-powered optimization procedures use complex algorithms, machine learning, and deep learning techniques to automate many parts of network management and optimization. AI-powered systems can recognize trends, forecast network activity, and make intelligent judgments by analyzing massive volumes of network data.

4. CURRENT TRENDS IN AI-POWERED NETWORKS

The integration of AI-powered technology into networks has accelerated in recent years, with an increased emphasis on automation and intelligent decision-making processes. Some of the current trends in AI-powered network optimization are:

1.Automated Network Management and Operations: AI-powered solutions are progressively taking over duties like network configuration, defect detection, and performance optimization, eliminating the need for manual intervention and human-centered decision-making.

2.Self-Organizing Networks (SON): AI-powered SON technologies allow networks to adapt to changing conditions, optimize resource allocation, and rearrange themselves to maintain peak performance without requiring human involvement.

3.Predictive Analysis and Decision Making: AI-powered predictive analytic and decision-making processes allow network operators to anticipate network difficulties, address possible problems proactively, and make more informed strategic decisions to improve network performance and operational efficiency.

These AI-powered trends are transforming the network industry, allowing network operators to achieve new levels of agility, responsiveness, and optimization in their network operations, resulting in better user experiences and a competitive advantage in the dynamic digital landscape.

5. AI TECHNOLOGIES USED FOR NETWORK OPTIMIZATION

The incorporation of Artificial Intelligence (AI) technology in the network industry has aided in the evolution of network optimization. AI-powered approaches, such as machine learning, deep learning, natural language processing, and reinforcement learning, have become critical components in the optimization of modern telecommunication networks. These AI technologies enable network operators to evaluate massive volumes of data, forecast network behavior, and make informed decisions that improve performance, reliability, and user experience.

5.1 Machine learning (ML)

Machine learning is an essential component of AI-powered network optimization. ML algorithms are used to evaluate network data, detect trends, and make predictions that can then be utilized to improve various aspects of network operations. This includes using supervised learning algorithms to forecast traffic patterns and resource utilization, unsupervised learning techniques to detect anomalies and identify network problems, and reinforcement learning approaches to dynamically optimize resource allocation and network configurations.

5.2 Deep learning (DL)

Deep learning, a more advanced branch of machine learning, has becoming widely used in network optimization. Deep neural networks can handle complex network data, extract relevant features, and make smart judgments to improve network performance. Fault identification, anomaly recognition, and predictive maintenance are examples of DL applications in network optimization, where deep learning models outperform standard rule-based systems at identifying and addressing issues.

5.3 Natural language processing (NLP)

Natural language processing (NLP) is essential for network optimization, notably in network diagnosis and customer service automation. NLP algorithms are used to scan network logs, incident reports, and customer interactions, allowing network operators to swiftly discover and address issues while also automating customer care processes.

5.4 Reinforcement learning (RL)

Reinforcement learning is a strong AI technique that has been used for a variety of network optimization challenges. RL algorithms learn by constantly interacting with the network environment, making decisions and getting feedback to improve network operations including traffic engineering, spectrum allocation, and dynamic resource management. RL's self-learning and adaptive nature make it an effective tool for optimizing complicated network processes.

5.5 AI-Powered Predictive Analytics

AI-driven predictive analytics is a critical component of network optimization in the telecommunications industry. Using machine learning and deep learning models, network operators may foresee network activity, identify possible congestion or performance deterioration, and address issues before they affect end users. This predictive feature offers a more proactive and efficient approach to network management,hence improving overall network performance and dependability.

5.6 AI for Edge Computing and 5G Networks

The integration of AI technologies at the network edge, combined with the deployment of 5G networks, has increased the potential of network optimization. Edge computing, which moves processing and decision-making closer to data sources, allows for real-time data processing and optimization, meeting the low-latency requirements of modern applications. AI-powered edge devices and 5G network architectures work together to meet the increased complexity and performance requirements of next-generation telecommunications networks.

Network providers can achieve unprecedented levels of network optimization by leveraging these diverse AI technologies, resulting in improved performance, reliability, and user experience while lowering operational costs and maintaining a competitive edge in the rapidly changing digital landscape.

6. ADVANTAGES OF AI IN NETWORK OPTIMIZATION

The incorporation of Artificial Intelligence (AI) into network optimization has resulted in numerous benefits, allowing service providers to improve network performance, operational efficiency, and deliver greater client experiences. Let's look at the main advantages of AI-driven network optimization:

6.1 Improved Network Performance

AI-powered network optimization strategies have shown considerable gains in overall network performance.Network companies can improve network performance, reduce latency, and increase data transmission rates by utilizing machine learning and deep learning techniques. This optimization directly translates into improved user experiences, including seamless connectivity and speedier data delivery across several applications and services.

6.2 Cost Efficiency

The use of AI in network optimization has had a significant influence on cost efficiency for Network companies. AI-driven automation and reduced reliance on manual intervention have resulted in significant savings in operating costs, such as labor, maintenance, and energy use. Furthermore, AI-powered optimization can assist providers in maximizing the utilization of their existing network infrastructure, reducing capital expenditures and deferring the need for costly network upgrades.

