Quantum Secure and Resilient 5G Network Slicing

Asi Kuushalie
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22204@bl.students.amrita.edu

C V Sree Pranavi
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22216@bl.students.amrita.edu

Velumury Varshita
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
bl.en.u4cse22264@bl.students.amrita.edu

Shinu M Rajagopal
Department of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
mr_shinu@blr.amrita.edu

***Abstract*—5G is a fifth-generation mobile network that provides efficient wireless communication over the previous generation. It provides faster data speeds, lower delays, and more capacity to connect with many devices simultaneously. In this work, network slicing in 5G networks is discussed with regard to security measures which include QKD(Quantum Key Distribution) and PQC(Post-Quantum Cryptographic). It allows for the formation of numerous granular and independent virtual networks based on a shared physical network. The model explores security where QKD keys address links and encompass PQC to counter other quantum technology threats in the future. Furthermore, there are reliability measures introduced, including route adjustments, with a self-repairing capability for link failure in multi-slice networks. In this approach, the security and reliability features are incorporated in 5G network slicing to address the delivery of the services in the next-generation networks.**

***Index Terms*—Network slicing, QKD, PQC, link failure, self-healing**

I. Introduction

5G technology otherwise known as the 5th generation of mobile communication technology system and offers higher data rate, lower latency, and far more capacity than before. This technology underpins many diverse complex applications including autonomous driving, smart cities, IoT, and the ability to make high bandwidth, real-time connections between devices.

Network slicing is one of the central tenets of 5G wherein multiple instances of the network (slices) can be designed on top of a single hardware layer. Every slice is personalized with the objective of giving the application or service, high bandwidth, for instance, to support videos or low latency to support games. This flexibility optimizes 5G networks and also improves the usability of devices by directing network resources most efficiently possible to types of services. Network slicing make it possible that the operators can effectively allocate the resource and provide network services for various applications.

Quantum Key Distribution (QKD) is a secure way of sending keys for encryption. It uses quantum mechanics to allow two parties, denoted by Alice and Bob to establish a secure channel and exchange an encrypted key. Among others, there are two main fundamental features, that make BB84 protocol secure the quantum uncertainty, which is inherent in any measurement process, and the no-cloning theorem, which states that one cannot make a copy of an arbitrary unknown quantum state. This feature brings the ability to eavesdrop on the knowledge of other members of the group because any act of intercepting the key causes the state of the system to change.

Post-quantum cryptography (PQC) refers to cryptographic algorithms that cannot be vulnerable to quantum computing attack that is a threat to conventional cryptographic techniques. As the quantum computing performance continues to improve, the data is protected by using symmetric encryption called Advanced Encryption Standard(AES) to maintain the security of the network slices.

Self-healing in network systems is an aspect of overall network security, which requires recognizing anomalies or intrusions and making corrections on its own accord without the need for intervention. In 5G network slicing, this feature enhances resilience by allowing the network to automatically recover from issues, maintaining continuity and reliability.

Network slicing is done where the nodes are the network slice components like the routers or the servers. Every slice possesses links (ports) of unique weight regarding quality characteristics such as bandwidth or latency [1]. QKD keys are created for nodes to encrypt their messages safely and PQC provides an additional layer of encryption for the data. The self-healing mechanisms allow them to respond to any problems in the network and redundancy and failover prevent the network from going down. By emulating the slices of the network, resources can be designed to allocate specifically to what an application needs.

This project brings the network slices in addition to robust security assurances to ensure that the communications are only safe against current threats including potentially even quantum computers in the future [2]. Moreover, such a system can self-diagnose the problem and start to rectify it even before human intervention is sought thus making the system very reliable. This project is relevant and helpful to establish the current demand for diverse and dependable networks in numerous industries and to be more ready for the development of technology in the future.

The Key contributions of this work are :

- Implementation of 5G network slicing
- Integration of Security mechanisms:
  Quantum Key Generation using BB84 protocol
  Post-Quantum Cryptography using Advanced Encryption System-256.
- Self-Healing mechanism for the network resilience
- Visualized 5G network slices

The subsequent sections of this paper give an overview of the research and its contributions. Section II discusses related works, evaluating the existing solutions in the 5G network slicing solutions, security measures, and self-healing systems, while also identifying the gaps and challenges. Section III represents the sequential approach and the overall planning of the paper. Section IV presents the results, it demonstrates the efficacy of network slicing, the stability of the security features, and the active self-healing mechanism. Section V presents the conclusion of the paper by summarizing the findings as well as possible areas for future research.

