A Novel Framework for Secure Broadband and MPLS Network Design in Critical Infrastructure Sectors

AFEES OLANREWAJU AKINADE[1], PETER ADEYEMO ADEPOJU[2], ADEBIMPE BOLATITO IGE[3], ADEOYE IDOWU AFOLABI[4]
[1]*Independent Researcher, USA*
[2]*Independent Researcher, United Kingdom*
[3]*Independent Researcher, Canada*
[4]*CISCO, Nigeria*

Abstract- ***In critical infrastructure sectors, secure and efficient network design is paramount to ensure operational resilience, safeguard sensitive data, and mitigate cyber threats. This paper proposes a novel framework for designing secure broadband and Multi-Protocol Label Switching (MPLS) networks tailored to the unique demands of critical infrastructure. The framework emphasizes a layered security approach, combining advanced encryption protocols, intelligent traffic segmentation, and adaptive routing mechanisms to enhance network robustness. Leveraging cutting-edge technologies such as software-defined networking (SDN) and artificial intelligence (AI), the framework offers real-time threat detection, anomaly detection, and dynamic response capabilities, thereby minimizing vulnerabilities. A key feature of the proposed design is its scalability and flexibility, which enables seamless integration with existing network infrastructures while accommodating future technological advancements. The use of SDN simplifies network management and allows for centralized control, ensuring optimal performance and rapid adaptability to changing network conditions. Furthermore, the integration of AI-driven analytics enhances situational awareness by providing predictive insights into network performance and security risks. The framework also addresses compliance with industry standards and regulations, ensuring alignment with best practices for cybersecurity and data protection in critical infrastructure sectors. A case study is presented to validate the framework's effectiveness in a real-world setting, focusing on its application in the energy sector to secure data exchanges between distributed control systems and remote monitoring units. Results indicate significant improvements in network reliability, reduced latency, and strengthened security postures. This research provides a comprehensive roadmap for deploying secure broadband and MPLS networks, catering to the needs of critical infrastructure operators. It contributes to the broader discourse on resilient network design, offering practical insights for stakeholders aiming to bolster the security and efficiency of their communication networks.***

Indexed Terms- ***Secure Broadband, MPLS, Critical Infrastructure, Network Design, Cybersecurity, Software-Defined Networking (SDN), Artificial Intelligence (AI), Threat Detection, Adaptive Routing, Compliance.***

I. INTRODUCTION

Critical infrastructure sectors, including energy, transportation, healthcare, and finance, form the backbone of modern society, supporting essential services and economic stability. These sectors increasingly depend on robust and secure communication networks to ensure reliable operations, protect sensitive data, and facilitate seamless coordination across distributed systems (Agupugo, 2023, Kaul, 2021). However, the growing reliance on interconnected digital systems has exposed critical infrastructure to an evolving array of cyber threats, heightening the need for resilient and secure network architectures.

Broadband and Multi-Protocol Label Switching (MPLS) networks play a pivotal role in the efficient functioning of critical infrastructure. Broadband

enables high-speed data transmission across extensive geographical areas, while MPLS provides scalable and efficient traffic management by creating virtual links between nodes. Together, these technologies form the foundation of modern communication systems, supporting real-time data exchange and enabling advanced monitoring and control capabilities essential for critical infrastructure operations (Avwioroko, 2023, Kalusivalingam, et al., 2021). Despite their benefits, ensuring the security of broadband and MPLS networks is a significant challenge, given the increasing sophistication of cyberattacks and the complexity of protecting distributed environments.

Securing network communications in critical infrastructure sectors presents several challenges. The rise of advanced persistent threats, ransomware, and distributed denial-of-service attacks demands innovative approaches to detect and mitigate vulnerabilities. Furthermore, ensuring data integrity and availability in environments with legacy systems, which often lack modern security features, complicates network security efforts (Agupugo & Tochukwu, 2021, Kaloudi & Li, 2020). The rapid pace of technological advancements, coupled with stringent regulatory requirements, adds to the complexity, necessitating a comprehensive framework that addresses these multifaceted challenges.

This paper introduces a novel framework for designing secure broadband and MPLS networks tailored to the specific needs of critical infrastructure sectors. By leveraging advanced technologies such as Software-Defined Networking (SDN) and Artificial Intelligence (AI), the proposed framework aims to enhance security, scalability, and resilience while ensuring compliance with industry standards. This approach offers a pathway to safeguarding essential services, mitigating risks, and promoting operational continuity in an era of increasing digital interdependence (Kaistinen, 2017, Qureshi, 2021).

2.1. Methodology

The methodology for developing a novel framework for secure broadband and MPLS network design in critical infrastructure sectors involves a comprehensive approach, combining theoretical research, system design, and empirical validation. The first phase of the methodology focuses on a thorough review of existing literature and industry best practices to identify the key security challenges and requirements for network communication in critical infrastructure sectors (Agupugo, 2023, Ighodaro & Ndem, 2023). This review includes analyzing the vulnerabilities inherent in broadband and MPLS networks, current security measures in place, and their limitations in protecting against advanced cyber threats.

Next, the proposed framework is designed with a focus on addressing the unique needs of critical infrastructure. The design incorporates key principles such as scalability, flexibility, and a layered security approach. The framework integrates advanced encryption protocols, intelligent traffic segmentation, adaptive routing, and network resilience strategies, with an emphasis on real-time monitoring and automated threat response. The role of emerging technologies like Software-Defined Networking (SDN) and Artificial Intelligence (AI) is explored, leveraging SDN for centralized control and AI for predictive threat detection and anomaly identification. This ensures that the network remains responsive to evolving security threats while maintaining high performance (Jiang, et al., 2021, Pölöskei & Bub, 2021).

Once the framework is conceptualized, a simulation-based approach is employed to model and test the network design. The simulation environment is set up to mimic the operational conditions of critical infrastructure sectors such as energy, healthcare, and transportation. This allows for testing the scalability, performance, and security capabilities of the framework under different threat scenarios (Jackson, 2019, Plugge & Janssen, 2014). The framework is also validated through a case study, focusing on the energy sector, to assess its practical implementation in securing data exchanges between distributed control systems and remote monitoring units. Key metrics such as network latency, data integrity, reliability, and the framework's ability to detect and mitigate security breaches are evaluated to ensure its effectiveness.

Finally, the results from the simulations and case study are analyzed to refine the framework, highlighting any potential weaknesses and proposing further improvements. The insights gained from these tests

contribute to the overall evaluation of the framework's suitability for deployment in real-world critical infrastructure environments. The methodology emphasizes an iterative design and validation process to ensure that the proposed framework addresses both current and future security challenges.

2.2. Background and Related Work

The evolution of broadband and Multi-Protocol Label Switching (MPLS) technologies has been critical to the development of modern communication networks. These technologies are foundational in ensuring the connectivity, efficiency, and performance of critical infrastructure sectors. Broadband technology allows for high-speed data transmission over long distances, providing the necessary bandwidth for data-heavy applications such as remote monitoring, control systems, and cloud computing. MPLS, on the other hand, offers a robust solution for managing traffic flow within large-scale networks by labeling data packets to optimize routing and reduce network congestion (Agupugo, et al., 2022, Islam, Babar & Nepal, 2019). Together, these technologies enable seamless communication across geographically dispersed systems, which is especially important in critical infrastructure sectors like energy, transportation, healthcare, and finance.

Broadband networks enable fast and efficient communication between critical infrastructure components such as power grids, transportation networks, and healthcare monitoring systems. These networks support high-volume data exchange, real-time monitoring, and control, making them essential for ensuring the smooth operation of critical services. However, the growing dependence on broadband for mission-critical operations also increases the exposure to cyber risks, highlighting the need for robust security measures (Bello, et al., 2023, Hughes, 2016). MPLS further enhances network performance by optimizing routing, enabling efficient resource usage, and providing better service quality (QoS) for critical applications. The combination of these technologies ensures high reliability, low latency, and secure data transport across complex infrastructure networks.

Despite their advantages, both broadband and MPLS networks face significant security challenges. Broadband networks, due to their open and shared nature, are vulnerable to a range of cyber threats, including unauthorized access, data interception, and distributed denial-of-service (DDoS) attacks. These networks are frequently targeted by cybercriminals aiming to exploit their vulnerabilities, especially as the number of connected devices and the volume of transmitted data continue to increase (Avwioroko, 2023, Holm, et al., 2017). The challenge is compounded by the rapid expansion of the Internet of Things (IoT) and the growing reliance on cloud-based services, which introduce additional attack vectors. The inherent openness of broadband networks also makes it difficult to implement strong access controls and encrypt sensitive data in transit. This increases the risk of data breaches, which can have severe consequences in critical infrastructure sectors, where confidentiality, integrity, and availability are paramount. Yahya, 2017 presented Multilayer Control in Software Defined networking (SDN) a shown in figure 1.