6.3 Scalability and Flexibility

AI-driven network optimization allows networks to scale quickly in response to rising traffic volumes and changing customer needs.AI-powered systems may dynamically assign network resources, update configurations, and rearrange network topologies in response to abrupt spikes in traffic or changes in usage patterns by employing predictive analytics and real-time decision-making capabilities. This versatility and flexibility ensures that networks can keep up with the ever-increasing demands of the digital environment.

6.4 Enhanced Customer Experience

The usefulness of artificial intelligence in network optimization goes beyond improving technical performance; it also improves the consumer experience dramatically. AI-powered systems can anticipate and respond to consumer demands, personalize services, and assure consistent network quality by evaluating user behavior, network data, and customer feedback. This proactive and tailored approach to network management results in greater customer happiness, loyalty, and perceived value for Network services.

6.5 Real-time Decision Making

One of the primary benefits of AI-driven network optimization is the capacity to make real-time decisions.AI algorithms can evaluate massive amounts of network data, find trends, and make intelligent judgments in near-real time, allowing networks to react quickly to changing conditions.This real-time decision-making power is critical for managing large traffic loads, reducing network congestion, and assuring network resilience and responsiveness.

Network service providers can achieve transformative benefits by leveraging AI, such as greater network performance, operational efficiency, scalability and flexibility, enhanced consumer experiences, and real-time decision-making capabilities.This convergence of AI and network optimization has the potential to transform the network business by fostering innovation, boosting consumer satisfaction, and maintaining a competitive advantage in the dynamic digital landscape.

7. CHALLENGES AND LIMITATIONS OF AI IN NETWORK OPTIMIZATION.

While the use of Artificial Intelligence (AI) in network optimization has produced significant benefits, network operators must overcome a number of problems and constraints to ensure successful implementation and long-term sustainability.

7.1 Data Quality and Availability.

One of the most significant obstacles in using AI for network optimization is ensuring the quality and availability of the necessary data. AI models use huge, high-quality datasets to understand patterns, generate accurate predictions, and drive optimization decisions. The gathering, storage, and administration of network data in the telecommunications business can be complex, with problems related to data integration, quality, and accessibility.

Addressing these data-related difficulties necessitates a comprehensive data management strategy that includes investments in advanced data infrastructure, data governance frameworks, and data preparation capabilities to assure data reliability and usability throughout AI model training and deployment.

7.2 Complexity of AI Integration

Integrating AI-driven optimization technologies into current network architecture can be a challenging and technical task. Telecommunications providers must overcome the obstacles of integrating AI technologies with legacy systems, enabling seamless data interchange, and retaining the overall scalability and modularity of the network architecture.

Furthermore, because network circumstances and user demands are always changing, AI models must be updated and retrained on a regular basis to ensure their relevance and efficacy. Network providers may have substantial challenges in maintaining and adapting AI systems on an ongoing basis.

7.3 Privacy and Security Concerns

The extensive use of AI in network optimization raises questions regarding data privacy and security. Networks carry massive volumes of user data, which, if not properly secured, can result in data breaches and privacy violations. To preserve the integrity of their AI-powered systems and the sensitive data on which they rely, network providers must employ robust security measures such as strong access limits, encryption, and anomaly detection.

7.4 Lack of AI expertise in telecommunications.

Implementing and administering AI-powered network optimization solutions necessitates specialist knowledge in fields such as machine learning, deep learning, and data science. However,the network industry has always battled a dearth of skilled individuals with AI and analytics capabilities.Bridging this skill gap requires recruiting, training, and coordination with external AI experts to ensure the effective deployment and continuous maintenance of AI systems within networks.

7.5 Regulatory and Ethical Considerations

The use of AI in network optimization also poses regulatory and ethical considerations that network carriers must overcome.Regulatory organizations may establish standards or restrictions surrounding the openness, explainability, and accountability of AI-driven decision-making processes, particularly in areas that may effect customer experiences or network stability.Furthermore, there are ethical concerns regarding the fairness, bias, and societal impact of AI algorithms in network management.

To guarantee that their AI-powered network optimization efforts comply with emerging regulatory frameworks and adhere to the highest ethical standards, network companies must engage with regulators, legislators, and ethical review boards on a proactive basis.

Addressing these issues and constraints necessitates a complete and strategic strategy from network providers, including investments in data infrastructure, talent development, rigorous security measures, and close coordination with regulatory authorities and AI experts.By overcoming these limitations,network operators will be able to fully realize AI's transformative potential for driving network efficiency and maintaining a competitive advantage in the dynamic digital landscape.

8. FUTURE DIRECTIONS AND EMERGING TRENDS

As the network sector evolves, Artificial Intelligence (AI) will play an increasingly important and transformational role in network optimization. Here are some of the most important future directions and developing trends in this domain:

8.1 AI-driven 6G networks

The development of 6G networks is projected to usher in a new era of AI-powered optimization, with AI playing an important role in the design, deployment, and management of these future networks. 6G networks will prioritize ultra-reliable, low-latency, and energy-efficient communications to meet the growing need for immersive apps, autonomous systems, and mission-critical services.

AI algorithms will be fully integrated into 6G network topologies, allowing for real-time decision making, dynamic resource allocation, and intelligent fault detection and mitigation. The use of AI in 6G networks will be important in managing the additional complexity, ultra-high bandwidth, and severe performance standards that these next-generation networks must meet.