II. Related Works

The study offers a methodology for employing virtual network functions (VNF) to manage network slicing in 5G. For effective resource allocation and quality of service in 5G networks, the suggested methodology tackles the three fundamental facets of network slicing: creation, isolation, and administration [3]. The authors suggest a three-stage method: Making slices with a machine Acquiring the ability to categorize network requirements, Slice isolation using multi-criteria decision-making-based resource allocation, Using resource transfer, and slice management allows resources to be dynamically adjusted. By employing these strategies, the framework hopes to increase network slicing's effectiveness and versatility while meeting the demands of various 5G applications with varying performance requirements. According to simulation studies, the framework improves network service request acceptance rates and resource usage, offering a scalable solution for 5G network management.

The paper explores the evolution from 4G to 5G, highlighting advanced services like AR/VR and Mission Critical applications, with Open RAN and network slicing enabling Ultra Reliable Low Latency Communication [4]. It introduces a framework for ultra-low latency in 5G, especially for Smart Cities and IIoT, and discusses the role of Software Defined Networking (SDN) and Network Function Virtualization (NFV) in enabling Latency-as-a-Service.

the paper address the issues of resource allocation based on service characteristics of 5G network slicing, such as ultra-reliable low-latency communications (uRLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC) [5]. They put particular emphasis on the challenges with resource efficiency, low latency, and security that face network slicing in light of advances such as those reported by the International Telecommunication Union (ITU) and the Next Generation Mobile Networks (NGMN) Alliance, positing machine learning as a viable solution to the problems surrounding management. Their heuristic fuzzy approach-based node and link mapping is shown to outperform Nearest Neighbor Ranking (NNR), Closeness-based Node Ranking (CN), and VIKOR algorithms. The framework achieves the best possible QoS on a basis of dynamic infrastructure.

The methods of synchronization that are pivotal and of serious consideration in 5G by Rajagopal and Raj include frequency alignment and phase synchronization [6]. The most significant algorithms, such as Cristian's, Network Time Protocol and Precision Time Protocol are discussed with respect to their criticality in meeting 5G high demands. They consider the 4G issues with regards to energy use and spectrum and propose a 5G synchronization architecture to ameliorate latency and data rates. In future directions, in synchronization with Network Function Virtualization (NFV) and Software-defined Networking (SDN), they envisage a more integrated approach.

The emergence of possibilities for building dedicated logical networks enables the use of Network Slicing, which is essential for serving different types of 5G applications through Software Defined Networking (SDN) and Network Function Virtualisation (NFV) [7]. Resource allocation, fault management, and security issues in slice instantiation are tackled with the help of AI and machine learning algorithms. Still, the balance between the desired slice isolation and resource efficiency utilization remains a problem. The study focuses on the optimization of slices in order to better cope with the increasing interconnected devices and the growing complexity of the beyond 5G networks.

The work examines Beyond 5G (B5G) network slicing in the context of smart cities by considering specific parameters and issues [8]. It relates smart city applications to other verticals such as industrial IoT and stress the need for more detailed studies. The significance of 3GPP standards is of utmost importance in performing the function of unifying technological platforms and optimizing resources. AI and ML are studied for improving dynamic resource allocation and Quality of Service (QoS). The research outlines the technical barriers and recommends course of future studies aimed at the improvement of B5G network slicing in smart cities.

The paper addresses the issues related to resource allocation and Quality of Service (QoS) in network slicing in the case of critical applications like healthcare [9]. Deployed key 5G services – Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC), and Massive Machine-Type Communications (mMTC) – are still

a join of separate spheres. Both Machine Learning (ML) and Reinforcement Learning (RL) are quite useful and easy to implement but most of the time forget about packet drop chances. Some augmentation of algorithms and improvement of wider performance parameters are needed for Beyond 5G optimization.