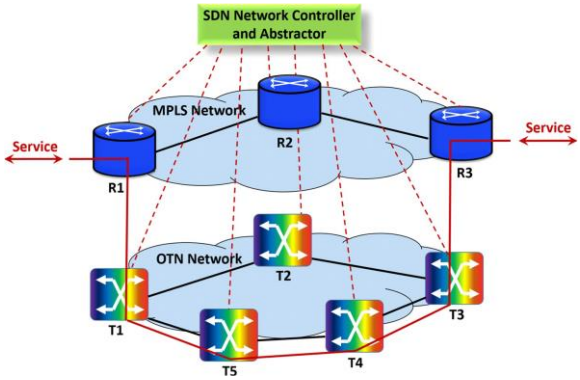

Figure 1: Multilayer Control in SDN (Yahya, 2017).

MPLS networks, while offering better traffic management and reliability, are also susceptible to several security threats. One of the key vulnerabilities lies in the label distribution protocol (LDP) used to assign labels to packets for routing. If attackers gain access to this protocol, they can reroute traffic, potentially causing service disruptions or enabling data interception. MPLS networks are also vulnerable to attacks such as man-in-the-middle (MITM), traffic sniffing, and label spoofing, which can compromise the integrity of data being transmitted (Elujide, et al., 2021, Hazra, et al., 2021). As the number of MPLS-enabled devices and networks increases, ensuring the secure management of labels and maintaining the integrity of routing paths becomes even more critical.

In the context of critical infrastructure, the security of MPLS networks is particularly important as a breach can lead to operational failures, data theft, or even large-scale disruptions to essential services.

The increasing complexity of broadband and MPLS networks in critical infrastructure sectors demands advanced security strategies that can address the vulnerabilities inherent in both technologies. A variety of approaches have been proposed to safeguard these networks from cyber threats. One widely adopted approach is the use of encryption to protect data in transit. End-to-end encryption ensures that even if data is intercepted during transmission, it remains unreadable to unauthorized parties (Gudala, et al., 2019). Virtual Private Networks (VPNs) and Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols are commonly used to secure broadband networks by creating encrypted tunnels for data transmission (Agupugo, et al., 2022). In MPLS networks, traffic encryption can be implemented using protocols such as IPsec, which secures the data at the IP layer. These encryption methods provide a level of protection, but they are not foolproof. Encryption alone cannot defend against attacks targeting the routing infrastructure or address the risks associated with poorly configured network elements.

Another approach to securing broadband and MPLS networks is the deployment of intrusion detection and prevention systems (IDPS). These systems monitor network traffic in real-time to identify and mitigate suspicious activities such as unauthorized access attempts or abnormal data flows. IDPS solutions can be integrated with existing network management tools to provide automated responses to detected threats, such as blocking malicious traffic or alerting administrators to potential breaches (Bello, et al., 2023, Ghobakhloo, 2020). However, IDPS solutions often face challenges in detecting sophisticated or zero-day attacks, making it necessary to combine them with other advanced security measures. For example, machine learning algorithms can be used to analyze network traffic patterns and identify anomalies that may indicate an attack. The integration of Artificial Intelligence (AI) in network security is a growing trend, as AI can improve the accuracy of threat detection and reduce response times.

Firewalls, which monitor incoming and outgoing traffic based on predefined security rules, also play a critical role in network security. In MPLS networks, firewalls are used to enforce access control policies and prevent unauthorized data flows between different network segments. For broadband networks, firewalls can be used to block malicious traffic, limit access to sensitive resources, and restrict the types of services accessible to external users (Ighodaro & Agbro, 2010, Ighodaro, Ochornma & Egware, 2020). However, firewalls alone are not sufficient to ensure comprehensive security, as they cannot protect against internal threats or complex attack strategies that bypass traditional defenses.

Despite the various security measures available, existing frameworks for securing broadband and MPLS networks in critical infrastructure sectors have several limitations. One significant limitation is their inability to provide end-to-end security across complex, distributed networks. Traditional security measures often focus on securing individual network segments or endpoints but fail to account for the interconnected nature of modern critical infrastructure (Elujide, et al., 2021, Ighodaro, 2010). As networks become more complex, with a mix of on-premises, cloud-based, and IoT systems, securing communication across all parts of the infrastructure becomes increasingly difficult. Moreover, traditional network security frameworks tend to be reactive rather than proactive, focusing on detecting and responding to threats after they have occurred, rather than preventing them in the first place.

Another limitation of existing security frameworks is their lack of scalability and flexibility. Many traditional network security approaches are designed for static, on-premises environments and struggle to accommodate the dynamic nature of modern, cloud-enabled infrastructures. As critical infrastructure sectors continue to evolve, with greater integration of emerging technologies like 5G, IoT, and AI, existing security models may not be equipped to handle the new challenges posed by these technologies. A more flexible and scalable approach is needed to ensure that network security can adapt to changing infrastructure needs and evolving threats (Gadde, 2021, Petrenko, Mashatan & Shirazi, 2019)..

Finally, compliance with regulatory standards is another challenge for securing broadband and MPLS networks. In critical infrastructure sectors, organizations must adhere to a range of industry-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in healthcare or the Federal Energy Regulatory Commission (FERC) standards in energy. These regulations often mandate specific security measures, such as data encryption and incident reporting, which can be difficult to implement and maintain across complex network environments (Bello, et al., 2023, Kwasi & Ighodaro, 2023). Ensuring compliance with these regulations while balancing the need for network performance and flexibility remains a significant challenge for many organizations in the critical infrastructure space.

In conclusion, while broadband and MPLS technologies offer significant advantages for the operation of critical infrastructure sectors, they also introduce a range of security challenges. The current approaches to securing these networks, though effective to some extent, face several limitations, including a lack of end-to-end security, scalability, and flexibility. There is a pressing need for innovative frameworks that can address these challenges and provide more robust, proactive, and adaptable security measures for broadband and MPLS networks in critical infrastructure sectors (Ighodaro & Egware, 2014, Onochie, 2019). The proposed framework aims to fill this gap, offering a novel solution that leverages emerging technologies like Software-Defined Networking (SDN) and Artificial Intelligence (AI) to enhance security, scalability, and resilience in complex network environments.

2.3. Proposed Framework

The increasing complexity and security challenges associated with broadband and MPLS networks in critical infrastructure sectors demand a novel approach to network design. The proposed framework addresses these needs by focusing on key design principles and integrating advanced technologies that enhance both the security and performance of these networks (Avwioroko, 2023, Nwulu, et al., 2023). The framework is intended to ensure that communication within critical infrastructure is resilient, scalable, and adaptable to evolving threats and operational demands. The overall goal is to create a network environment that not only ensures high performance but also maintains stringent security standards while adhering to industry regulations.

The framework is built on several core design principles that aim to provide a secure, scalable, and flexible network infrastructure. Scalability and flexibility are key to ensuring that the network can evolve with the changing needs of critical infrastructure sectors. As these sectors increasingly rely on dynamic, cloud-based systems and emerging technologies, it is essential that the network can scale to accommodate these new demands without compromising on performance or security (Avwioroko, 2023, Gadde, 2019). The proposed framework incorporates a modular design approach that allows for easy expansion, enabling the integration of additional network components, new technologies, and an increasing number of connected devices. This scalability ensures that as infrastructure grows, the network can seamlessly support additional traffic, users, and services without becoming a bottleneck or a point of vulnerability. Yahya, 2017 presented an MPLS Network as shown in figure 2.

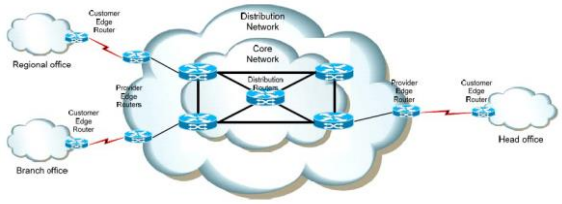

Figure 2: MPLS Network (Yahya, 2017).

Flexibility in the framework is crucial for accommodating different deployment scenarios and business needs. Critical infrastructure sectors often consist of diverse environments, ranging from legacy systems to modern, cloud-based solutions. The framework is designed to provide a flexible approach to network architecture that supports a wide range of deployment models, including hybrid, on-premises, and cloud-based networks. This flexibility ensures that organizations can tailor the network design to their specific needs while maintaining a high level of security (Furdek, et al., 2021, Peltonen, et al., 2020).

A layered security approach is another fundamental principle of the proposed framework. Security must be

integrated at every layer of the network, from the physical infrastructure to the application layer. This approach ensures that even if one layer is compromised, other layers will continue to provide protection. The framework includes strong encryption protocols, firewalls, intrusion detection systems, and access control mechanisms to create multiple layers of defense against cyber threats (Elete, et al., 2023, Ohile, et al., 2023). Additionally, by incorporating intelligent threat detection and analytics, the framework ensures that potential vulnerabilities are identified and mitigated in real time, preventing attacks before they can escalate.