8.2 AI at the edge.

The increasing importance of edge computing in networks will intensify the role of AI. Edge computing, by bringing AI-powered processing and decision-making capabilities closer to data sources, will enable real-time optimization and analytics, meeting the low-latency requirements of new applications and services.

AI-powered edge devices and micro-data centers will play an important role in managing the dynamic flow of data, improving resource use, and ensuring network performance and stability at the edge.The combination of AI and edge computing will be a major driver of innovation in the network industry, allowing service providers to provide more responsive and intelligent network services.

8.3 AI-enabled autonomous networks

The growth of fully autonomous networks, fueled by advances in AI, is a promising future trend. These AI-enabled autonomous networks will be able to configure, heal, and optimize themselves, minimizing the need for manual intervention and human knowledge in network management.

The combination of reinforcement learning, neural networks, and other advanced AI techniques will allow networks to constantly learn, adapt, and make intelligent decisions in order to maximize performance, maintain reliability, and improve user experiences.This change to autonomous network management may have substantial repercussions for the network workforce, necessitating a rethinking of jobs and the development of new skill sets.

8.4 Collaborative AI and Federated Learning

Emerging advances in collaborative AI and federated learning will have a significant impact on the future of network optimization. Network providers can use distributed learning models over a network of devices or network nodes to optimize various network functions while protecting data privacy and security.

Federated learning approaches, in which AI models are trained on distributed data sources without sharing raw data, would allow networks to reap the benefits of AI-driven optimization while protecting the privacy of customer information and network operational data.

8.5 AI for Green Networks

As the network sector prioritizes sustainability and environmental responsibility, AI will play an increasingly important role in optimizing energy use and driving green network operations.AI algorithms can be used to monitor energy usage patterns, identify areas for efficiency improvement, and dynamically manage power consumption across the network infrastructure.

Network providers can lower their environmental impact, operational expenses, and contribute to a more sustainable digital ecosystem by leveraging predictive analytics, load balancing, and AI-powered smart energy management approaches.

These future prospects and emerging trends in AI-driven network optimization show that this technology is still evolving and has the potential to alter the network industry.As service providers traverse the intricacies of 6G networks, edge computing, autonomous systems, and sustainability programs,the integration of advanced AI capabilities will become a critical enabler of innovation, efficiency, and competitive advantage in the coming years.

9. LAYERED ARCHITECTURE AND DESIGN FOR ROBUST NETWORK SYSTEMS

By segmenting network communication into separate layers, each with its own set of protocols and functions, network layered architecture makes it simpler to manage and troubleshoot complex networks. Communication can be divided into layers so that any modifications or problems can be restricted to a single layer and not affect the entire network. Another benefit of this strategy is that it promotes standardization, which facilitates interoperability between various systems. The layered architecture approach is the foundation of a number of well-known networking models, including the OSI model and the TCP/IP model. Computer networks can be optimized for increased resilience and reliability by using a layered architecture, putting into place strong network protocols, and choosing dependable network components. Better scalability, fault tolerance, and effective network management are all made possible by this method. While the layered architecture enables effective resource management and makes problem-solving simpler, the use of standardized protocols ensures interoperability and compatibility among network devices. By avoiding the possibility of device failure, reliable network components further boost the resilience and reliability of the network. In the end, this strategy enhances network performance and cuts down on downtime.

The components of a computer network are arranged into layers of abstraction in a layered architecture, a particular kind of computer network design. With this architecture, the layers above and below are kept separate from one another details while still interacting with each other. As a result, you have the freedom to quickly swap out and replace various system components without affecting others. Given that the functionality of the components is independent of one another, a layered architecture offers flexibility and resilience. It facilitates the maintenance of a distinct separation of responsibilities between shifts, making maintenance and problem-solving simpler. This architecture also makes it possible to create new components without affecting already existing ones. Hierarchical architectures are a popular option for setting up and running computer networks because of these benefits. You can start to understand how computer networks function and what technologies enable successful data transfers by becoming familiar with the fundamentals of their layered architecture. A complex process is broken down into various layers according to the network design philosophy known as layered architecture. It is possible to create a network that is better organized and easier to maintain by layering these processes. The separation of various network components is another feature of this architecture. This is an excellent method for network development teams to divide their work and assign tasks to various team members. A layered architecture is used to compartmentalize the components that go into making the finished product. This can include a user interface, business logic, and data access layers. Each layer has its purpose and is used to accomplish specific tasks. By isolating each layer from other layers, you can avoid complex interactions and dependencies between components. A layered architecture also supports the troubleshooting process. As long as each layer is implemented correctly, it's relatively easy to identify where a problem occurred in the network. Generally, when you find a problem in a layer, it's easy to identify and fix it because the problem is contained within the closed domain of the network process.

A layered architecture makes it easier to ensure that the network process succeeds. It is simpler to specify specifications, requirements, and goals when a complex process is broken down into layers. By enabling network engineers to follow more complicated configuration processes without running into unexpected issues, it also ensures that these objectives are achieved. The creation of the most effective and efficient network is made possible by network teams using a layered architecture to organize their work. This architecture make sure the finished product satisfies the team's objectives, follows the established plans, and solves issues. In the development of contemporary networks, layered architecture is a key idea. It is a technique for breaking the entire system down into layers, each of which offers a different set of services and communicates with the layers above and below. This promotes modularity, network stability, and increased scalability and flexibility. The physical layer, which connects the different nodes that make up the system, is the lowest layer and is responsible for transferring raw data. The data link layer, which is situated above that, manages data transfer between nodes and upholds communication integrity. The session layer, which is placed above that, synchronizes traffic between two endpoints and creates and maintains network connections between various applications. The presentation layer sits on top of that, transforming the data into a format appropriate for your application. The application layer is also in charge of creating the interface between users and the system. .

