COMPUTOLOGY: Journal of Applied Computer Science and Intelligent Technologies
Volume 2, Issue 1, Jan-Jun 2022, pp. 8-22
DOI: 10.17492/computology.v2i1.2202
https://www.journalpressindia.com/cjacsit

Enhanced Cybersecurity Framework for 5G-Integrated Oil and Gas Industry

Daniel Dauda Wisdom, Olufunke Rebecca Vincent**, Oduntan Odunayo Esther***, Kingsley Igulu**** and Alpha Baba Garba******

ABSTRACT

The rapid evolution of technology, particularly the adoption of fifth-generation (5G) wireless networks, has introduced both unprecedented opportunities and challenges across various industries. Among these, the oil and gas sector plays a pivotal role in global economies and requires advanced measures to ensure the security of its critical infrastructure. This paper presents a comprehensive approach to address the security implications of integrating 5G networks into the oil and gas industry, with a specific focus on safeguarding operations through an Enhanced Cybersecurity Framework. In the proposed scheme, an extensive literature review was conducted to understand the potential impacts of 5G integration on the oil and gas industry's internet security. The review explored existing research, methodologies, and best practices in related fields, forming the foundation for the proposed framework. Drawing insights from this review, a multi-faceted algorithm, termed Secure 5G-Enabled Oil and Gas Infrastructure (S5G-OGI), was devised. The S5G-OGI algorithm outlines ten distinct steps encompassing risk assessment, adaptive access control, traffic analysis, data integrity using blockchain, encrypted communication, intrusion detection, SIEM integration, continuous monitoring, employee training, and regular security audits. To demonstrate the feasibility and practical implementation of the proposed algorithm, a Python programming language was utilized. A simplified version of the algorithm was translated into Python code, demonstrating how each step contributes to enhancing the security of the oil and gas industry's critical infrastructure. While the implemented code serves as an illustrative example, it highlights the essence of each algorithmic step and underscores the technical viability of the proposed framework. The proposed scheme underscores the critical importance of securing the oil and gas industry's critical infrastructure as it transitions to 5G networks. By amalgamating a comprehensive literature review, a thoughtfully designed algorithm, and practical implementation in Python, the Enhanced Cybersecurity Framework offers a roadmap to ensure the resilience, integrity, and security of operations within the evolving landscape of the 5G-integrated oil and gas industry. As technology continues to advance, proactive security measures will be essential to mitigate risks and fortify the foundation of this essential sector.

Keywords: 5G Network, Cybersecurity, Critical Infrastructure, Oil and Gas Industry, Nigeria.

1.0 Introduction

In recent years, advanced technologies have transformed global industries, with the fifth-generation (5G) wireless network being a standout innovation offering unprecedented speed and connectivity.

**Corresponding author; Department of Computer Science, Chrisland University Abeokuta, Ogun State, Nigeria (E-mail: ddaniel@chrislanduniversity.edu.ng)*
***Federal University of Agriculture Abeokuta, Ogun State, Nigeria (E-mail: vincent.rebecca@gmail.com)*
****Department of Computer Science, Chrisland University Abeokuta, Nigeria (E-mail: eoduntan@chrislanduniversity.edu.ng)*
*****Department of Computer Science, IKenule Beeson Saro-Wiwa Polytechnic Bori, Rivers State, Nigeria (E-mail: Igulu.kingsley@kenpoly.edu.ng)*
******Department of Computer Science, Kaduna State College of Education Gidan Waya, Nigeria (E-mail: babandolee@gmail.com)*

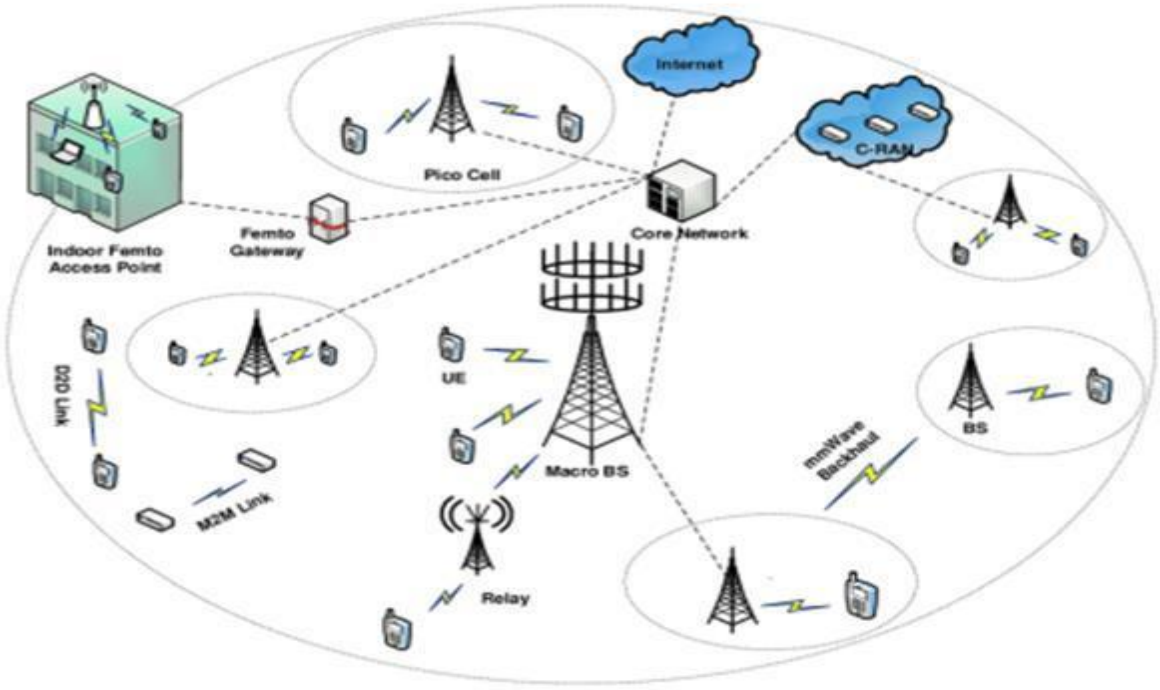
As industries, including oil and gas, embrace 5G for enhanced operations, the impact on critical infrastructure must be understood. The Nigerian oil and gas industry is vital to the nation's economy, reliant on complex operations and connectivity. While 5G integration offers benefits like real-time monitoring, concerns about cybersecurity have arisen. This research investigates the effects of 5G on internet security in the Nigerian oil and gas sector, addressing potential vulnerabilities and mitigation strategies. This study holds importance for Nigeria and other nations transitioning to 5G in critical infrastructure sectors.