The study is done in 5G to create tailored virtual network slices for specific service needs to enhance resource efficiency [10]. With an appropriate network resource management strategy and optimal traffic prediction models, maximum performance would be achieved. Edge computing can help to reduce system latency, while leasing is optimized through dynamic prioritization using blockchain technology. Homomorphic encryption and secure multi-party computation remain on the agenda list for further research. Future studies will enlighten the consensus about quantum-resistant encryption and the impact of AI and quantum computing on the 5G security framework.

The paper enables technologies, design principles, and network slicing management focusing on radio access and core networks [11]. Another survey on the process of 3GPP standardization and challenges on enabling network slicing for 5G has been conducted. The paper will present a holistic taxonomy for network slicing in the fields of design principles, enablers, resource levels, service function chaining, physical infrastructures, and security [12]. This defines essential requirements for deploying smart services in 5G networks and identifies open research challenges, offering solutions as well as future research directions.

The study focuses on resource allocation algorithms and Multi-Agent Deep Reinforcement Learning (DRL) in the context of Cellular Vehicle-to-Everything (C-V2X) communication in 5G, suggesting strategies including energy efficiency optimization through latency reduction and joint resource allocation with power control [13]. Actor-critic learning algorithms can enhance D2D-enabled V2X device resource allocation while preserving the quality of service of both V2V and V2I users in 5G environments [14].

The above study explains the role that 5G network slicing plays in optimizing the allocation, QoS, and scalability for diverse applications. In this regard, the above research/techniques rely on VNFs, SDNs, and NFVs intending to provide an efficient and dynamic method for slice management. Custom and flexible designs will form an important point of adaptation for 5G services in the studies.

III. Methodology

The implementation starts by importing the required Python libraries: 'networkx', used for the manipulation of the graph and is helpful in creating and analyzing complex networks; 'matplotlib' is used for plotting the graph; 'cryptography' library used for secure key generation and encryption that is used to ensure safe communications in a network, 'qiskit' is a quantum computing library and runs quantum circuits 'numpy' for numerical operations and 'random' library is used for the random generation of the input parameters each time it is run.

Then the input parameters which are the number of slices, total number of nodes per slice, and minimum and maximum weights for nodes as well as for edges are given. A Graph G is initialized as a new graph using nx.Graph(), which will contain the nodes and edges in the network. then nodes are created by allocating them to slices respectively. Every node is labeled with a name (for example A, B, C) and possesses a random weight within the given set. When a node is added they are given attributes for weight and slice.

The implementation continues with the creation of the edges within each of the slices made of the nodes, where slice_num is the ID of the slice to make. It probabilistically decides whether to form an edge between two nodes and the threshold for this probability is random. Some random weights that were generated were assigned to the edges and the colors of the edges show the slice they belong to, Blue color for Slice 1, Green color for Slice 2, and Red color for Slice 3. Also, inter-slice edges are formed between the nodes which are black and belong to distinct slices, with less probability of connection. This leads to the formation of the network structure that emulates the 5G network slicing environment. In the 5G, network slicing is performed when multiple 'slices', or virtual networks, can be implemented on the same physical infrastructure with dedicated resources and capabilities to meet particular needs, The generated graph is represented by the use of Matplot lib, a Python graphical library. The nodes are simply the circles where the label gives information regarding the node name and node weight. Also, edge labels are used as the representation of the connection weights, and a graph is created showing the 5G network slicing.

Security features like the Quantum Key distribution generation are included, the BB84 protocol enables Alice and Bob to generate a secret key using quantum properties such as photons. When Alice sends quantum bits (qubits) to Bob, she randomly chooses how to prepare each qubit using one of two different methods, called bases: There is the Z-basis in which qubits are measured as either 0 or 1, and the X-basis, which measures qubits as an equal ratio of 0 and 1. Bob also randomly selects one of these bases to measure the qubits he obtains. As per quantum mechanics law, if an interceptor tries to measure the Qubits, it affects the Qubits, producing errors that can be detected. For these errors, Alice and Bob after transmission look into some of the bits in the measurement choices and the outcomes to check on the key and to ensure the security of the key.