10. OPTIMIZING NETWORK RESILIENCE AND RELIABILITY.

A layered architecture that is implemented with suitable network protocols and network components can lead to the optimization of resilient and reliable computer networks. In order to increase flexibility, manageability, and scalability, layering makes it possible to distribute network functions among various modules. A variety of services and applications are supported by protocols, which ensure effective communication between network components. Choosing dependable and fault-tolerant network components also ensures high network availability, fault tolerance, and redundancy. All of these elements work together to create a strong and reliable network that can withstand a range of difficulties, including hardware failures, network congestion, and cyberattacks. Layered architecture, network protocols, and network components must be used in order to design resilient and reliable computer networks. Network protocols guarantee seamless communication, while the layered architecture ensures modular’s design. Firewalls, routers, and switches are examples of network devices that offer security and effective data transmission. Fewer service interruptions, less downtime, and improved network performance result from the optimization of these components. A well-designed network architecture and strong network protocols increase network resilience and reliability, supporting continuous service delivery.

The creation of multi-layered architectures that offer thorough defense against intricate network functions and malicious threats is a requirement for creating resilient, dependable, and secure computer networks. This type of architecture includes a variety of elements that can interact with one another at the same layer or at different layers, ranging from devices and protocols to applications and physical connections. In addition to removing network’s single points of failure, this enables organizations to reduce complexity, expense, and physical resource requirements. Businesses must first choose the right network protocols and technologies before designing a comprehensive network architecture. Ethernet, OSI, TCP/IP, broadcast networks, and link layer protocols are typical alternatives. The network protocol you select should be able to offer a secure, scalable, and redundant platform in order to make sure that your network is dependable and resistant to all malicious attacks. The next step is to choose the kinds of devices you'll need to build your network after deciding on your network protocol and technology. They must be able to communicate with the system using a standard network management protocol, including servers, routers, firewalls, and switches. Devices must also be able to communicate with one another in the language used by the chosen protocol. The physical connections between these devices must be designed after they have been configured. This covers both wired and wireless connections, including satellite, cable, and fiber optic connections.

Network operator should also select technologies that ensure connection performance and reliability. Installing and configuring the application on your device is the last step. This includes the operating system and programs used to access and manage your network. Additionally, businesses must guarantee that users can access their applications safely. Organizations can lessen the risk of malicious threats by implementing the necessary network protocols and technologies, choosing the right devices, creating secure physical connections between them, and installing and configuring the required applications. Organizations should make sure that their network architecture is properly designed and tested prior to deployment in order to quickly and easily create resilient and reliable computer networks that are protected.

11. SEVEN(7) LAYERS OF THE OPEN SYSTEMS INTERCONNECTION (OSI) MODEL.

The Open Systems Interconnection (OSI) model defines the seven levels that computer systems employ to interact across a network. The OSI model is divided into seven levels, each with a specialized responsibility, ranging from physical hardware connections to high-level application interactions. The International Organization for Standardization (ISO) developed this conceptual framework to explain how different devices and networks can communicate with one another. The OSI model divides network communication into seven layers, each with unique duties as follows:

Layer 7 - This layer, known as the application layer, is in charge of providing users a way to communicate with the network. In addition to HTTP, FTP, and SMTP, this layer also handles conversation protocols. These protocols enable data transfer between applications running on different parts of the network.

Layer 6 - The presentation layer is also referred to as the translation layer in Layer 6. This layer is where data is formatted for network transmission and extracted from the software program application utility software program application layer. Encryption and decryption of data (also known as encryption and decryption) are done at the presentation layer. Data that has been decrypted is referred to as plain text, and vice versa for data that has been encrypted. Key values are employed in both data encryption and decryption. Bits that need to be sent over the network are narrowed down by compression.