Compliance with industry standards is also a cornerstone of the framework. Given the regulatory requirements for critical infrastructure sectors, including energy, healthcare, and finance, the framework ensures that security measures align with these standards. Adhering to these regulations not only helps organizations avoid penalties but also ensures that the network is equipped to protect sensitive data, maintain operational continuity, and prevent disruptions that could affect public safety and national security (Derhamy, 2016, Elujide, et al., 2021). The framework incorporates security measures that comply with industry-specific regulations such as the Federal Energy Regulatory Commission (FERC) guidelines for energy, the Health Insurance Portability and Accountability Act (HIPAA) for healthcare, and the Payment Card Industry Data Security Standard (PCI DSS) for financial services.

The key components of the proposed framework include encryption protocols, intelligent traffic segmentation, adaptive routing, Software-Defined Networking (SDN), and AI-driven threat detection and analytics. Encryption protocols form the foundation of secure data transmission across the network (Ighodaro & Osikhuemhe, 2019, Onochie, et al., 2017). By encrypting data at multiple points along its journey, the framework ensures that sensitive information is protected from interception or unauthorized access. The encryption protocols are designed to be scalable and adaptable, allowing for the integration of new encryption technologies as they emerge.

Intelligent traffic segmentation and adaptive routing are essential for optimizing the performance and security of the network. Traffic segmentation allows the network to create isolated channels for different types of data, reducing the risk of cross-contamination between critical services and less secure components. This segmentation also enables the implementation of differentiated security policies for different types of traffic, ensuring that more sensitive data is afforded higher levels of protection (Debbabi, Jmal & Chaari Fourati, 2021, Egware & Ighodaro, 2023). Adaptive routing ensures that network traffic is dynamically routed based on real-time conditions, such as network congestion or security threats. This ensures optimal performance and resilience, even in the face of changing network conditions or attacks.

The integration of Software-Defined Networking (SDN) enables centralized control and management of the network, which enhances both scalability and security. SDN allows network administrators to define and manage network policies and configurations from a central point, providing more granular control over network traffic (Parikh, 2019). This centralized management enables real-time adjustments to the network, which is particularly important in critical infrastructure environments that require constant monitoring and quick responses to potential threats (Bello, et al., 2023, Chirra, 2021). SDN also facilitates the integration of new technologies and services into the network, allowing for a more flexible and adaptable infrastructure.

AI-driven threat detection and analytics form an integral part of the security framework. By analyzing network traffic patterns, the system can identify anomalies that may indicate a potential security breach. Machine learning algorithms are employed to continuously refine the system's ability to detect threats and predict future attack vectors (Agupugo & Tochukwu, 2021, Ighodaro & Akhihiero, 2021). This proactive approach to threat detection ensures that the network is constantly evolving to defend against new and emerging cyber threats. In addition, AI can help automate responses to security incidents, reducing the time required to mitigate threats and preventing damage to the network.

The implementation architecture of the proposed framework is designed to optimize both performance and security while ensuring that the network can be

easily integrated into existing critical infrastructure environments. The network topology is flexible, allowing for the creation of both centralized and distributed network designs depending on the specific requirements of the infrastructure (Avwioroko, 2023, Nwulu, et al., 2023). In a centralized topology, control and management of the network are consolidated in one location, allowing for easier monitoring and maintenance. In a distributed topology, control is decentralized, allowing for better resilience and fault tolerance, as each segment of the network can operate independently if needed. The proposed framework supports both topologies, enabling organizations to choose the one that best meets their needs.

The communication protocols and interfaces within the framework are designed to ensure interoperability between different components of the network. These protocols support seamless communication between legacy systems and new, cloud-based technologies, facilitating the integration of diverse infrastructure components. The use of standard communication protocols, such as IPsec for secure tunneling and TLS for encrypted communication, ensures that the framework can integrate with existing network components while maintaining high security (Ighodaro & Scott, 2013, Onochie, 2020).

Finally, the framework incorporates both centralized and distributed control mechanisms. Centralized control enables easier policy enforcement and network configuration management, as all decisions are made from a central point. However, decentralized control mechanisms are also incorporated to ensure that network segments can continue to operate independently in the event of a failure or attack. This hybrid approach allows the framework to combine the benefits of both centralized and distributed control, providing a more resilient and adaptable network design (Boda & Immaneni, 2019, Noura, Atiquzzaman & Gaedke, 2019).

In conclusion, the proposed framework for secure broadband and MPLS network design in critical infrastructure sectors is built on a set of core principles and key components designed to address the unique security challenges faced by these sectors. By incorporating advanced technologies such as SDN, AI-driven threat detection, and intelligent traffic management, the framework provides a scalable, flexible, and resilient solution for securing communication networks in critical infrastructure (Nimmagadda, 2021). The architecture is designed to be adaptable to a wide range of deployment scenarios, ensuring that the framework can meet the evolving needs of organizations in diverse sectors while maintaining high levels of security and compliance with industry regulations.

2.4. Validation and Case Study

The validation of the proposed framework for secure broadband and MPLS network design in critical infrastructure sectors is essential to assess its effectiveness, performance, and adaptability in real-world applications. The validation process includes testing the framework's components under various conditions to ensure it meets the security, scalability, and reliability requirements specific to critical infrastructure environments (Bello, et al., 2022). Additionally, a case study in the energy sector provides a tangible application of the framework, demonstrating its ability to secure communication systems while enhancing overall network performance.

The methodology for validating the proposed framework involves a combination of simulation, testing, and real-world deployment. The initial validation process begins with a series of simulations designed to test the framework’s scalability, flexibility, and security under a variety of traffic loads and network configurations. These simulations evaluate how well the framework can handle the volume of traffic typically seen in critical infrastructure sectors, as well as its ability to mitigate various types of cyber threats (Ighodaro & Essien, 2020, Onochie & Ighodaro, 2017). This testing environment provides an opportunity to measure performance metrics such as network throughput, latency, and security incident response times. It also ensures that the system can handle increasing network demands without compromising security or performance.

Following the simulation phase, the framework is then tested in a controlled environment within a real-world critical infrastructure setting. The case study focuses on the energy sector, a critical infrastructure domain

that heavily relies on secure and reliable network communications for operations such as power generation, distribution, and remote monitoring (Muhammad, 2021). In this sector, ensuring the confidentiality, integrity, and availability of communication systems is vital, as any compromise could lead to widespread operational disruptions, financial losses, or even endanger public safety.

One of the critical areas of focus for this case study is securing data exchanges within distributed control systems (DCS). DCS are used to monitor and control industrial processes across remote locations and are vital to ensuring the smooth operation of power plants and substations. These systems require constant data exchange between sensors, controllers, and monitoring units to maintain process stability and respond to changing operational conditions. Given the potential vulnerabilities in these systems, especially with the increasing connectivity to broader networks, securing these exchanges becomes paramount (Bello, et al., 2023, Kwasi-Effah, et al., 2023). The proposed framework employs strong encryption protocols, access control mechanisms, and real-time intrusion detection systems to protect data in transit across the network. This ensures that the data exchanged between devices in the DCS remains confidential and tamper-proof, even when transmitted over potentially unsecured communication channels.

Another area where the framework is applied in the energy sector is enhancing the reliability of remote monitoring units. These units, deployed at critical infrastructure sites such as remote power plants or substations, play a crucial role in ensuring that real-time data is collected and transmitted back to central monitoring stations. These units often operate in environments with limited resources, such as power supply and bandwidth, making it difficult to ensure a reliable communication link (Ighodaro, 2016, Ighodaro, Scott & Xing, 2017). The proposed framework addresses these challenges by integrating intelligent traffic segmentation, adaptive routing, and AI-driven analytics to optimize the communication channels and ensure that critical data is delivered reliably, even under challenging network conditions. This also enables the energy company to conduct predictive maintenance, by analyzing data patterns to detect potential failures before they occur, improving operational efficiency and preventing costly downtimes.

The validation of the proposed framework in this case study reveals several key findings. One of the most significant findings is the framework's ability to provide secure and efficient communication in a dynamic and resource-constrained environment. The integration of intelligent traffic segmentation and adaptive routing ensures that traffic is optimized, reducing congestion and improving overall network performance. This feature proves particularly beneficial in the energy sector, where remote monitoring units may experience fluctuating network conditions due to bandwidth limitations or temporary outages (Egware, Ighodaro & Unuareokpa, 2016, Ighodaro, Okogie & Ozakpolor, 2010). The framework's dynamic routing capabilities ensure that traffic is rerouted in real-time to ensure uninterrupted communication, which is crucial for maintaining operational continuity and safety.

Another critical finding is the effectiveness of the layered security approach in safeguarding data exchanges. The encryption protocols, intrusion detection systems, and access control mechanisms provide multiple layers of defense against cyber threats, reducing the likelihood of data breaches or unauthorized access to sensitive information. In the energy sector, where operational data is highly sensitive and must be protected from tampering, this multi-layered approach significantly enhances the overall security posture of the network (Elete, et al., 2023, Kwasi & Ighodaro, 2023). The inclusion of AI-driven analytics further strengthens security by providing proactive threat detection, identifying anomalies in network traffic that could signal a potential breach. This enables security teams to take swift action to mitigate threats before they escalate into more significant incidents.