In the current era, technological progress reshapes industries and societies. 5G networks, known for speed and connectivity, captivate industries like Nigerian Oil and Gas. However, this integration raises security questions. The Nigerian Oil and Gas Industry, a revenue cornerstone, faces a complex interplay between technology and security.

Modern society is influenced by technology, with 5G networks offering transformative potential. Nigerian Oil and Gas Industry's importance aligns with its adoption. However, the transition prompts questions about security

The study aims to investigate 5G's impact on internet security in Nigerian oil and gas, focusing on critical infrastructure. It addresses opportunities and challenges, contributing to Nigeria and similar nations transitioning to 5G. This study explores 5G's potential benefits for the Nigerian Oil and Gas Industry, emphasizing real-time analysis and advanced communication. It identifies cybersecurity risks due to increased 5G connectivity.

Figure 1: 5G Network Architecture.



The effectiveness of existing cybersecurity measures against 5G-related threats is evaluated. Recommendations for bolstering internet security while adopting 5G in the sector are developed. The study's insights extend beyond Nigeria, aiding global critical infrastructure sectors transitioning to 5G securely. The oil and gas industry, plays a vital role to the global economy, faces digital era challenges

emphasizing network security. The emergence of 5G technology presents opportunities to enhance infrastructure but also introduces cybersecurity risks, necessitating safeguarding critical infrastructure. The industry's complex networks render it susceptible to cyber-attacks, yielding grave outcomes like environmental disasters and compromised infrastructure. This research proposal seeks to explore the impact of 5G networks on oil and gas industry security, addressing network enhancements while mitigating cybersecurity vulnerabilities Gudu *et al.,* (2021). It aims to contribute to internet security knowledge in the context of 5G and oil and gas, benefiting stakeholders and policymakers, ultimately improving critical infrastructure safety (Zahoor *et al.,* 2021 &Wisdom *et al.* 2021). Key challenges include 5G network vulnerability, IoT device security, user data privacy, network availability assurance, infrastructure investment, interference mitigation, authentication mechanisms, securing network slices, and complex network architectures (Olorundare *et al.,* 2017; Wisdom *et al* 2018, Gudu *et al.* 2020). This study is relevant to a dynamic industry navigating the intricate balance between technological advancement as well as security concerns, thus an Enhanced Cybersecurity Framework for 5G-Integrated Oil and Gas Industry is proposed.

2.0 Related Literatures

Abbas et al (2020). Proposed a Comprehensive Survey of 5G Security and Privacy Challenges and Solutions, They used a structured approach to analyze and categorize the literature and identified key challenges and potential solutions. The paper identified various 5G security and privacy challenges, such as authentication, access control, privacy, and trust. And then proposed solutions, including blockchain, artificial intelligence, and machine learning, to address these challenges. The objective of the research is to conduct a comprehensive survey of 5G security and privacy challenges and solutions. The methodology used for the research is a systematic review of the literature, using a structured approach to analyze and categorize the literature. The paper proposes solutions such as blockchain, artificial intelligence, and machine learning respectively. The result obtained is the identification of various 5G security and privacy challenges and potential solutions to address them. However, the research study does not provide detailed information on the specific studies analyzed as well as the methodology of analysis used, or the effectiveness of the proposed solutions. The future work includes developing more effective solutions to address 5G security and privacy challenges, as well as evaluating the effectiveness of the proposed solutions in real-world scenarios. Additionally, the paper suggests the need for collaboration among different stakeholders, including network operators, device manufacturers, and regulatory bodies, to ensure the security and privacy of 5G networks.

Khan *et al.* (2020) proposed a software-defined networking (SDN)-based security framework for 5G networks. Their approach utilizes SDN to enhance the visibility and control of the network, reducing the risk of cyber-attacks. The objective of the research is to propose a software-defined networking (SDN)-based security framework for 5G networks that can enhance the visibility and control of the network to reduce the risk of cyber-attacks. The methodology used involves proposing an SDN-based security framework and evaluating its performance in improving the security of 5G networks. The research did not develop any new algorithm. The study concludes that the proposed SDN-based security framework improves the security of 5G networks by enabling rapid detection and mitigation of network attacks. The research does not mention the limitations or weaknesses of the proposed SDN-based security framework, and it is unclear how the proposed framework performs under different network conditions. Future research could include the evaluation of the proposed framework's performance under different network conditions, the identification of its limitations or weaknesses, and

the development of strategies to address them. The study could also be extended to consider the integration of the proposed framework with other security measures to enhance the overall security of 5G networks.