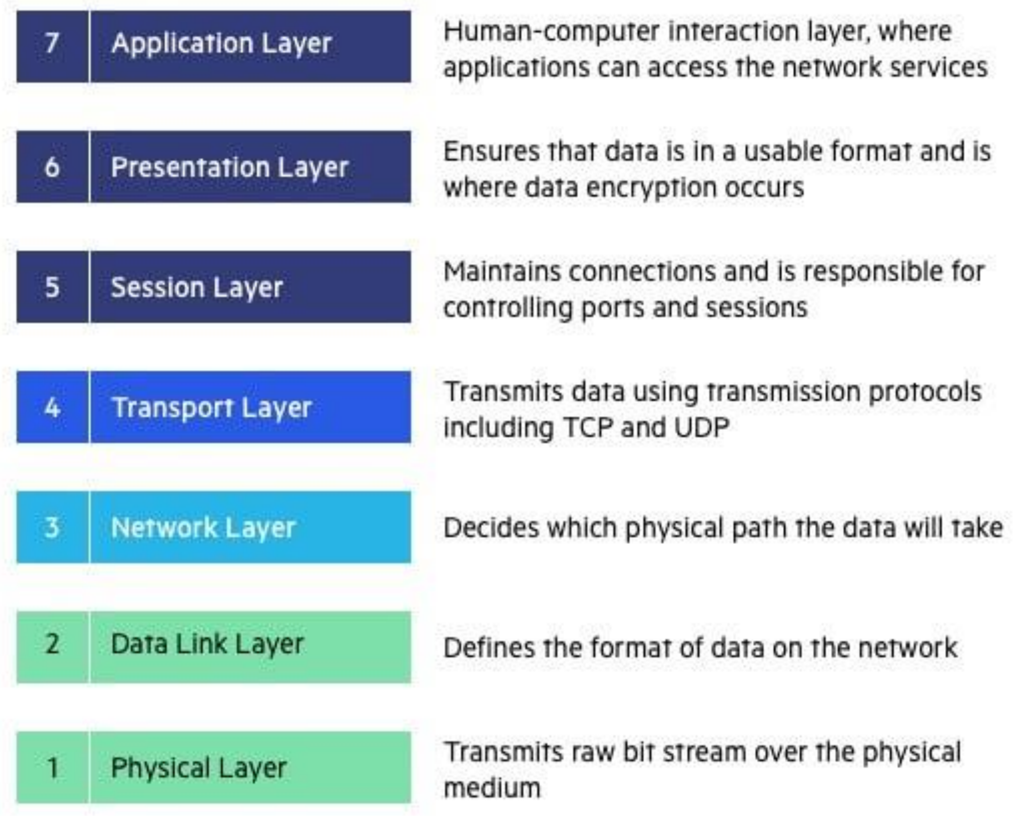
Layer 5 - The session layer, found in Layer 5, is used to create, manage, and end sessions. This layer makes it possible for two processes to connect and sync with one another. This layer allows the use of checkpoint methods to synchronization points. These synchronization points aid in locating errors. The data is correctly re-synchronized, the message does not end abruptly, and data loss is avoided as a result of doing this. Dialog Controller: The session layer enables the beginning of either half-duplex or full-duplex communication between two systems.

Layer 4 - Transport layer The transport layer is in charge of dependable communication and end-to-end delivery of frames to guarantee no data is lost. In order to prevent the receiving device from becoming overloaded, it also offers a flow control mechanism. manages two systems' end-to-end communication. The data integrity and flow control required for dependable communication are provided by them, and they connect and disassemble as needed. User Data Gram Protocol (UDP) and Transmission Control Protocol (TCP) are frequent protocols used at this layer.

Layer 3 - Network layer Layer 3 is in charge of managing network-level services, such as routing, addressing, and organizing incoming and outgoing data packets. From a range of options, it selects the shortest path to send packets. Network layer segments are known as packets. At this layer, IP, IPX, and OSGI are the most frequently used protocols.

Layer 2 - Data packets from the network layer are sent to the physical layer via Layer 2, the data link layer. Data from the physical layer is transferred to the data link layer, where frames are created by the addition of headers and trailers. After that, the network layer manages frame addressing and forwarding to the appropriate location. The data link layer has two sub-layers: (a) The LLC sub-layer manages network functions like error checking, flow control, and addressing. (b) The MAC sub-layer deals with hardware and protocol-related issues that arise when connecting devices to the network.

Layer 1 - The physical layer, or layer 1, manages the physical connection between two devices and offers the mechanical and electrical specifications required for communication. The actual network media and cabling that connects devices are included in the physical layer. Fiber optics, wireless antennas, and Ethernet cables.



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Fig. 1 OSI model

12. PERFORMANCE OPTIMIZATION OF NETWORKS COMPONENTS

Performance optimization of network components involves improving the efficiency of different elements in a network, such as routers, switches, and servers, to enhance overall network performance. This can be achieved by fine-tuning configurations, upgrading hardware components, and optimizing network protocols. By optimizing network components, organizations can improve network speed, reduce latency, and boost reliability. Regular monitoring and testing can help identify and address network performance issues before they become more significant problems. The performance optimization of network components is essential to ensure efficient and reliable communication. This process requires identifying the specific bottlenecks that are slowing down the network and taking steps to address them. Common strategies for optimization may include optimizing routing and switching protocols, upgrading hardware resources such as network cards and processors, and using traffic-shaping techniques to prioritize critical traffic. By optimizing network components, organizations can improve network speed, reduce downtime, and enhance overall user experience.

Various methods, such as load balancing, traffic shaping, packet filtering, and caching, can be used to improve the performance of network components. To avoid overloading on particular nodes, load balancing distributes network traffic across several servers or paths. Different types of network traffic are given different bandwidth allocations, which are prioritized and constrained by traffic shaping. Network congestion is decreased by packet filtering, which stops unwanted traffic. To improve network performance, these methods can be used on servers, routers, switches, firewalls, and other hardware and software components of networks. For businesses to guarantee quick and dependable network communication, performance optimization of network components is crucial. This can be accomplished by performing routine maintenance on the hardware, updating the software, and using network security protocols. Additionally, it is important to regularly check for proper operation and make any necessary upgrades on network components like servers, routers, and switches. Achieving better network performance can also be accomplished by implementing contemporary technology such as cloud computing and virtualization. To ensure the best performance of the network components, network administrators should regularly run performance tests to find any weak spots and take proactive steps to fix them.