In terms of performance, the framework demonstrates its scalability and flexibility. The ability to adapt to varying traffic loads and network configurations ensures that the framework can meet the growing demands of critical infrastructure sectors. In the energy sector case study, the framework was able to scale seamlessly to accommodate additional remote monitoring units and increased data traffic, without

compromising on performance or security (Muhammad, 2019). This scalability is essential for supporting the expanding network requirements of modern energy grids, particularly as smart grid technologies and IoT devices become more widespread.

Furthermore, the case study demonstrates the framework's compliance with industry standards and regulations. The energy sector is subject to stringent security and operational regulations, and the framework's design ensures that it meets these requirements. By adhering to industry-specific standards such as the NIST Cybersecurity Framework and the IEC 61850 standard for communication in power systems, the framework ensures that energy companies can maintain compliance while simultaneously enhancing their security posture (Osarobo & Chika, 2016). This compliance is critical not only for avoiding regulatory penalties but also for building trust with stakeholders, including customers, regulators, and investors.

Performance metrics collected during the case study include network throughput, latency, data integrity, and security incident response times. These metrics provide a comprehensive picture of the framework's effectiveness in delivering secure and efficient communication. The results indicate that the framework delivers high throughput and low latency, even under heavy traffic conditions, ensuring that critical data is delivered in real-time (Onyiriuka, et al., 2019, Orumwense, Ighodaro & Abo-Al-Ez, 2021). The framework's encryption and security measures have a minimal impact on performance, ensuring that the network can maintain its operational efficiency without sacrificing security. Security incident response times were also improved with the integration of AI-driven analytics, which enabled the system to detect and mitigate threats more quickly than traditional security measures.

In conclusion, the validation and case study of the proposed framework for secure broadband and MPLS network design in the energy sector demonstrate its effectiveness in addressing the unique security challenges faced by critical infrastructure sectors. The integration of advanced technologies such as intelligent traffic segmentation, adaptive routing, and AI-driven threat detection ensures that the framework provides a secure, scalable, and resilient network solution (Ighodaro & Scott, 2017, Onochie, et al., 2017). By applying the framework to the energy sector, the case study illustrates its potential to enhance data security, network performance, and operational reliability in critical infrastructure settings. The findings underscore the framework's ability to meet the evolving demands of modern infrastructure, providing a robust foundation for securing communication systems in high-risk sectors.

2.5. Benefits and Advantages of the Framework

The benefits and advantages of the proposed framework for secure broadband and MPLS network design in critical infrastructure sectors are numerous, addressing both immediate security needs and long-term operational goals. These benefits are realized across various dimensions, including enhanced security and threat mitigation, improved network performance and reliability, scalability for future technological advancements, and ensuring regulatory compliance (Elujide, et al., 2021, Ighodaro & Aburime, 2011). The framework leverages advanced technologies and best practices to provide a robust, secure, and flexible solution for the unique challenges faced by critical infrastructure sectors, such as energy, transportation, and telecommunications.

A key benefit of the proposed framework is its enhanced security and threat mitigation capabilities. Critical infrastructure sectors, due to their vital role in public safety and economic stability, are frequent targets of cyberattacks. These attacks can range from data breaches and denial-of-service incidents to more sophisticated and damaging intrusions designed to compromise or disrupt operations. The framework employs a multi-layered security approach that integrates advanced encryption protocols, intrusion detection systems, access control measures, and AI-driven threat detection to safeguard sensitive data and critical systems from a variety of cyber threats (Asibor & Ighodaro, 2019, Ighodaro, Olaosebikan & Egware, 2020). By implementing these security features, the framework significantly reduces the risk of unauthorized access, tampering, and data breaches. The encryption protocols ensure that data in transit is protected, while intrusion detection systems continuously monitor network traffic for abnormal

patterns that could indicate potential threats. Furthermore, AI-driven threat detection improves the framework's ability to identify and respond to new and evolving cyber threats, offering proactive protection rather than relying solely on reactive measures. This combination of advanced security technologies ensures that the network remains secure, even as new vulnerabilities and attack vectors emerge, providing a high level of resilience against cyber threats.

In addition to enhanced security, the framework offers improved network performance and reliability. Critical infrastructure sectors rely on their networks to maintain real-time communication between various components, such as control systems, monitoring units, and remote sensors. Network downtime or slow performance can have significant consequences, including disruptions to service, financial losses, and safety hazards. The framework addresses these concerns by incorporating intelligent traffic segmentation and adaptive routing. These technologies optimize network traffic, reducing congestion and ensuring that critical data is transmitted efficiently (Bello, et al., 2023, Nwulu, et al., 2023). Intelligent traffic segmentation enables the framework to categorize different types of data based on their priority, ensuring that high-priority traffic, such as safety-critical messages, is given precedence over less critical data. Adaptive routing, on the other hand, adjusts the path of data in real-time based on network conditions, ensuring that traffic can be rerouted to avoid congestion or failures in certain parts of the network. This dynamic routing capability enhances the network's resilience and minimizes the likelihood of service interruptions. Furthermore, the integration of Software-Defined Networking (SDN) enables centralized control of the network, providing better visibility into network performance and allowing for more efficient management and troubleshooting. As a result, the framework improves overall network reliability, ensuring that critical infrastructure systems remain operational even in the face of network challenges or failures. A Global MPLS IP VPN Services market by service (USD Million) as presented by Mustapha, 2019 is shown in figure 3.

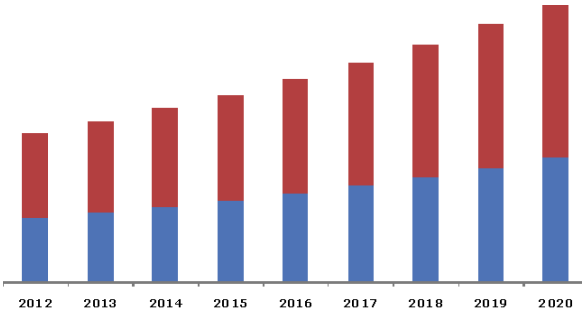

Figure 3: Global MPLS IP VPN Services market by service (USD Million) (Mustapha, 2019).

Another significant advantage of the proposed framework is its scalability, which is essential for accommodating future technological advancements. The needs of critical infrastructure sectors are constantly evolving, with new technologies being deployed to improve efficiency, expand capacity, and enhance functionality. For example, the growing use of Internet of Things (IoT) devices and smart grid technologies in the energy sector requires networks that can handle increased traffic, support new devices, and integrate with emerging technologies. The framework's scalability ensures that it can adapt to these changes without requiring a complete overhaul of the network (Kwasi-Effah, et al., 2022, Onyeke, et al., 2022). Its modular design allows new components and features to be added as needed, ensuring that the network can accommodate future growth and technological innovations. The framework's ability to scale also ensures that it can support the increasing demands of data processing, storage, and transmission as the volume of data generated by critical infrastructure systems grows. Additionally, the integration of SDN and AI-driven analytics enhances scalability by enabling more flexible and efficient network management (Min-Jun & Ji-Eun, 2020). These technologies allow the network to be dynamically reconfigured to meet changing requirements, such as adjusting to fluctuating traffic loads or incorporating new technologies, without disrupting service.

The framework also offers significant advantages in terms of regulatory compliance and alignment with industry best practices. Critical infrastructure sectors are subject to strict regulations and standards designed to ensure the safety, security, and reliability of their

operations. These regulations may vary depending on the sector, but they all require that network systems adhere to high standards of security, data protection, and operational continuity (Ighodaro & Osikhuemhe, 2019, Onochie, et al., 2017). The proposed framework is designed to meet these regulatory requirements by incorporating industry standards such as the NIST Cybersecurity Framework, IEC 61850 for power systems, and other relevant compliance frameworks. By aligning the design with these standards, the framework helps organizations in critical infrastructure sectors avoid potential legal and financial penalties associated with non-compliance. Additionally, the framework's adherence to best practices in cybersecurity, network design, and system integration ensures that organizations can maintain their reputation and trust with stakeholders, including customers, investors, and regulatory bodies. Compliance with these standards not only helps organizations meet legal requirements but also demonstrates a commitment to maintaining the highest levels of security and operational excellence, which can enhance stakeholder confidence and support the long-term success of the organization.

One of the most compelling aspects of the framework is its ability to provide a secure, efficient, and scalable solution that addresses the unique needs of critical infrastructure sectors. In sectors such as energy, transportation, and telecommunications, where the stakes are high and the consequences of network failure can be severe, the framework offers a robust solution that helps mitigate risks, enhance performance, and ensure compliance (Egware, et al., 2021, Ighodaro & Egbon, 2021). The combination of advanced security features, such as encryption and AI-driven threat detection, with intelligent network optimization technologies, such as traffic segmentation and adaptive routing, ensures that critical systems remain secure and operational under a wide range of conditions. Furthermore, the framework's scalability and flexibility enable it to accommodate future technological advancements, ensuring that organizations can continue to meet the evolving demands of their industries.