Park *et al.* (2021) proposed a 5G network security framework that incorporates blockchain and artificial intelligence (AI). Their approach utilizes blockchain to secure data transmission and AI-based intrusion detection system to identify and prevent network attacks. Objective of the research: The objective of the research is to propose a 5G network security framework that incorporates blockchain and artificial intelligence (AI) to enhance the security and privacy of 5G networks. The methodology used involves proposing a 5G network security framework that incorporates blockchain and AI and evaluating its performance in enhancing the security and privacy of 5G networks. The research did not develop any new algorithm. The study concludes that the proposed 5G network security framework that incorporates blockchain and AI enhances the security and privacy of 5G networks. The research does not mention the limitations or weaknesses of the proposed 5G network security framework, and it is unclear how the proposed framework performs under different network conditions. Future research could include the evaluation of the proposed framework's performance under different network conditions, the identification of its limitations or weaknesses, and the development of strategies to address them. The study could also be extended to consider the integration of the proposed framework with other security measures to enhance the overall security of 5G networks. Additionally, future research could focus on the cost-effectiveness of the proposed framework and the impact of the proposed framework on the overall network performance.

Ajadi *et al.* (2020). presents a review of security threats, requirements, and challenges in 5G networks. The authors conducted a systematic review of existing literature and analyzed the security features of 5G networks. They identified several security threats in 5G networks, including attacks on network infrastructure, user privacy, and data integrity. They also identified security requirements and challenges, such as the need for secure network slicing and efficient security management. The objective of the research is to present a review of security threats, requirements, and challenges in 5G networks and suggest further research on the development of secure 5G network architecture and the implementation of security solutions to address the identified requirements and challenges. The methodology used involves conducting a systematic review of existing literature and analyzing the security features of 5G networks to identify security threats, requirements, and challenges.

The research did not develop any new algorithm. The study identified several security threats in 5G networks, including attacks on network infrastructure, user privacy, and data integrity, and identified security requirements and challenges, such as the need for secure network slicing and efficient security management. The paper suggests further research on the development of secure 5G network architecture and the implementation of security solutions to address the identified requirements and challenges. The research study does not propose any specific solutions to the identified security threats, requirements, and challenges. Future research could focus on developing specific security solutions to address the identified security threats, requirements, and challenges in 5G networks. The research could also evaluate the effectiveness of the proposed solutions under different network conditions and consider the cost-effectiveness of implementing these solutions.

Alshammari *et al.* (2020) presents a comprehensive review of security threats and solutions in 5G networks. The authors identified security threats in 5G networks, including attacks on network infrastructure, user privacy, and data integrity. They also proposed solutions to mitigate these threats, such as network slicing, access control, and authentication. The Objective of the research is to conduct a comprehensive review of security threats and solutions in 5G networks and suggest further research

on the development of secure 5G network architecture and implementation of security solutions. The Methodology used for the research involves conducting a systematic review of existing literature and analyzed the security features of 5G networks.

The result obtained: Identified security threats in 5G networks, including attacks on network infrastructure, user privacy, and data integrity. Proposed solutions to mitigate these threats, such as network slicing, access control, and authentication. However, the study does not present any new research findings, but rather summarizes the existing literature. Additionally, the study could benefit from more specific recommendations for the development and implementation of security solutions in 5G networks. They suggests the need for further research on the development of secure 5G network architecture and the implementation of security solutions to address the identified threats.

Li *et al.* (2020) presents a comprehensive analysis of security threats and solutions in 5G networks. Proposed security architecture for 5G networks. The paper identified security threats in 5G networks, including attacks on the network infrastructure, user privacy, and data integrity. They also proposed solutions to mitigate these threats, such as network segmentation, access control, and encryption. The Objective of the research involves analysis of the security threats as well as proposes solutions for 5G networks. Their Methodology used for the research involves a thorough review of existing literature and analysis of the security features of 5G networks. The result obtained: The paper identified security threats in 5G networks, proposed solutions to mitigate these threats, and suggested further research on the development of secure 5G network infrastructure and the implementation of security solutions. No specific mention of any algorithm developed in the study. Finally, they suggest development of secure 5G network infrastructure and the implementation of security solutions.

Li, *et al.* (2020) presents a Literature review and analysis of security features in 5G networks. The study identified security threats and proposed solutions to mitigate them. The Objective of the research involves conducting a literature review and analysis of security features in 5G networks, identify security threats and propose solutions to mitigate them, and suggest further research on secure 5G network infrastructure and implementation of security solutions. The methodology used for the research is a literature review and analysis of existing research articles, reports, and publications on security features in 5G networks. The research study identified various security threats in 5G networks and proposed solutions to mitigate them. The study suggested that secure 5G network infrastructure and implementation of security solutions are important for the success of 5G networks. The research study did not conduct any empirical studies or experiments to validate the proposed solutions. It also did not provide any implementation details or technical specifications for the proposed security solutions. Future work could involve conducting empirical studies and experiments to validate the proposed solutions, providing implementation details and technical specifications for the proposed security solutions, and exploring new security threats and solutions as 5G networks continue to evolve