13. ENABLING AND MANAGING END-TO-END RESILIENCE WITHIN THE NETWORK ARCHITECTURE

Enabling and managing end-to-end resilience within the network architecture involves implementing strategies and technologies that ensure network availability, reliability, and security. This includes redundancy, fail-over mechanisms, load balancing, and Disaster Recovery (DR) solutions. End-to-end resilience also requires proactive monitoring and analysis of network performance, identification and mitigation of vulnerabilities, and continuous improvement of network infrastructure. By implementing these measures, organizations can ensure that their network can withstand disruptions, maintain business continuity, and deliver seamless user experiences. End-to-end resilience within the network architecture is critical for ensuring uninterrupted business operations. Enabling this resilience requires a comprehensive approach that involves analyzing potential risks, designing resilient network topologies, implementing fault-tolerant technologies, and continuously testing and validating the network's ability to withstand disruptions. Effective resilience management also involves proactive monitoring, incident response planning, and disaster recovery preparation. By establishing end-to-end resilience as a core principle, organizations can mitigate the impact of disruptions and maintain a high level of availability and performance for their critical network services.

Ensuring that all network systems, including hardware and software, are built and configured to withstand failures and disruptions is a necessary step in implementing end-to-end resilience within the network architecture. This entails putting redundancy and fail-over mechanisms in place, performing routine testing and maintenance, keeping an eye on performance and security, and setting up backup plans and procedures. End-to-end resilience management requires a comprehensive strategy that involves cooperation among many stakeholders, including network engineers, IT staff, and business leaders, in order to ensure that all potential risk factors are identified and addressed. Security features in network architecture should also guard against online threats and assaults. To find and fix vulnerabilities and make sure that systems are operating as intended, managing resilience necessitates continuous testing and monitoring. Organizations can maintain business continuity and lessen the effects of disruptions by managing end-to-end resilience effectively.

14. NETWORK TOPOLOGY REQUIREMENT ANALYSIS

Network topology requirement analysis is an essential step in designing a network infrastructure. It involves analyzing the network requirements, such as bandwidth, security, scalability, cost, and redundancy, and determining the appropriate topology that meets those needs. The outstanding varieties of network topology encompass mesh, star, bus, ring, and hybrid. Factors such as distance, devices, and connectivity also play a vital role in selecting a network topology. The network topology requirement analysis ensures that the network is designed with an optimal configuration that delivers the best performance, reliability, and security.

Network topology requirement analysis is the process of identifying the specific needs and goals related to the design, implementation, and management of a network infrastructure. It involves assessing the business requirements, technological capabilities, bandwidth needs, and security concerns of the network. The outcome of this analysis is a clear understanding of the network topology that best fits the organization's needs. The topology may include physical or logical configurations of devices and connections, as well as protocols and operating systems that support the network. The topological design should be flexible, scalable, and adaptable to future changes in the organization.

When performing a network topology requirement analysis, it is important to identify the types of devices and their locations, the number of users, the types of services and applications required, security requirements, and redundancy needs. By looking at these factors, the most suitable topology can be determined to meet the organization's needs, whether it be a star, bus, ring, mesh, or hybrid topology. This analysis allows for efficient use of network resources, improved performance, and reduced downtime. It involves assessing the organization's needs and requirements, such as the number of users, devices, and locations. The analysis considers the strengths and weaknesses of different topologies, such as bus, ring, star, and mesh. The output is a recommendation of the most appropriate topology or combination of topologies for the organization's network infrastructure. This analysis also includes evaluating the cost, security, scalability, and reliability of the network topology.