Another feature called Post-Quantum Cryptography is integrated it uses Advanced Encryption Standard(AES) 256 in Galois Counter Mode (GCM) which is a symmetric encryption algorithm to encrypt and decrypt data. The PBKDF2 (Password-Based Key Derivatio Function 2) converts a dynamically generated QKD key into a strong encryption key. Salt is a random string that is attached to the derived key so that even if the key is reused the salt will make sure to attach a random string and make the key unique each time. IV is a unique value added to plaintext so that different cipher text is generated even if we use the same plaintext again. After

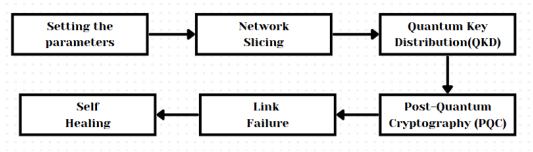

Figure 1: Block Diagram

encryption, decryption reverses the process using the same derived key, IV, and salt to get the original plaintext. AES-GCM mode provides confidentiality, integrity, and authenticity.

Reliability measures are also integrated which is shown by a function that shows the failure of an edge by taking it as an input removing it and checking if the rest of the graph is connected with the help of 'nx.is_connected()'. if the rest of the graph is still connected it finds other paths between the nodes or else considers it as a fragmentation of the network. the self-healing mechanism tries to reconnect broken parts of the network in case it gets disconnected because of a link failure. It checks the connectivity of the graph, if that is not the case, it finds the connected components using 'nx.connected_components()'. It chooses one node for each of the first two components and adds a new edge between them, making the network effectively reconnect as if nothing had happened to it. This self-healing mechanism is very fundamental to the unbroken service provisioning in a 5G network.

Figure 1 shows the overview of the project workflow from the initialization to the automated self-healing of failed network components. The process starts with the input parameter setting, in which all necessary variable configurations and key settings are set properly for the correct process running. Subsequently, the system applies network slicing, which creates segments of the network that can be customized for application or function, to optimize the use of resources. Following the network slicing, QKD is included for secure communication. To augment QKD, a principle of Post Quantum Cryptography, or PQC has been included, which provides protection against quantum computing threats by using mathematics that such computers cannot penetrate. For link failures which usually affect the performance of the network, the system has detected mechanisms for handling the failure. A unique feature that defined this project was the self-healing feature that was implemented into a system to enable it to self-repair and rectify problems affecting the network without assuming outside help.

RESULT

This work shows that 5G can perform highly complex tasks reliably, specifically in the context of network slicing, secure communication procedures, and self-repair functions. Through reproducing and mapping various components of the network including resources management, security, and fault tolerance, the research demonstrates how 5G networks can adequately meet the various application requirements while maintaining reliability and dependability. Each figure describes particular aspects of the system with emphasis on how it manages

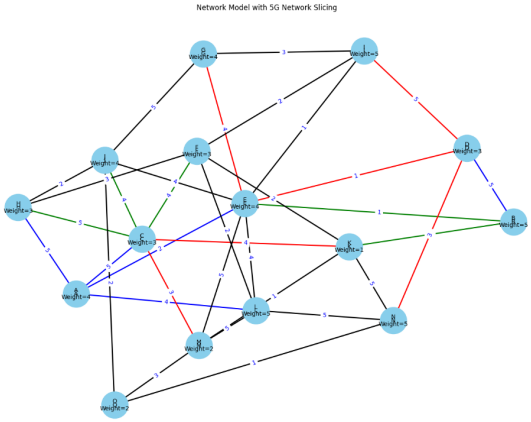

Figure 2: 5G network slicing

```
Link ('P', 'S'): BB84 QKD Key = 111101000
Link ('Q', 'S'): BB84 QKD Key = 110111101
Link ('R', 'X'): BB84 QKD Key = 101011010
Link ('S', 'T'): BB84 QKD Key = 000111011
Link ('S', 'V'): BB84 QKD Key = 011000010
Link ('S', 'W'): BB84 QKD Key = 001111110
Link ('T', 'V'): BB84 QKD Key = 000110101
Link ('V', 'W'): BB84 QKD Key = 110101110
Link ('W', 'X'): BB84 QKD Key = 100110010
```

Figure 3: Quantum Key Distribution result

resources, establishes and protects channel, responds to link failures, and pursues the path of self-recovery.