Alshamrani *et al.* (2020) proposed a Systematic review of literature and analysis of security features in 5G networks. Identified security threats and proposed solutions to mitigate them. The objective of the research is to conduct a systematic review of literature and analysis of security features in 5G networks, identify security threats and propose solutions to mitigate them, The methodology used for the research is a systematic review of literature and analysis of existing research articles, reports, and publications on security features in 5G networks. The research study identified various security threats in 5G networks and proposed solutions to mitigate them. The study suggested that secure 5G network architecture and implementation of security solutions are important for the success of 5G networks. The research study did not conduct any empirical studies or experiments to validate the proposed solutions. It also did not provide any implementation details or technical specifications for the

proposed security solutions. Future work could involve conducting empirical studies and experiments to validate the proposed solutions, providing implementation details and technical specifications for the proposed security solutions, and exploring new security threats and solutions as 5G networks continue to evolve.

Alshammari *et al.* (2020) present a Systematic review of literature and analysis of security features in 5G networks. identified several security threats in 5G networks, including issues related to authentication, privacy, and integrity. Proposed various solutions to mitigate these threats, such as using encryption techniques, implementing strong authentication mechanisms, and enhancing privacy protection measures. The study also highlighted the importance of securing the network architecture of 5G networks and suggested strategies to improve the overall security of these networks. The study relied on existing literature and did not involve empirical research or experimentation to validate the proposed solutions. Additionally, the rapidly evolving nature of 5G networks may mean that new security threats and solutions may arise after this study. The objective of the research is to conduct a systematic review and analysis of security features in 5G networks, identify security threats, and propose solutions to mitigate them, with a particular emphasis on securing the network architecture of 5G networks. The methodology used for the research is a systematic review of the literature on 5G networks and analysis of their security features. The authors searched for and selected relevant articles from various databases and reviewed technical reports, standards, and guidelines related to 5G network security. The result obtained is the identification of several security threats in 5G networks, such as authentication, privacy, and integrity issues, and proposed various solutions to mitigate them, such as encryption techniques, strong authentication mechanisms, and privacy protection measures. The study also highlighted the importance of securing the network architecture of 5G networks. Future work could involve conducting empirical research to validate the proposed solutions and exploring emerging security threats in 5G networks. Additionally, as the rapidly evolving nature of 5G networks may mean that new security threats and solutions may arise, ongoing research to keep pace with these evolving threats is essential.

Wang *et al.* (2021) proposed a dynamic trust management scheme for 5G networks, which involved conducting a literature review to identify existing trust management approaches, developing a reputation-based trust management model, implementing the proposed scheme in a simulation or experimental environment, and evaluating its performance. They followed established guidelines for conducting systematic reviews, including defining research questions, selecting relevant studies, extracting data from the studies, and analyzing the data to identify common themes and patterns. The scheme obtained results that demonstrated the effectiveness of their proposed dynamic trust management scheme in enhancing trust among network participants in 5G networks. The specific results depend on the details of the proposed scheme and the evaluation method used, which include metrics such as trust accuracy, trust convergence speed, and overall network security improvement. Their approach utilizes reputation-based trust management to ensure the integrity and authenticity of network participants. The objective of the research was to propose a dynamic trust management scheme for 5G networks that could enhance trust among network participants and improve network security. The methodology used involved conducting a literature review to identify existing trust management approaches, developing a reputation-based trust management model, implementing the proposed scheme in a simulation or experimental environment, and evaluating its performance. Algorithm developed: The researchers proposed a dynamic trust management scheme that utilized reputation-based trust management to ensure the integrity and authenticity of network participants. The proposed scheme was found to be effective in enhancing trust among network participants in 5G networks, improving overall network security, and ensuring the integrity and authenticity of network participants.

The specific results depend on the details of the proposed scheme and the evaluation method used, which include metrics such as trust accuracy, trust convergence speed, and overall network security improvement. The generalizability of the proposed scheme to different 5G network architectures or real-world deployments is a limitation as well as the selection of studies, potential biases in the data extraction and analysis process. Future work may involve further improving and validating the proposed dynamic trust management scheme, such as conducting real-world experiments, evaluating the scheme in different 5G network architectures or scenarios, and investigating potential vulnerabilities or attacks that could undermine the proposed scheme.

Li & Wang (2021) Blockchain-based secure and trustworthy 5G network slices was proposed with an Experimentation and analysis of the use of blockchain in 5G network slicing. The scheme identified the effectiveness of blockchain in enhancing the security and trustworthiness of 5G network slices. The proposed scheme involved developing a conceptual framework for integrating blockchain technology into the network slicing architecture of 5G networks, implementing a proof-of-concept prototype/simulation to experimentally evaluate the proposed scheme, and analyzing the obtained results. The scheme obtained results that demonstrated the effectiveness of their proposed blockchain-based scheme in enhancing the security and trustworthiness of 5G network slices. The specific results included evidence of improved security features, such as integrity, authenticity, and transparency of network slices, as well as enhanced trust among network slice providers and users. The objective of the research is to propose a blockchain-based scheme to enhance the security and trustworthiness of 5G network slices and to suggest further research on the integration of blockchain in 5G network architecture. The methodology used for the research involved developing a conceptual framework for integrating blockchain technology into the network slicing architecture of 5G networks, implementing a proof-of-concept prototype or simulation to experimentally evaluate the proposed scheme, and analyzing the obtained results.