The framework also helps to future-proof critical infrastructure networks, ensuring that they can adapt to emerging trends, such as the increasing integration of IoT devices, the expansion of smart grid technologies, and the growing reliance on AI and machine learning for operational optimization. By providing a secure and reliable foundation for these technologies, the framework enables organizations to leverage these innovations without compromising security or network performance. As a result, the framework not only addresses current security and performance challenges but also positions organizations in critical infrastructure sectors for success in the future (Avwioroko, 2023, Onyeke, et al., 2023).

In conclusion, the proposed framework offers a comprehensive solution for secure broadband and MPLS network design in critical infrastructure sectors. Its benefits span across multiple dimensions, including enhanced security, improved network performance, scalability, and regulatory compliance (Mazurek & Małagocka, 2019). These advantages make the framework an essential tool for organizations seeking to strengthen their network infrastructures while adapting to the rapidly changing technological landscape. Through its advanced features and adherence to industry standards, the framework provides a robust, flexible, and future-proof solution for securing the networks that underpin critical infrastructure systems.

2.6. Challenges and Future Directions

The challenges and future directions of the proposed framework for secure broadband and MPLS network design in critical infrastructure sectors are multifaceted, reflecting both the complexities of the current technological landscape and the evolving nature of cyber threats. While the framework offers a comprehensive approach to securing critical infrastructure networks, its implementation and long-term success face several hurdles that must be addressed (Ighodaro & Egwaoje, 2020, Onochie, Obanor & Ighodaro, 2017). Additionally, as the cybersecurity and technology landscapes continue to evolve, the framework must remain adaptable to emerging threats and technological advancements, ensuring that critical infrastructure systems are resilient, secure, and capable of handling future challenges.

One of the primary challenges in implementing the proposed framework is the complexity involved in integrating new security measures with existing legacy systems in critical infrastructure sectors. Many critical infrastructure systems, particularly in sectors such as energy and telecommunications, are built upon long-established technologies that may not be fully compatible with modern security protocols or network design principles. Upgrading or replacing these legacy systems can be costly, time-consuming, and disruptive to ongoing operations (Elete, et al., 2023, Nwulu, et al., 2023). Furthermore, organizations may face resistance from stakeholders who are concerned about the potential risks associated with transitioning to new systems, particularly when it comes to network downtime or the complexity of training personnel to operate new technologies. Overcoming these challenges requires careful planning, coordination, and investment in both technical and human resources to ensure a smooth transition while minimizing disruptions to critical services. Additionally, the need for backward compatibility with older systems could necessitate the development of hybrid solutions that bridge the gap between existing infrastructure and the new security framework, further adding to the complexity.

Another significant challenge is the continuous evolution of cyber threats, which requires that the framework remain adaptable and capable of responding to new attack vectors. While the proposed framework incorporates advanced security measures such as encryption, AI-driven threat detection, and adaptive routing, the rapidly changing nature of cyber threats means that these measures may become outdated or ineffective over time (Martinez, et al., 2014). Cybercriminals and nation-state actors are constantly developing more sophisticated attack techniques, including advanced persistent threats (APTs) that target critical infrastructure sectors with high levels of precision and stealth. For example, emerging threats like ransomware attacks, supply chain vulnerabilities, and attacks on industrial control systems pose unique challenges for securing critical infrastructure networks (Ibrahim, et al., 2023, Kwasi-Effah, et al., 2023). To address these threats, the framework must be regularly updated and enhanced, with continuous monitoring and the integration of new security tools to detect and respond to evolving attack techniques. Organizations must also invest in ongoing training and awareness programs to ensure that their personnel are prepared to recognize and respond to new types of cyber threats effectively. The ability to rapidly adapt to new threats is critical for ensuring that the security measures in place remain effective in the long term, and that organizations can continue to safeguard their networks against emerging risks.

In addition to the challenges of adapting to evolving threats, there are opportunities for integrating new and emerging technologies into the framework that could further enhance its effectiveness and future-proof critical infrastructure networks. One such technology is quantum computing, which has the potential to revolutionize both network security and the way data is transmitted and processed (Egware, Onochie & Ighodaro, 2016, Ighodaro & Aregbe, 2017). Quantum computing could significantly enhance encryption methods, offering much stronger protection against cyber threats by utilizing quantum encryption techniques that are virtually impossible to break using traditional computing methods. For example, quantum key distribution (QKD) could be used to generate and share encryption keys in a manner that guarantees their security, even in the face of potential future attacks. However, the integration of quantum computing into the framework poses several challenges, including the need for specialized hardware, the lack of quantum-safe encryption standards, and the potential for disrupting existing encryption protocols (Marda, 2018). As quantum computing technology matures, the framework must be updated to incorporate quantum-resistant encryption methods and other related innovations to ensure that critical infrastructure networks remain secure in the face of this disruptive technology.

Another promising technology is the increasing use of artificial intelligence (AI) and machine learning (ML) to enhance network security and operational efficiency. AI-driven analytics and automated threat detection can provide real-time insights into network activity, helping to identify anomalies and potential security breaches before they cause significant damage. By leveraging AI, the framework can be enhanced to detect and respond to threats more quickly, improving overall network resilience (Ighodaro & Saale, 2017, Onochie, et al., 2018).

Furthermore, AI-powered systems can automate routine tasks such as traffic optimization, fault detection, and maintenance, reducing the workload on human operators and allowing them to focus on more complex and critical tasks. The integration of AI into the framework also offers opportunities for continuous improvement, as machine learning models can be trained on vast amounts of data to identify patterns and predict potential vulnerabilities in the network. As AI and ML technologies continue to evolve, their integration into the framework will help to keep it responsive to emerging threats and operational challenges, enabling critical infrastructure networks to adapt and improve over time.

The potential for integrating blockchain technology into the framework is another area of interest. Blockchain's decentralized and immutable nature could offer enhanced security for critical infrastructure networks, particularly in sectors where data integrity and traceability are paramount. By using blockchain to log network activities, transactions, and changes in configuration, organizations can ensure that all actions are securely recorded and cannot be altered or tampered with, creating a permanent and auditable record (Lees, 2019). This could be particularly useful in industries like energy and transportation, where regulatory compliance and data integrity are critical. Blockchain could also be used to facilitate secure and transparent supply chain management, helping to ensure that only authorized devices and software are deployed within the network. While blockchain technology offers significant potential, its integration into the framework would require careful consideration of scalability, energy consumption, and compatibility with existing network architectures. Furthermore, it would necessitate the development of new standards and protocols to ensure seamless integration and operation.

As these technologies evolve, they will likely offer new opportunities to enhance the security and performance of the framework. However, integrating these cutting-edge technologies into existing infrastructures will require significant effort and investment, as well as careful coordination to avoid introducing new vulnerabilities or disruptions. Moreover, the framework will need to be flexible enough to accommodate future technological innovations that have not yet been fully developed or implemented (Kijewski, 2015).

Another important consideration for the future of the framework is the increasing interconnectivity of critical infrastructure sectors. As networks become more integrated and reliant on cross-sector communication and data exchange, the potential attack surface for cyber threats grows. The convergence of technologies such as IoT, smart grids, and autonomous systems in critical infrastructure creates new challenges in ensuring that all components are securely connected and can operate seamlessly together (Koufos, et al., 2021). As the framework is further developed, it will need to account for the complexities of multi-sector interconnectivity, ensuring that the security and performance of each individual sector are not compromised by vulnerabilities in another sector.

In conclusion, while the proposed framework offers a robust solution for secure broadband and MPLS network design in critical infrastructure sectors, its implementation and long-term success face several challenges. The continuous evolution of cyber threats, the need to integrate new technologies, and the complexities of securing interconnected systems all pose significant hurdles (Khurana, 2020). However, these challenges also present opportunities for innovation and improvement. By incorporating emerging technologies like quantum computing, AI, and blockchain, and by ensuring that the framework remains adaptable to evolving security threats and industry requirements, the proposed framework has the potential to provide a future-proof solution for securing critical infrastructure networks. The ongoing development and refinement of the framework will be essential in addressing these challenges and ensuring that critical infrastructure sectors remain secure, resilient, and capable of meeting the demands of the future.

2.7. Conclusion

In conclusion, the proposed framework for secure broadband and MPLS network design in critical infrastructure sectors offers a comprehensive and forward-thinking approach to addressing the unique challenges of securing these vital networks. By integrating a combination of advanced security

protocols, intelligent traffic management, and adaptive technologies such as AI-driven threat detection and software-defined networking (SDN), the framework ensures that the network remains resilient in the face of growing cyber threats. The incorporation of these technologies provides not only enhanced security but also improved operational efficiency, allowing critical infrastructure systems to better withstand disruptions and optimize performance.