Figure 2 shows the result of a 5G network slicing that is randomly generated with nodes and edges. The circles in sky blue are nodes and each node represents a network function with some capacity and the weights reflect it. The strengths of connecting them are indicated through weights on edges. The lines drawn between these nodes depict the channels that enable interaction and the weight placed on the line depicts the robustness of the interaction channels. The following graph shows how the network slices can be formed, connected, and used for resource management in 5G networks and it shows how the slicing method is versatile and modular in its application.

Figure 3 shows the outcome of the simulation is to produce exclusive quantum keys for each of the connections between nodes in a network that are needed to ensure the security of the communications. For instance, in a network with nodes labeled 'A', 'B', 'C', etc., the keys produced for specific links might look like this: Link with A and C: BB84 QKD Key = 11011111, Link with A and E: BB84 QKD Key = 01100000, Link with B and D: BB84 QKD Key = 10111110. These pieces known as quantum keys, play a very crucial role in allowing nodes to ensure that all data exchanged between them is secure and this includes the security of the actual data and also the integrity of it. Another benefit of the keys is that they are essentially generated for each of the links, so, if one key is compromised, the others cannot be affected. The mentioned keys are generated dynamically making the system resistant to security threats such as eavesdropping.

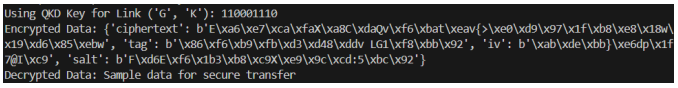

Figure 4: Post Quantum Cryptography result

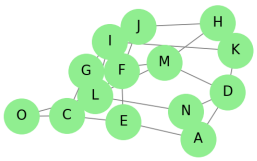

Figure 5: Network after link failure

Figure 4 shows data encryption using AES-256 bits in GCM mode encrypts the plaintext into ciphertext and can be decrypted using the correct key, salt, and IV. The salt ensures that every key generated is unique even if the same key is reused and IV ensures the same plaintext for different ciphertext. The PBKDF2 iterates over 100000 for the key derivation which makes it difficult for the attackers to hack and enhances security. The authentication tag ensures data integrity and detects any tampering during the transmission. In real-world deployments of can used in 5G-specific slices where several users and end devices are connected over the same physical layer these Quantum keys ensure end-to-end isolation and security preventing cyber-attacks and preserving privacy in mission-critical situations.

Figure 5 shows the link failure of the network by the removal of an edge which leads to the fragmentation of the network. This disrupts the working of the network and its functionality and the fact is that it remains a challenge to run such networks optimally, especially in systems such as 5G networks. The figure was introduced to demonstrate the drawbacks of networks, where even one link can have a critical impact on the performance.

Figure 6 shows a network after a self-healing mechanism. When an edge is removed, the nodes are dynamically reconstructed, and the network is enabled to work again, without external assistance. This graph focuses on the self-healing capabilities of the system to be able to support the service continuity of the 5G network. Through a continuous failure handling approach, the self-healing mechanism reduces the amount of time that the system is unavailable, improves dependability, and ensures that important network services are delivered without interruption.

All the above mechanisms when added up together showcase the advanced capabilities and the resilience of modern 5G networks. These features guarantee that the required performance will be supported in the case of failure, protect communications, and dynamism the failures in the 5G networks, making them highly robust and reliable. This kind of approach takes into consideration new requirements and difficulties of next-generation communication systems.

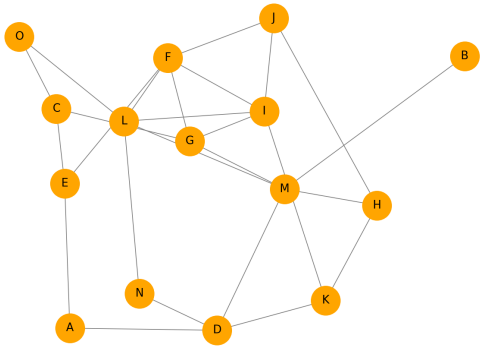

Figure 6: Network after self-healing

Conclusion

The project emulates 5G network slicing and offers detailed insight into how nodes with edges can represent the constitutive elements of network functionalities and their relations. This visualization shows how different vertical slices work in parallel within the essentially shared network manifestation while demonstrating that 5G networks are both scalable and efficient means of addressing heterogeneous user demands. Superior cryptographic mechanisms like Quantum Key Distribution are incorporated to promote security while in the network. Post-quantum cryptography (PQC) encrypts data to protect data from cyber theft risks. The work also focuses on the ability of 5G networks to handle dynamic changes through the integration of an automated self-healing feature. The self-healing mechanism allows mankind to serve the clients continually and keep the network strong without interruptions. Future work may examine the possibility of utilizing artificial intelligence for network slicing management. Extending the scope to 6G networks could also improve the system, by incorporating features for holographic communication and terahertz bandwidth so that security, scalability, and robustness principles are enhanced as the 6G networks are developed.