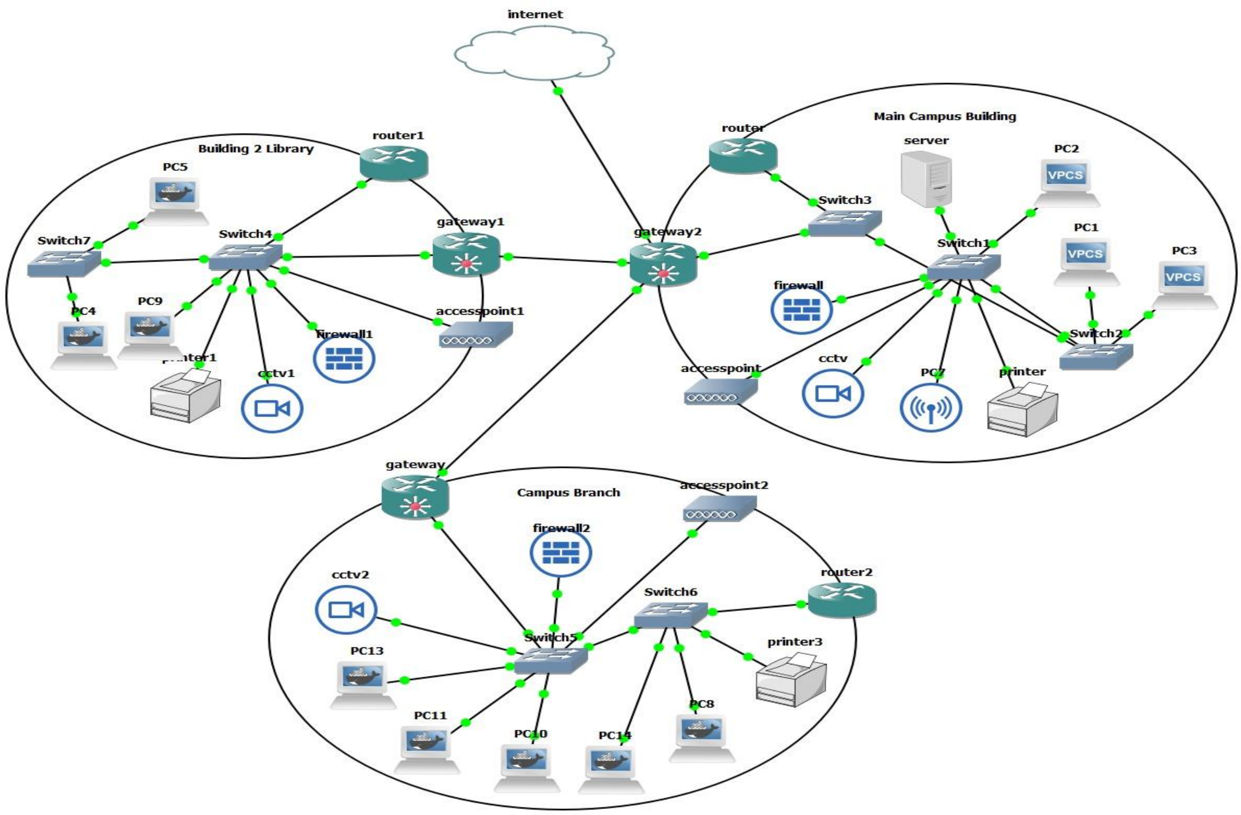


Fig. 2 Campus Area Network Layout

15. METHODS AND ANALYSIS

Methods employed in this study for network optimization include linear programming, queuing theory, simulation, and heuristic algorithms. The method and analysis of this study for network optimization involves identifying performance metrics, gathering data, developing models, and testing various configurations to identify the optimal solution. The method of this study for Network optimization involves the use of mathematical algorithms and models to improve the performance and efficiency of network systems. This can include optimizing routing, reducing congestion, minimizing latency, and maximizing throughput.

Ultimately, the goal of this study for network optimization is to improve the reliability and speed of network systems, leading to improved user experience and cost savings.

16. RESULTS AND FINDINGS

The findings of the study showed that there was a significant correlation between the network layers and the network components. The study also found that properly layering of computer network components enables efficient communication while ensuring security and reliability. These results suggest that in incorporating a network with the OSI architecture, each layer communicates only with the layer directly above or below, allowing hardware and software components to be optimized independently of each other also computer networks are designed in layers of components and topologies to provide efficient, secure, and reliable communication between two or more devices. Each layer of the architecture, from the physical layer to the application layer, performs specific tasks to ensure the successful and optimal delivery of data.

In this detailed examination of Artificial Intelligence (AI) in network optimization, I looked at the various applications, benefits, and issues that network providers face as they seek to harness the power of this technology. Throughout this examination, we have seen the extraordinary influence of AI-driven approaches like machine learning, deep learning, natural language processing, and reinforcement learning on optimizing many parts of networks. From automating network configuration and self-healing operations to improving traffic management and customer experience, AI has emerged as a crucial enabler of increased network performance, cost efficiency, scalability, and real-time decision-making. However, incorporating AI into network optimization presents certain obstacles. Network providers must solve data quality and availability difficulties, navigate the intricacies of AI integration, protect privacy and security, close the skills gap, and deal with legal and ethical concerns. To ensure the effective and long-term adoption of AI technologies, it is necessary to overcome these barriers in a systematic and comprehensive manner. As the network sector evolves, the role of AI in network optimization will become more important. The introduction of 6G networks, the growing importance of edge computing, and the push for autonomous network management will all rely significantly on AI's ability to manage complexity, improve performance, and drive innovation. Network operators must embrace emerging trends and strategically align their AI activities with long-term commercial goals. This could include investments in data infrastructure, talent development, collaborative collaborations, and the implementation of AI-powered solutions throughout the network's life-cycle.

17. DISCUSSION

The future of AI in the network business is undeniably promising. As service providers continue to investigate and embrace AI's disruptive potential, we may expect to see a seismic shift in how networks are planned, implemented, and operated. AI will not only improve the technical performance of telecommunications networks, but will also allow for more personalized, sustainable, and customer-centric services, bolstering the industry's position as a driving force in the digital age. The network industry's use of AI-driven network optimization will be critical to its capacity to stay ahead of the curve, provide excellent customer experiences, and maintain a competitive advantage in the quickly changing digital landscape. By carefully exploiting AI capabilities, telecommunications providers may open up new horizons of innovation, efficiency, and growth, influencing the industry's future for years.

18. CONCLUSION

The OSI model layer provides a standard framework for transferring data over various types of networks. Understanding the various layers and how they interact can help you use network services more effectively. The application layer provides an interface for independent applications to communicate. Below that is the presentation layer, which consolidates and formats data for transmission over the network. The session layer provides a means of initiating, maintaining, and terminating connections between applications and the network. The transport layer provides reliable but not guaranteed services for communication between hosts. Below that is the data link layer, which detects and corrects errors in data frames and manages the physical connection to the network. The physical layer is at the bottom and transfers raw data bits over physical media. It also defines the physical and electrical characteristics of the connection, such as data rate, modulation scheme, and cable type. Together, the seven layers of the OSI model define the structure of the protocol stack and enable networks to transmit data in packet form.