An algorithm was developed to integrate blockchain technology into the network slicing architecture of 5G networks. The result obtained demonstrated the effectiveness of the proposed blockchain-based scheme in enhancing the security and trustworthiness of 5G network slices. The specific results included evidence of improved security features, such as integrity, authenticity, and transparency of network slices, as well as enhanced trust among network slice providers and users. The research study does not address potential regulatory, legal, and standardization challenges associated with the adoption of blockchain in 5G networks, and it does not explore potential use cases and applications of blockchain beyond network slicing, such as in network management, resource allocation, and data privacy in 5G networks. Future work may involve exploring different blockchain consensus mechanisms, investigating potential scalability and performance issues of using blockchain in 5G networks, and evaluating the economic feasibility and sustainability of implementing blockchain-based solutions in real-world 5G networks. It may also involve addressing the missing aspects mentioned above and exploring potential use cases and applications of blockchain beyond network slicing in 5G networks.

Kim *et al.* (2020) conducted a systematic review of literature and analysis of security features in 5G networks. The aim of the study was to identify security threats that may arise in 5G networks and propose countermeasures to mitigate them. The paper Identified security threats in 5G networks, including issues related to authentication, encryption, and privacy. Proposed countermeasures to mitigate these threats, such as using stronger authentication methods, implementing end-to-end encryption, and enhancing network segmentation. Analyzed existing security features in 5G networks and highlighted areas that need improvement. Discussed the impact of emerging technologies, such as

edge computing and IoT, on 5G security. The study was conducted using a systematic review approach. The authors searched various academic databases and industry reports for relevant studies on 5G security. They analyzed the studies using a qualitative content analysis method to identify common themes and patterns related to security threats and countermeasures. The objective of the research is to identify security threats in 5G networks and propose countermeasures to mitigate them. The methodology used for the research is a systematic review approach. The authors searched various academic databases and industry reports for relevant studies on 5G security. They analyzed the studies using a qualitative content analysis method to identify common themes and patterns related to security threats and countermeasures. No algorithm was developed in this research study. The result obtained includes the identification of security threats in 5G networks, proposed countermeasures to mitigate these threats, and highlighted areas that need improvement. The paper also discussed the impact of emerging technologies, such as edge computing and IoT, on 5G security. However, the research study did not conduct any empirical analysis of the proposed countermeasures, and it did not include a discussion of the economic feasibility of implementing the proposed solutions. Also, the research did not evaluate the effectiveness of the proposed countermeasures. Future work may involve evaluating the effectiveness of the proposed countermeasures and analyzing the potential impact of emerging technologies on 5G security. Additionally, further research may focus on the development of new security protocols to enhance 5G security and exploring the economic feasibility of implementing the proposed solutions. The authors also suggested collaboration among different stakeholders to ensure the security of 5G networks.

Vasilakos *et al.* (2020) conducted a systematic review of literature and analysis of security and privacy features in 5G networks. The aim of the study was to identify security and privacy challenges that may arise in 5G networks and propose solutions to address them. The study was conducted using a systematic review approach. They analyzed the studies using a qualitative content analysis method to identify common themes and patterns related to security and privacy challenges and proposed solutions. They Identified security and privacy challenges in 5G networks, including issues related to authentication, access control, and data protection. Proposed solutions to address these challenges, such as using multi-factor authentication, implementing network slicing for better access control, and using data anonymization techniques for better data protection. Analyzed existing security and privacy features in 5G networks and highlighted areas that need improvement. Discussed the impact of emerging technologies, such as blockchain and AI, on 5G security and privacy. The main objective of the research is to identify security and privacy challenges that may arise in 5G networks and propose solutions to address them. Additionally, the paper aims to analyze existing security and privacy features in 5G networks and highlight areas that need improvement. The methodology used for the research is a systematic review approach. The authors searched various academic databases and industry reports for relevant studies on security and privacy in 5G networks. They analyzed the studies using a qualitative content analysis method to identify common themes and patterns related to security and privacy challenges and proposed solutions. The paper did not mention the development of any new specific algorithm. The result obtained includes the identification of security and privacy challenges in 5G networks, such as issues related to authentication, access control, and data protection. The paper proposed solutions to address these challenges, such as using multi factor authentication, implementing network slicing for better access control, and using data anonymization techniques for better data protection. The paper also analyzed existing security and privacy features in 5G networks and highlighted areas that need improvement. The authors discussed the impact of emerging technologies, such as blockchain and AI, on 5G security and privacy. However, the research study did not evaluate

the effectiveness of the proposed solutions, and there is a need for further research on the integration of security and privacy in 5G network architecture. Additionally, the paper did not discuss the potential ethical and legal implications of the proposed solutions. The future work suggested includes evaluating the effectiveness of the proposed solutions and analyzing the potential impact of emerging technologies on 5G security and privacy. The paper also highlighted the need for collaboration among different stakeholders, including network operators, device manufacturers, and regulatory bodies, to ensure the security and privacy of 5G networks.