References

[1] **Lekshmi, S.S., Anjana, M.S., Nair, B.B., Raj, D. and Ponnekanti, S., 2019, March. Framework for generic design of massive IoT slice in 5G. In 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET) (pp. 523-529). IEEE.**

[2] **Srinivasan, T., Venkatapathy, S., Jo, H.G. and Ra, I.H., 2023. VNF-Enabled 5G Network Orchestration Framework for Slice Creation, Isolation and Management. Journal of Sensor and Actuator Networks, 12(5), p.65.**

[3] Sukumar, A., Singh, A., Gupta, A. and Singh, M., 2024, January. Enhancing security and privacy implications in 5G network slicing. In 2024 Fourth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-8). IEEE.

[4] Das, R.M., Sree, L.S., Ponnekanti, S. and Paunovic, M., 2019, November. Key enablers to deliver latency-as-a-service in 5G networks. In 2019 27th Telecommunications Forum (TELFOR) (pp. 1-4). IEEE.

[5] Mahmoud, H., Aneiba, A., He, Z., Tong, F., Guo, L., Asyhari, T., Wang, Z. and Gao, Z., 2024, March. Intelligent Network Optimisation for Beyond 5G Networks Considering Packet Drop Rate. In 2024 IEEE International Conference on Industrial Technology (ICIT) (pp. 1-6). IEEE.

[6] **Rajagopal, L. and Raj, D., 2017, October. Study of synchronization facets for 5G small cell use case scenario. In 2017 2nd International Conference on Communication and Electronics Systems (ICCES) (pp. 529-534). IEEE.**

[7] **Venkatapathy, S., Srinivasan, T., Jo, H.G. and Ra, I.H., 2023. An E2E Network Slicing Framework for Slice Creation and Deployment Using Machine Learning. Sensors, 23(23), p.9608.**

[8] Rafique, W., Barai, J., Fapojuwo, A.O. and Krishnamurthy, D., 2024. A survey on beyond 5g network slicing for smart cities applications. IEEE Communications Surveys & Tutorials.

[9] Thiruvenkadam, S., Sujitha, V., Jo, H.G. and Ra, I.H., 2022. A heuristic fuzzy based 5G network orchestration framework for dynamic virtual network embedding. Applied Sciences, 12(14), p.6942.

[10] Rahmanian, G., Shahhoseini, H.S. and Pozveh, A.H.J., 2021. A review of network slicing in 5G and beyond: Intelligent approaches and challenges. 2021 ITU Kaleidoscope: Connecting physical and virtual worlds (ITU K), pp.1-8.

[11] Khan, L.U., Yaqoob, I., Tran, N.H., Han, Z. and Hong, C.S., 2020. Network slicing: Recent advances, taxonomy, requirements, and open research challenges. IEEE Access, 8, pp.36009-36028.

[12] **Sree Lekshmi, S., Bandodkar, S.S., Vippalapalli, V., Susarla, A. and Ponnekanti, S., 2021. Data optimization-based security enhancement in 5G edge deployments. In Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2020 (pp. 347-362). Springer Singapore.**

[13] Akhter, J., Hazra, R., Mihovska, A. and Prasad, R., 2024. A Novel Resource Sharing Scheme for Vehicular Communication in 5G Cellular Networks for Smart Cities. IEEE Transactions on Consumer Electronics.

[14] **Enayati, M., Lekshmi, S.S., Toby, T., Prabhu, M., Rahul, K.P., Parvathy, S. and Ponnekanti, S., 2022. Blockchain-based location sharing in 5g open ran infrastructure for sustainable communities. In Intelligent Sustainable Systems: Selected Papers of WorldS4 2021, Volume 1 (pp. 571-585). Springer Singapore.**