The contributions of this framework are significant, as it provides a holistic, scalable, and flexible approach to network design that can be tailored to the specific needs of various critical infrastructure sectors, including energy, telecommunications, and transportation. It advances the state of network security by addressing the complexities of securing both existing legacy systems and emerging technologies, ensuring that critical infrastructure remains protected against both current and future threats. Through its layered security measures, the framework improves the ability of organizations to mitigate potential cyberattacks, safeguard sensitive data, and maintain service continuity.

Moreover, the framework serves as a valuable guide for both practitioners and policymakers. For practitioners, it offers a roadmap for building secure, reliable, and high-performance networks that can adapt to evolving challenges. It emphasizes the importance of adopting a proactive security stance, where threats are anticipated and mitigated before they can cause harm. Policymakers can benefit from the framework by recognizing the need for consistent, industry-wide standards for network security and for supporting initiatives that facilitate the secure integration of new technologies. Collaboration between government bodies, industry leaders, and cybersecurity experts will be crucial to ensuring the framework's successful adoption and to addressing the rapidly changing landscape of cyber threats.

As critical infrastructure sectors continue to evolve and become more interconnected, the framework provides a vital tool for safeguarding these systems. Moving forward, continuous refinement and adaptation of the framework will be essential to address emerging challenges and opportunities. By embracing new technologies and maintaining a focus on security, the framework will ensure that critical infrastructure networks remain resilient, secure, and capable of supporting the complex demands of the future.

REFERENCES

[1] Agupugo, C. (2023). Design of A Renewable Energy Based Microgrid That Comprises of Only PV and Battery Storage to Sustain Critical Loads in Nigeria Air Force Base, Kaduna. ResearchGate.

[2] Agupugo, C. P., & Tochukwu, M. F. C. (2021): A model to Assess the Economic Viability of Renewable Energy Microgrids: A Case Study of Imufu Nigeria.

[3] Agupugo, C. P., Ajayi, A. O., Nwanevu, C., & Oladipo, S. S. (2022); Advancements in Technology for Renewable Energy Microgrids.

[4] Agupugo, C. P., Ajayi, A. O., Nwanevu, C., & Oladipo, S. S. (2022): Policy and regulatory framework supporting renewable energy microgrids and energy storage systems.

[5] Asibor, J. O., & Ighodaro, O. (2019). Steady State Analysis of Nanofuel Droplet Evaporation. *International Journal of Nanoscience and Nanotechnology*, *15*(3), 145-155.

[6] Avwioroko, A. (2023). Biomass Gasification For Hydrogen Production. *Engineering Science & Technology Journal*, *4*(2), 56-70.

[7] Avwioroko, A. (2023). The integration of smart grid technology with carbon credit trading systems: Benefits, challenges, and future directions. *Engineering Science & Technology Journal*, *4*(2), 33–45.

[8] Avwioroko, A. (2023). The potential, barriers, and strategies to upscale renewable energy adoption in developing countries: Nigeria as a case study. *Engineering Science & Technology Journal*, *4*(2), 46–55.

[9] Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions. *International Journal of Management Technology*, *10*(1), 85-108.

[10] Bello, O. A., Folorunso, A., Ogundipe, A., Kazeem, O., Budale, A., Zainab, F., & Ejiofor, O. E. (2022). Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection. *International Journal of Network and Communication Research*, *7*(1), 90-113.

[11] Bello, O. A., Folorunso, A., Onwuchekwa, J., & Ejiofor, O. E. (2023). A Comprehensive Framework for Strengthening USA Financial Cybersecurity: Integrating Machine Learning and AI in Fraud Detection Systems. *European Journal of Computer Science and Information Technology*, *11*(6), 62-83.

[12] Bello, O. A., Folorunso, A., Onwuchekwa, J., Ejiofor, O. E., Budale, F. Z., & Egwuonwu, M. N. (2023). Analysing the Impact of Advanced Analytics on Fraud Detection: A Machine Learning Perspective. *European Journal of Computer Science and Information Technology*, *11*(6), 103-126.

[13] Boda, V. V. R., & Immaneni, J. (2019). Streamlining FinTech Operations: The Power of SysOps and Smart Automation. *Innovative Computer Sciences Journal*, *5*(1).

[14] Chirra, D. R. (2021). Mitigating Ransomware in Healthcare: A Cybersecurity Framework for Critical Data Protection. *Revista de Inteligencia Artificial en Medicina*, *12*(1), 495-513.

[15] Debbabi, F., Jmal, R., & Chaari Fourati, L. (2021). 5G network slicing: Fundamental concepts, architectures, algorithmics, projects practices, and open issues. *Concurrency and Computation: Practice and Experience*, *33*(20), e6352.

[16] Derhamy, H. (2016). *Towards Interoperable Industrial Internet of Things: An On-Demand Multi-Protocol Translator Service* (Doctoral dissertation).

[17] Egware, H. O., & Ighodaro, O. O. (2023). Evaluating the effect of ambient air temperature on the exergy sustainability of a 153MW gas turbine power plant. *International Journal of Thermofluids*, *18*, 100375.

[18] Egware, H. O., Ighodaro, O. O., & Unuareokpa, O. J. (2016). Experimental design and fabrication of domestic water heating from solid waste incinerator. *Journal of Civil and Environmental Systems Engineering*, *14*(1), 180–192.

[19] Egware, H. O., Obanor, A. I., Aniekwu, A. N., Omoifo, O. I., & Ighodaro, O. O. (2021). Modelling and simulation of the SGT5–2000E gas turbine model for power generation. *Journal of Energy Technology and Environment*, *3*(2).

[20] Egware, H. O., Onochie, U. P., & Ighodaro, O. O. (2016). Prospects of wind energy for power generation in university of Benin. *Int. J. of Thermal & Environmental Engineering*, *13*(1), 23-28.

[21] Elete, T. Y., Nwulu, E. O., Erhueh, O. V., Akano, O. A. & Aderamo, A. T., 2023. Early startup methodologies in gas plant commissioning: An analysis of effective strategies and their outcomes. International Journal of Scientific Research Updates, 5(2), pp. 49–60. Available at: https://doi.org/10.53430/ijsru.2023.5.2.0049.

[22] Elete, T. Y., Nwulu, E. O., Omomo, K. O., Esiri, A. E. & Aderamo, A. T., 2023. Alarm rationalization in engineering projects: Analyzing cost-saving measures and efficiency gains. International Journal of Frontiers in Engineering and Technology Research, 4(2), pp. 22–35. Available at: https://doi.org/10.53294/ijfetr.2023.4.2.0022.

[23] Elete, T. Y., Nwulu, E. O., Omomo, K. O., Esiri, A. E. & Aderamo, A. T., 2023. Achieving operational excellence in midstream gas facilities: Strategic management and continuous flow assurance. International Journal of Frontiers in Science and Technology Research, 4(2), pp. 54–67. Available at: https://doi.org/10.53294/ijfstr.2023.4.2.0054.

[24] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Application of deep and machine learning techniques for multi-label classification performance on psychotic disorder diseases. *Informatics in Medicine Unlocked*, *23*, 100545.

[25] Elujide, I., Fashoto, S. G., Fashoto, B., Mbunge, E., Folorunso, S. O., & Olamijuwon, J. O. (2021). Informatics in Medicine Unlocked.

[26] Furdek, M., Natalino, C., Di Giglio, A., & Schiano, M. (2021). Optical network security management: requirements, architecture, and efficient machine learning models for detection of evolving threats. *Journal of Optical Communications and Networking*, *13*(2), A144-A155.

[27] Gadde, H. (2019). AI-Driven Schema Evolution and Management in Heterogeneous Databases. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *10*(1), 332-356.

[28] Gadde, H. (2021). Secure Data Migration in Multi-Cloud Systems Using AI and Blockchain. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 128-156.

[29] Ghobakhloo, M. (2020). Determinants of information and digital technology implementation for smart manufacturing. *International Journal of Production Research*, *58*(8), 2384-2405.

[30] Gudala, L., Shaik, M., Venkataramanan, S., & Sadhu, A. K. R. (2019). Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT Networks. *Distributed Learning and Broad Applications in Scientific Research*, *5*, 23-54.

[31] Hazra, A., Adhikari, M., Amgoth, T., & Srirama, S. N. (2021). A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions. *ACM Computing Surveys (CSUR)*, *55*(1), 1-35.

[32] Holm, H. H., Gezer, V., Hermawati, S., Altenhofen, C., & Hjelmervik, J. M. (2017). The CloudFlow Infrastructure for Multi-Vendor Engineering Workflows: Concept and Validation. *International Journal on Advances in Internet Technology*, *10*(1).

[33] Hughes, G. D. (2016). *A framework for software patch management in a multi-vendor environment* (Doctoral dissertation, Cape Peninsula University of Technology).

[34] Ibrahim, A. O., Ighodaro, O. O., Fasogbon, S. K., Orumwense, E. F., & Waheed, M. A. (2023). Failure investigation of the tube of a dual fired steam boiler in a western nigerian food and beverage manufacturing plant. *Engineering Failure Analysis*, *143*, 106906.