Kaloxylos & Kambourakis (2021) proposed enhancing 5G security through intelligent traffic profiling. They carried out the Experimentation and analysis of traffic profiling techniques in 5G networks. Identified the effectiveness of intelligent traffic profiling in enhancing 5G security. The objective of the research is to propose enhancing 5G security through intelligent traffic profiling and to identify the effectiveness of this approach. The methodology used for the research is experimentation and analysis of traffic profiling techniques in 5G networks. The paper proposes the use of intelligent traffic profiling for enhancing 5G security. The result obtained is the identification of the effectiveness of intelligent traffic profiling in enhancing 5G security. However, the research study does not provide detailed information on the experimentation and analysis methodology used or the specific techniques of intelligent traffic profiling used in the experiment. The future work includes further research on the application of intelligent traffic profiling for enhancing 5G security in more complex and diverse 5G environments. Additionally, the paper suggests exploring the integration of intelligent traffic profiling with other security mechanisms to further enhance 5G security.

Lim *et al.* (2021) conducted a comprehensive review of the existing literature on 5G security threats and countermeasures. The aim of the study was to analyze various attack scenarios and propose countermeasures to address them. The authors searched various academic databases and industry reports for relevant studies on 5G security. They analyzed the studies using a qualitative content analysis method to identify common themes and patterns related to security threats and proposed countermeasures. Identified various security threats to 5G networks, including issues related to authentication, privacy, and data protection. Analyzed attack scenarios, such as denial-of-service attacks, eavesdropping, and man-in-the-middle attacks, and proposed countermeasures to address them. More so, they Proposed countermeasures to enhance 5G security, such as implementing secure key management, enhancing network segmentation, and using secure boot mechanisms. Analyzed existing security features in 5G networks and highlighted areas that need improvement. The objective of the research is to propose enhancing 5G security through intelligent traffic profiling and to identify the effectiveness of this approach. The methodology used for the research is experimentation and analysis of traffic profiling techniques in 5G networks. The paper proposes the use of intelligent traffic profiling for enhancing 5G security. The result obtained is the identification of the effectiveness of intelligent traffic profiling in enhancing 5G security. However, the research study does not provide detailed information on the experimentation and analysis methodology used or the specific techniques of intelligent traffic profiling used in the experiment. The future work includes further research on the application of intelligent traffic profiling for enhancing 5G security in more complex and diverse 5G environments. Additionally, the paper suggests exploring the integration of intelligent traffic profiling with other security mechanisms to further enhance 5G security. Finally, The authors suggested that further research is needed to evaluate the effectiveness of the proposed countermeasures and to analyze the potential impact of emerging technologies, such as edge computing and IoT, on 5G securities. They also recommended that future studies should focus on developing new security protocols to enhance 5G security. Additionally, the paper highlighted the need for collaboration among different stakeholders,

including network operators, device manufacturers, and regulatory bodies, to ensure the security of 5G networks. In addition, they also suggested that future research should focus on developing automated security solutions to detect and mitigate attacks in real-time, which is a key motivation for this research studies.

3.0 Proposed Scheme

The Enhanced Cybersecurity Framework is designed to safeguard the Nigerian Oil and Gas Industry's critical infrastructure during the adoption of 5G networks. This scheme integrates advanced cybersecurity practices and technologies tailored to the unique challenges posed by 5G integration, ensuring the resilience and security of operations respectively. The proposed scheme proposed a ten step procedural algorithm that successfully helped in safeguarding the Nigerian oil and gas industry effectively as follows.

Step 1: Risk Assessment and Threat Modeling the scheme Identify and assess potential cyber threats and vulnerabilities posed by 5G integration and Analyze the specific risks to critical infrastructure components in the oil and gas sector.

Step 2: Adaptive Access Control Management the scheme Develop an adaptive access control system that dynamically adjusts access permissions based on user roles, device characteristics, and operational context and Implement continuous authentication mechanisms, such as biometric verification, to ensure authorized personnel access.

Step 3: Traffic Analysis and Anomaly Detection the scheme Deploy Deep Packet Inspection (DPI) and traffic analysis tools to monitor data flows within the 5G network as well as Develop machine learning algorithms to detect anomalous patterns in network traffic that may indicate cyberattacks.

Step 4: Blockchain-based Data Integrity, the scheme Implement blockchain technology to ensure data integrity in real-time monitoring and communication processes while creating an immutable and transparent record of data exchanges, enhancing trust and accountability.

Step 5: Encrypted Communication Channels, the scheme Establish end-to-end encrypted communication channels between critical infrastructure components and external stakeholders, Utilizing robust encryption protocols to prevent unauthorized access and eavesdropping.

Step 6: Multi-Layered Intrusion Detection and Prevention System (IDPS), the scheme Deploy an IDPS with multiple layers of defense, including network, host, and application-based intrusion detection mechanisms; Integrate anomaly-based and signature-based detection to identify known and novel cyber threats respectively.

Step 7: Security Information and Event Management (SIEM) Integration, the scheme Integrate SIEM tools to collect, correlate, and analyze security events and incidents across the 5G-enabled infrastructure while Enabling real-time threat detection and response by aggregating data from various sources.

Step 8: Continuous Monitoring and Incident Response, the scheme Establish a 24/7 Security Operations Center (SOC) to monitor system behavior and promptly respond to emerging threats and Develop incident response playbooks to guide the mitigation of security incidents.

Step 9: Employee Training and Awareness, the scheme Conduct regular cybersecurity training for employees to enhance their understanding of potential risks and best practices as well as Foster a culture of cybersecurity awareness and vigilance among all personnel.