ACKNOWLEDGEMENTS

I acknowledge Malaysia University of Science and Technology, Malaysia.

REFERENCES

[1] Resilience and survivability in communication networks: Strategies, principles, and a survey of disciplines. https://www.sciencedirect.com/science/article/pii/S1389128610000824 Accessed 2023-04-09.

[2] [2] Architecture and design for resilient networked systems Hutchison, David ; Sterbenz, James P.G. Elsevier B.V Computer communications, 2018-10, Vol.131, p.13-21 Accessed 2023-04-09.

[3] [3] A unified architectural strategy for cyberattack-resistant industrial control systems. November 2020 Proceedings of the IEEE PP(99):1-25 DOI:10.1109/JPROC.2020.3034595 Accessed 2023-04-09.

[4] [4] A survey on https://onlinelibrary.com on software-defined networking (SDN). https://doi.org/10.1002/sec.Wiley.com 2023-04-09 accessed 1737.

[5] Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities. Accessed on 2023-04-09.

[6] https://www.researchgate.net/publication/261801398_Communication_network_requirements_for_major_smart_grid_ applications_in_HAN_NAN_and_WAN. Accessed 2023-04-09.

[7] [7] Invited paper on multilevel network resilience, survivability, and disruption tolerance. Accessed 2023-04-09. Available at: springer.com/article/10.1007/s11235-013-9816-9

[8] [8] A. T. Alashaikh. The spine concept for increasing network availability was developed by Gomes and D. Tipper.Comput.Elsevier, Networks, vol.82, no.5, may 2015, p.4-25.

[9] [9] M.J. F.Alenzi, E.K."etinkaya, J.".P.G.Improved centrality-balanced network design under cost constraints, Sterbenz IEEE/IFIP Rel. Net. Des. Model. (2014), pp. (RNDM'14), cv87szBarcelona, Spain.194-201.

[10] I. The author is B. Askoxylakis. L. Bencsáth. Buttyana, L. Dóra, V. SIRISS, A.Traganitis. resilience and cross-layer security in wireless mesh networks N. C. Zorba. (Skianis) C. Verikoukis (Editors. Cross Layer Designs in WLAN Systems, (2010) Emerging Communication and Service Technologies Series, Troubador Publishing Ltd.

[11] [11] A. AVIZIENS, J.-C.Lauree, B. Randall, C. Landwehr Basic ideas and taxonomy of dependable and secure computing Trans. dependable secure computing. , 1 (1) (2004), pp. 11-33.

[12] [12] J.S. Busby, D. Hutchison, and MdotF. The Rouncefield, H. Niedermayer as well as P. Smith, "Network of excellence in Internet science: Social aspects in understanding internet as critical infrastructure and implications for future networks (EINS Internet Science)", Lancaster University, Tech. Rep. [Online]. accessible at: http://www. internetscience.eu/sites/eins/files/biblio/EINS_JRA7_D7.2. 2

[13] E.K.Etinkaya, J.P.G.Sterbenz, "A Taxonomy of Network Challenges," 9th IEEE/IFIP Conference on Design of Reliable Communication Networks (DRCN), Budapest, April 2013, pp.322-330.

[14] E.K.Itinkaya, Moh. J.F.Alenzi, A.M. Peck, J.P.Röhrer, J.P.G. Sterbenz Multilevel Resilience Analysis of Transportation and Communications Networks Telecommun. Syst. , Springer, 60(4), December 2015, p. 515-537.

[15] Sridharan, Harish & Govindarajan, Sangeetha. (2019). Measuring Real Customer Experience Across and in Wireless Technologies. INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING & TECHNOLOGY. 10. 613-634.

[16] Sridharan, Harish & Govindarajan, Sangeetha. (2023). Sustainability in Telecom: Reducing the Environmental Impact of Networks. International Journal of Science and Research (IJSR). 12. 1352-1365. 10.21275/SR24913031348.

[17] Al Dallal, Haroon Rashid Hammood, and Ali Hadi Hasan Mohammed AlAbedi. "TELEHEALTH WIRELESS SYSTEMS: APPLICATIONS AND FUTURE PROSPECTS."

[18] Mohammed, Ali Hadi Hasan, and Haroon Rashid Hammood Al. "Arduino Smart Home Design."

[19] Al, Haroon Rashid Hammood, and Yasir Adil Mukhlif. "Infiltrations into Wireless Networks by Attackers."

[20] Dallal, Haroon Rashid Hammood. "Adaptive Arbitration Algorithms for Capacity in WCDMA (UMTS) Wireless Systems."

[21] Sharify, Thimar Falih Yasir, and Haroon Rashid Hammood Al Dallal. "The Evolution of Communication Engineering in Iraq." International Journal of Computational & Electronic Aspects in Engineering (IJCEAE) 3, no. 3 (2022).

[22] Dallal, Haroon Rashid Hammood, and Wijdan Noaman Marzoog Al Mukhtar. "A QR Code Used for Personal Information Based On Multi-Layer Encryption System." Int. J. Interact. Mob. Technol. 17, no. 9 (2023): 44-56.