[35] Ighodaro, O. O. (2010). Reliability and availability analysis of gas turbine plants. *International Journal of Engineering and Technology*, *2*(1), 38–50.

[36] Ighodaro, O. O. (2016). *Modelling and simulation of intermediate temperature solid oxide fuel cells and their integration in hybrid gas turbine plants* (Doctoral dissertation, Newcastle University).

[37] Ighodaro, O. O., & Aburime, B. A. (2011). Exergetic appraisal of Delta IV power station, Ughelli. *Journal of Emerging Trends in Engineering and Applied Sciences*, *2*(2), 216-218.

[38] Ighodaro, O. O., & Agbro, E. B. (2010). Efficiency Analysis of Power Generation in Gas Turbine Plants. *International Journal of Natural and Applied Sciences*, *2*(1), 20-31.

[39] Ighodaro, O. O., & Aregbe, O. (2017). Conceptual design and fabrication of a dual powered self cleaning marker board. *Journal of the Nigerian Association of Mathematical Physics*, *39*, 379-384.

[40] Ighodaro, O. O., & Egbon, O. C. (2021). Comparative Performance Assessment of Different Gas Turbine Configurations: A Study of a Local Power Station in Nigeria. *Nigerian Journal of Engineering*, *28*(2).

[41] Ighodaro, O. O., & Egwaoje, S. O. (2020). Design and Feasibility Study of a PV-Micro Hydro Off-Grid Power Generating System. *NIPES-Journal of Science and Technology Research*, *2*(1).

[42] Ighodaro, O. O., & Egware, H. O. (2014). Experimental design and fabrication of displacer-type Stirling engine for small-scale electricity generation. *University of Benin*

Journal of Science and Technology, 2(1), 96–103.

[43] Ighodaro, O. O., & Essien, N. F. (2020). Experimental Analysis on the Characteristics of Pulverized Coal-Palm kernel Shell Fuel Blend. *CaJoST*, *2*(2), 89-93.

[44] Ighodaro, O. O., & Ndem, F. E. (2023). Performance Modelling of Co-Fired Palm Kernel Shell-Pulverized Coal Blend in Steam Power Plant. *Journal of Applied Sciences and Environmental Management*, *27*(5), 899-903.

[45] Ighodaro, O. O., & Orumwense, E. F. (2022). Performance analysis and ranking of selected organic fluids for use in an organic Rankine cycle. *Journal of Engineering for Development, 14*(3), 82–91.

[46] Ighodaro, O. O., & Osikhuemhe, M. (2019). Numerical investigation of the effect of tyre inflation pressure on fuel consumption in automobiles. *Nigerian Journal of Technological Research*, *14*(2), 38-47.

[47] Ighodaro, O. O., & Osikhuemhe, M. (2019). Thermo-economic analysis of a heat recovery steam generator combined cycle. *Nigerian Journal of Technology*, *38*(2), 342-347.

[48] Ighodaro, O. O., & Saale, G. B. (2017). Performance and exergy analysis of boiler (101-B-01) system at the Warri Refining and Petrochemical Company. *Journal of the Nigerian Association of Mathematical Physics*, *39*, 369-378.

[49] Ighodaro, O. O., & Scott, K. (2017). Polarisation modelling of an anode-supported solid oxide fuel cell. *Research Journal of Engineering and Environmental Sciences, 2*(1), 18–31.

[50] Ighodaro, O. O., Aburime, E. I., & Erameh, A. A. (2022). Off-design modelling of a turbo jet engine with operative afterburner. *Open Journal of Energy Efficiency*, *11*(3), 88-107.

[51] Ighodaro, O. O., Ilori, S. O., Aburime, E. I., & Obanor, A. I. (2022). An equilibrium model of NOx emission in gas turbine combustors. *Nigerian Journal of Technology*, *41*(4), 778-788.

[52] Ighodaro, O. O., Okogie, S., & Ozakpolor, J. (2010). Design and modelling of a wind power generating plant. *Journal of Engineering and Applied Science, 2*(1), 82–92.

[53] Ighodaro, O. O., Olaosebikan, F., & Egware, H. O. (2020). Technical analysis and economic assessment of a standalone solar PV/fuel cell hybrid power system. *Nigerian Journal of Engineering Science Research, 3*(1), 27–34.

[54] Ighodaro, O. O., Scott, K., & Xing, L. (2017). An isothermal study of the electrochemical performance of intermediate temperature solid oxide fuel cells. *Journal of Power and Energy Engineering*, *5*(2), 97-122.

[55] Ighodaro, O., & Akhihiero, D. (2021). Modeling and performance analysis of a small horizontal axis wind turbine. *Journal of Energy Resources Technology*, *143*(3), 031301.

[56] Ighodaro, O., & Scott, K. (2013): Numerical Modelling of Solid Oxide Fuel Cells: Role of Various Cell Parameters on Performance.

[57] Ighodaro, O., Ochornma, P., & Egware, H. (2020). Energy Analysis of A Retrofitted Regenerative Gas Turbine Organic Cycle in Ihovbor Power Plant. *International Journal of Engineering Technologies IJET*, *6*(3), 45-61.

[58] Islam, C., Babar, M. A., & Nepal, S. (2019). A multi-vocal review of security orchestration. *ACM Computing Surveys (CSUR)*, *52*(2), 1-45.

[59] Jackson, B. W. (2019). Cybersecurity, privacy, and artificial intelligence: an examination of legal issues surrounding the european union general data protection regulation and autonomous network defense. *Minn. JL Sci. & Tech.*, *21*, 169.

[60] Jiang, W., Han, B., Habibi, M. A., & Schotten, H. D. (2021). The road towards 6G: A comprehensive survey. *IEEE Open Journal of the Communications Society*, *2*, 334-366.

[61] Kaistinen, J. (2017). *Partner ecosystems in enterprise software: cause and effect of the business model from vendor, partner and customer perspectives* (Master's thesis).

[62] Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1-34.

[63] Kalusivalingam, A. K., Sharma, A., Patel, N., & Singh, V. (2021). Enhancing Smart City Development with AI: Leveraging Machine Learning Algorithms and IoT-Driven Data Analytics. *International Journal of AI and ML*, *2*(3).

[64] Kaul, D. (2021). AI-Driven Dynamic Upsell in Hotel Reservation Systems Based on Cybersecurity Risk Scores. *International Journal of Computer Engineering and Technology (IJCET)*, *12*(3), 114-125.

[65] Khurana, R. (2020). Fraud detection in ecommerce payment systems: The role of predictive ai in real-time transaction security and risk management. *International Journal of Applied Machine Learning and Computational Intelligence*, *10*(6), 1-32.

[66] Kijewski, R. J. (2015). *The impact of disruptive technology trends on networking hardware vendors* (Doctoral dissertation, Massachusetts Institute of Technology).

[67] Koufos, K., El Haloui, K., Dianati, M., Higgins, M., Elmirghani, J., Imran, M. A., & Tafazolli, R. (2021). Trends in intelligent communication systems: review of standards, major research projects, and identification of research gaps. *Journal of Sensor and Actuator Networks*, *10*(4), 60.

[68] Kwasi, C. C., & Ighodaro, O. O. (2023). Assessment of a UFAA-19 series hybrid vehicle's dynamics. *Journal of the Nigerian Institution of Production Engineers, 27*(March 2023), 45–55.

[69] Kwasi, C. C., & Ighodaro, O. O. (2023). Performance assessment of a hydram energy system on varying discharge head for power generation. *Journal of the Nigerian Institution of Production Engineers, 27*(March 2023), 69–79.

[70] Kwasi-Effah, C. C., Egware, H. O., Obanor, A. I., & Ighodaro, O. O. (2023). Development and characterization of a quaternary nitrate based molten salt heat transfer fluid for concentrated solar power plant. *Heliyon*, *9*(5).

[71] Kwasi-Effah, C. C., Ighodaro, O. O., Egware, H. O., & Obanor, A. I. (2023). Recent progress in the development of thermal energy storage mediums for solar applications. *J. Eng. Dev*, *15*(1), 146-170.

[72] Kwasi-Effah, C. C., Ighodaro, O., Egware, H. O., & Obanor, A. I. (2022). Characterization and comparison of the thermophysical property of ternary and quaternary salt mixtures for solar thermal power plant applications. *Results in Engineering*, *16*, 100721.

[73] Kwasi-Effah, C. C., Ighodaro, O., Egware, H. O., & Obanor, A. I. (2022). A novel empirical model for predicting the heat accumulation of a thermal energy storage medium for solar thermal applications. *Journal of Energy Storage*, *56*, 105969.

[74] Lees, A. (2019). Automation and AI in Network Scalability and Management. *International Journal of Advanced and Innovative Research*.

[75] Marda, V. (2018). Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180087.