Step 10: Regular Security Audits and Penetration Testing, the scheme Conduct routine security audits to assess the effectiveness of the S5G-OGI scheme and identify areas for improvement and

perform penetration testing to simulate cyberattacks and validate the scheme's resilience as well. The proposed Enhanced Cybersecurity Framework, implemented through the Secure 5G-Enabled Oil and Gas Infrastructure algorithm, addresses the potential security risks arising from the integration of 5G networks into critical infrastructure. This scheme provides a comprehensive approach to safeguarding the Nigerian Oil and Gas Industry's operations, ensuring a secure and seamless transition to 5G technology in the digital era. To be more precise the proposed algorithm is given in Algorithm 1 as follows:

Algorithm 1: Secure 5G-Enabled Oil and Gas Infrastructure (S5G-OGI)
Step 1: Risk Assessment and Threat Modeling
Step 2: Adaptive Access Control Management
Step 3: Traffic Analysis and Anomaly Detection
Step 4: Blockchain-based Data Integrity
Step 5: Encrypted Communication Channels
Step 6: Multi-Layered Intrusion Detection and Prevention System (IDPS)
Step 7: Security Information and Event Management (SIEM) Integration
Step 8: Continuous Monitoring and Incident Response
Step 9: Employee Training and Awareness
Step 10: Regular Security Audits and Penetration Testing

Program 1

```
class SecureOilAndGasInfrastructure:
    def __init__(self):
        self.access_control = {}
        self.network_traffic = []
        self.blockchain = {}
        self.encrypted_channels = {}
        self.intrusion_detection = {}
        self.security_events = []
        self.employees = []
        self.security_audits = []

    def risk_assessment(self):
        # Perform risk assessment and threat modeling
        # Identify potential cyber threats and vulnerabilities
        # Update threat database

    def adaptive_access_control(self, user, device):
        # Check user roles and device characteristics
        if user in self.access_control and device in self.access_control[user]:
            return True
        return False

    def traffic_analysis(self, data):
        # Analyze network traffic and detect anomalies
```

```
        # Add data to network_traffic list

    def blockchain_data_integrity(self, data):
        # Store data in blockchain for data integrity
        # Update blockchain dictionary

    def encrypted_communication(self, sender, receiver, message):
        # Encrypt and send message through encrypted channel
        if sender in self.encrypted_channels and receiver in self.encrypted_channels:
            encrypted_message = encrypt(message)
            return encrypted_message
        return None

    def intrusion_detection(self, data):
        # Perform multi-layered intrusion detection
        # Update intrusion_detection dictionary

    def siem_integration(self, event):
        # Integrate security information and event management
        self.security_events.append(event)

    def continuous_monitoring(self):
        # Continuously monitor security events
        # Trigger incident response if necessary

    def employee_training(self, employee):
        # Provide cybersecurity training to employees
        self.employees.append(employee)

    def security_audits(self):
        # Conduct regular security audits
        # Update security_audits list

    def penetration_testing(self):
        # Perform penetration testing
        pass

# Example usage
infrastructure = SecureOilAndGasInfrastructure()

# Step 1: Risk Assessment and Threat Modeling
infrastructure.risk_assessment()

# Step 2: Adaptive Access Control Management
user = “admin”
```

```
device = “mobile”
access_granted = infrastructure.adaptive_access_control(user, device)
if access_granted:
   print(“Access granted.”)
else:
   print(“Access denied.”)

# Step 3: Traffic Analysis and Anomaly Detection
data = “sensitive data”
infrastructure.traffic_analysis(data)

# Step 4: Blockchain-based Data Integrity
infrastructure.blockchain_data_integrity(data)

# Step 5: Encrypted Communication Channels
sender = “user1”
receiver = “user2”
message = “Hello, secure communication!”
encrypted_message = infrastructure.encrypted_communication(sender, receiver, message)
if encrypted_message:
   print(“Encrypted message:”, encrypted_message)
    # ... and so on for the remaining steps.
```

In the proposed Enhanced Cybersecurity Framework for 5G-Integrated Oil and Gas Industry a basic implementation of the proposed algorithm in Python programming language is implemented in program 1 above in a well-structured simplified manner. However, for a complete and effective solution. We will need to implement the specific details and functions for each step, for example integrate external libraries where necessary (e.g., for encryption), and possibly incorporate real-time monitoring and responses respectively.

4.0 Conclusion

The rapid progression of technology, particularly the incorporation of fifth-generation (5G) wireless networks, has brought forth unparalleled possibilities and complexities in diverse industries. Among these includes, the oil and gas sector, which is presently a cornerstone of global economies, demands advanced strategies to ensure the protection of its critical infrastructure. As technological advancements persist, proactive security measures stand crucial in mitigating risks and bolstering the foundation of this indispensable sector. This paper introduces a comprehensive strategy to address the security implications arising from the integration of 5G networks into the oil and gas industry. The strategy emphasizes safeguarding operations through an Enhanced Cybersecurity Framework. In line with this scheme, an extensive review of pertinent literature was conducted, probing the potential impacts of 5G integration on the industry’s online security. Drawing from this inquiry, a multifaceted algorithm named Secure 5G-Enabled Oil and Gas Infrastructure (S5G-OGI) was proposed. The S5G-OGI algorithm delineates ten distinctive stages, including risk evaluation, adaptive access control, traffic scrutiny, blockchain-enabled data integrity, encrypted communication, intrusion detection,

integration with Security Information and Event Management (SIEM), perpetual surveillance, employee training, and systematic security assessments. To demonstrate the practicability of this algorithm, Python programming was employed. While the code's implementation serves as a demonstrative illustration, it underscores the technical viability of the framework. Overall, the proposed scheme underscores the imperative of securing the critical infrastructure of the oil and gas industry amidst the transition to 5G networks. By amalgamating exhaustive literature scrutiny, a meticulously crafted algorithm, and tangible Python-based implementation was proposed, the proposed Enhanced Cybersecurity Framework provides a roadmap to guarantee operational resilience, integrity, and security as the oil and gas industry embarks on the dynamic journey of 5G integration.