[76] Martinez, A., Yannuzzi, M., López, V., López, D., Ramírez, W., Serral-Gracià, R., ... & Altmann, J. (2014). Network management challenges and trends in multi-layer and multi-vendor settings for carrier-grade networks. *IEEE Communications Surveys & Tutorials*, *16*(4), 2207-2230.

[77] Mazurek, G., & Małagocka, K. (2019). Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*, *6*(4), 344-364.

[78] Min-Jun, L., & Ji-Eun, P. (2020). Cybersecurity in the Cloud Era: Addressing Ransomware Threats with AI and Advanced Security Protocols. *International Journal of Trend in Scientific Research and Development*, *4*(6), 1927-1945.

[79] Muhammad, T. (2019). Revolutionizing Network Control: Exploring the Landscape of

Software-Defined Networking (SDN). *International Journal of Computer Science and Technology*, *3*(1), 36-68.

[80] Muhammad, T. (2021). Overlay Network Technologies in SDN: Evaluating Performance and Scalability of VXLAN and GENEVE. *International Journal Of Computer Science And Technology*, *5*(1), 39-75.

[81] Mustapha, O. Z. (2019). *Intelligent based Packet Scheduling Scheme using Internet Protocol/Multi-Protocol Label Switching (IP/MPLS) Technology for 5G. Design and Investigation of Bandwidth Management Technique for Service-Aware Traffic Engineering using Internet Protocol/Multi-Protocol Label Switching (IP/MPLS) for 5G* (Doctoral dissertation, University of Bradford

[82] Nimmagadda, V. S. P. (2021). Artificial Intelligence and Blockchain Integration for Enhanced Security in Insurance: Techniques, Models, and Real-World Applications. *African Journal of Artificial Intelligence and Sustainable Development*, *1*(2), 187-224.

[83] Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. *Mobile networks and applications*, *24*, 796-809.

[84] Nwulu, E. O., Elete, T. Y., Aderamo, A. T., Esiri, A. E. & Erhueh, O. V., 2023. Promoting plant reliability and safety through effective process automation and control engineering practices. World Journal of Advanced Science and Technology, 4(1), pp. 62–75. Available at: https://doi.org/10.53346/wjast.2023.4.1.0062.

[85] Nwulu, E. O., Elete, T. Y., Erhueh, O. V., Akano, O. A. & Omomo, K. O., 2023. Machine learning applications in predictive maintenance: Enhancing efficiency across the oil and gas industry. International Journal of Engineering Research Updates, 5(1), pp. 17–30. Available at: https://doi.org/10.53430/ijeru.2023.5.1.0017.

[86] Nwulu, E. O., Elete, T. Y., Omomo, K. O., Akano, O. A. & Erhueh, O. V., 2023. The importance of interdisciplinary collaboration for successful engineering project completions: A strategic framework. World Journal of Engineering and Technology Research, 2(3), pp. 48–56. Available at: https://doi.org/10.53346/wjetr.2023.2.3.0048.

[87] Nwulu, E. O., Elete, T. Y., Omomo, K. O., Esiri, A. E. & Erhueh, O. V., 2023. Revolutionizing turnaround management with innovative strategies: Reducing ramp-up durations post-maintenance. International Journal of Frontline Research in Science and Technology, 2(2), pp. 56–68. Available at: https://doi.org/10.56355/ijfrst.2023.2.2.0056.

[88] Ohile, S., Aboje, A., Uthman, H., Usman, R., & Ighodaro, O. (2023). Optimization and Characterization of Biodiesel Production from Mango Seed Oil (Magnifera indica) via Transesterification Reaction. *Journal of Energy Technology and Environment*, *5*(3).

[89] Okagbare, G. O., Omotehinse, S. A., & Ighodaro, O. O. (2022). An Investigation of the Hydro-Power Potential of the Ojirami Dam in Nigeria. *Journal of Energy Technology and Environment*, *4*(2).

[90] Onochie, U. P. (2019). A comprehensive review on biomass pelleting Technology and electricity generation from biomass. *Journal of Energy Technology and Environment*, *1*.

[91] Onochie, U. P. (2020). Evaluating the Energy Cost Benefit of a Biomass Fired Combined Heat and Power Plant. *NIPES-Journal of Science and Technology Research*, *2*(1).

[92] Onochie, U. P., & Ighodaro, O. O. (2017). Power generation potential from fuel pellets developed from oil palm residues. *African Journal of Renewable and Alternative Energy*, *2*(3), 32–38.

[93] Onochie, U. P., Ighodaro, O. O., Kwasi-Effah, C. C., & Otomi, K. O. (2018). One dimensional simulation of extrusion channel of biomass pelleting machine. *Journal of Applied Sciences and Environmental Management*, *22*(8), 1213-1217.

[94] Onochie, U. P., Madagwu, L. O., Kwasi-Effah, C. C., Ighodaro, O. O., Kubeynje, B. F., Akingba, O. O., & Damisah, L. E. (2022). Energy Audit of a Solar Panel Manufacturing Plant: A Case Study of NASENI Solar Panel

Plant, Karshi, Abuja. *Journal of Energy Technology and Environment*, *4*(1).

[95] Onochie, U. P., Obanor, A. I., & Ighodaro, O. O. (2017). Combustion performance and durability analysis of biomass fuel pellets from oil palm residues.

[96] Onochie, U. P., Obanor, A. I., Aliu, S. A., & Igbodaro, O. O. (2017). Proximate and ultimate analysis of fuel pellets from oil palm residues. *Nigerian Journal of Technology*, *36*(3), 987-990.

[97] Onochie, U. P., Obanor, A. I., Aliu, S. A., & Ighodaro, O. O. (2017). Determination of some thermal characteristics of fuel pellets obtained from oil palm residues. *J. Natl. Assoc. Math. Phys*, *40*, 447-450.

[98] Onochie, U. P., Obanor, A. L., Aliu, S. A., & Ighodaro, O. O. (2017). Fabrication and performance evaluation of a pelletizer for oil palm residues and other biomass waste materials. *Journal of the Nigerian Association of Mathematical Physics*, *40*, 443-446.

[99] Onyeke, F. O., Odujobi, O., Adikwu, F. E. & Elete, T. Y., 2022. Innovative approaches to enhancing functional safety in Distributed Control Systems (DCS) and Safety Instrumented Systems (SIS) for oil and gas applications. Open Access Research Journal of Multidisciplinary Studies, 3(1), pp. 106–112. Available at: <https://doi

[100] Onyeke, F. O., Odujobi, O., Adikwu, F. E. & Elete, T. Y., 2023. Functional safety innovations in burner management systems (BMS) and variable frequency drives (VFDs): A proactive approach to risk mitigation in refinery operations. International Journal of Science and Research Archive, 10(2), pp. 1223–1230. Available at: https://doi.org/10.30574/ijsra.2023.10.2.0917.

[101] Onyiriuka, E. J., Ighodaro, O. O., Adelaja, A. O., Ewim, D. R. E., & Bhattacharyya, S. (2019). A numerical investigation of the heat transfer characteristics of water-based mango bark nanofluid flowing in a double-pipe heat exchanger. *Heliyon*, *5*(9).

[102] Orumwense, E. F., Ighodaro, O. O., & Abo-Al-Ez, K. (2021). Energy growth and sustainability through smart grid approach: a case study of the Nigeria Electric grid. *International Review of Electrical Engineering (IREE)*, *16*(6), 542-551.

[103] Osarobo, I., & Chika, A. (2016). Neural network modeling for monitoring petroleum pipelines. *International Journal of Engineering Research in Africa*, *26*, 122-131.

[104] Parikh, A. (2019). *Cloud security and platform thinking: an analysis of Cisco Umbrella, a cloud-delivered enterprise security* (Doctoral dissertation, Massachusetts Institute of Technology).

[105] Peltonen, E., Bennis, M., Capobianco, M., Debbah, M., Ding, A., Gil-Castiñeira, F., ... & Yang, T. (2020). 6G white paper on edge intelligence. *arXiv preprint arXiv:2004.14850*.

[106] Petrenko, K., Mashatan, A., & Shirazi, F. (2019). Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. *Journal of Information Security and Applications*, *46*, 151-163.

[107] Plugge, A., & Janssen, M. (2014). Governance of multivendor outsourcing arrangements: a coordination and resource dependency view. In *Governing Sourcing Relationships. A Collection of Studies at the Country, Sector and Firm Level: 8th Global Sourcing Workshop 2014, Val d'Isere, France, March 23-26, 2014, Revised Selected Papers 8* (pp. 78-97). Springer International Publishing.

[108] Pölöskei, I., & Bub, U. (2021). Enterprise-level migration to micro frontends in a multi-vendor environment. *Acta Polytechnica Hungarica*, *18*(8), 7-25.

[109] Qureshi, H. (2021). Addressing training data sparsity and interpretability challenges in AI based cellular networks.

[110] Yahya, M. A. Y. (2017). *SDN improvements and solutions for traditional networks* (Master's thesis, Çankaya Üniversitesi).