References

Abbas, F., Song, H., Saba, S., Ali, A., Yasin, A., Umair, M., & Qureshi, M. I. (2020). A Comprehensive Survey of 5G Security and Privacy Challenges and Solutions.

Ajadi, M. O., Ogunleye, O. D., & Adeosun, O. O. (2020). 5G security: Threats, requirements and challenges. *Journal of Information Security and Applications*, 54, 102583.

Alshamrani, M., Li, F., Wang, L., & Jiang, Y. (2020). 5G security: a survey of threats and solutions. *Journal of Network and Computer Applications*, 168, 102747. https://doi.org/10.1016/j.jnca.2020.102747

Alshammari, H., Al-Dhief, F. T., Alshammari, N. A., & Almutairi, A. M. (2020). 5G security: a review of threats and solutions. *Security and Communication Networks*, *2020*, 1-17. https://doi.org/10.1155/2020/8844210

Alshamrani, M., Alharbi, R., & Almogren, A. (2020). 5G security: A survey of threats and solutions. *International Journal of Advanced Computer Science and Applications*, 11(3), 146-152.

Alshammari, H., Almutairi, A., & Alshammari, B. (2020). 5G security: A review of threats and solutions. *Journal of King Saud University-Computer and Information Sciences*, 32(6), 731-738.

Kaloxylos, A., & Kambourakis, G. (2021). Enhancing 5G security through intelligent traffic profiling. IEEE *Transactions on Network and Service Management*, 18(1), 179-193

Lim, J. T., Kim, D. J., Lee, S. J., & Lee, D. H. (2021). 5G Security: Threats and Countermeasures.

Olorundare, J. K., Olorundare, A. O., & Sayyadi, S. (2017). Internet of things Prospect in Nigeria: Challenges and Solutions. 2017 IEEE 3rd *International Conference on Electro-Technology for National Development (NIGERCON).*

Park, S., Kim, D., Park, Y., Cho, H., Kim, D., & Kwon, S. (2021). 5G Security Threat Assessment in Real Networks. *Sensors*, 21, 5524. https://doi.org/10.3390/s21165524.

Sullivan, S., Brighente, A., Kumar, S. A. P., & Conti, M. (2021). 5G Security Challenges and Solutions: A Review by OSI Layers. *IEEE Access*, 9, 84604-84625. https://doi.org/10.1109/access.2021.3087684

Vasilakos, A. V., Kaloxylos, A., & Kambourakis, G. (2020). Secure and privacy-preserving 5G communications: A survey. IEEE *Transactions on Network and Service Management*, 17(4), 1872-1895.

Li, F., Qiu, M., & Wu, Y. (2020). 5G security: Analysis of threats and solutions. IEEE *Access*, 8, 21800-21809.

Li, F., Wang, X., Wang, L., & Jiang, Y. (2020). 5G security: analysis of threats and solutions. Wireless Communications and Mobile Computing, 2020, 1-12. https://doi.org/10.1155/2020/8832434

Wang, Y., Gao, X., & Wang, Y. (2021). Privacy-preserving 5G network slicing: Issues and challenges. IEEE *Wireless Communications*, 28

Li, Y., & Wang, X (2021). Blockchain-based secure and trustworthy 5G network slices. IEEE *Transactions on Network and Service Management*, 18(2), 524-536.

Gudu, E. B. Wisdom, D. D. Gudu, G. J. Ahmad, M. A. Isaac. S. Akinyemi, A. E. (2020). Data Science for Covid-19 (Mathematical Recipe for Curbing Corona Virus (Covid- 19) Transmission Dynamics, *Elsevier*, August, 2021.

Kim, J., & Kang, J. (2020). 5G security: Threats and countermeasures. IEEE *Wireless Communications*, 27(4), 36-43.

Khan, J. A., & Chowdhury, M. M. (2021, May). Security Analysis of 5G Network. In 2021 International Conference on Emerging Trends in Information Technology (EIT) (pp. 1-5). IEEE. https://doi.org/10.1109/EIT51626.2021.9491923.

Wisdom, D. D., Tambuwal, A. Y., Khalid, H., Ajayi, E. A., & Chun, P. B. (2018). Enhanced model for computer viruses counter measures. In 1st International Conference on Education and Development (ITED), Baze University, Abuja Nigeria.

Gudu, E. B. Wisdom, D. D. Ahmed, M. A Akinyemi, A.E. Isaac, S. Dazi, A. J. (2020). Mathematical model for the spread and control of ebola virus by quarantine techniques, Anals Journal of computer science series, November, 2021.

Wisdom, D.D. Ajayi E. A. Arinze U.C. Idris, H. Bello, U.M. Aladesote O.I. (2021). An Optimized TWIN Battery Resource Management Scheme in Wireless Networks, Lecture Notes in Networks, Vol. 217, *Proceedings of Sixth International Congress on Information and Communication Technology, Springer Nature*, 2021. 978-981-16- 2101-7,511607.