COMMUNICATION TECHNOLOGIES FOR INTERNET OF THINGS

Abstract

Quantum and Internet of Things (IoT) technologies are driving transformative advancements across various industries, and their integration into drone communications presents promising opportunities for enhancing drone capabilities. This abstract explores the potential of leveraging quantum communication principles in IoT-based drone systems to address key challenges, such as security, data processing, and long-range connectivity. The conventional communication methods employed in drones often suffer from vulnerabilities, hindering the secure transmission of sensitive data. Quantum communication, with its inherent security features based on quantum key distribution and entanglement, offers a new paradigm for ensuring data integrity and confidentiality during drone operations. Furthermore, the exponential growth of IoT devices in drones generates massive amounts of data that require efficient processing and analysis. Quantum computing, with its immense computational power, has the potential to accelerate data processing in drone-based IoT applications, enabling real-time decision-making and resource optimization. Moreover, quantum-enhanced long-range communication can significantly extend the reach of drone networks, enabling seamless connectivity even in remote or challenging environments. Leveraging quantum entanglement for long-distance communication may enable efficient data exchange between drones and ground stations, leading to enhanced situational awareness and collaboration among drone fleets. Despite the promising prospects, several technical challenges need to be addressed in realizing quantum-enabled IoT communications in drones. These include integrating quantum communication modules into drone platforms, developing robust quantum algorithms for IoT data processing, and addressing issues related to quantum channel noise and coherence.

Keywords: Quantum, IoT, Drone, Autonomous System, Quantum key circulation, Quantum sensor networks, Quantum correspondence satellites

Authors

Atharsh JR
Computer Engineering
Presidency University
Bengaluru, India

Naren M
Computer science and Engineering
Presidency University
Bangalore, India

Karthik M H
Assistant Professor
Department of Civil Engineering
Presidency University
Bangalore, India

Nakul Ramana
Professor and HOD
Department of Civil Engineering
Presidency University
Bangalore, India

Shwetha A
Assistant Professor
Department of Civil Engineering
Presidency University
Bangalore, India

I. INTRODUCTION

The Internet is a structure made up of a network of networks that connects various sized networks, larger ones from fully functional autonomous systems (AS) that are economically operated to smaller ones of private or public organizations, through tens of thousands of gateways and router. Within this AS, communications are managed individually by each AS. Each restricted network typically. When specifically, these devices and their data as well as services move into the center of observation, it is frequently utilized to describe the umbrella of constrained networks and their devices as well as their connections. In these situations, the IoT gateway or router tends to have enough resources to handle sending traffic from one limited network to another. So, in contrast to many others, and.Therefore, a gateway falls within the classification of "resource-rich" devices in the IoT environment. Additionally, the foundation for safe internet of things connections is given by device-centric security features offered by the communication protocols in use. Human-to-human and human-to-device communication has both improved significantly all through time. Device to device communication becomes more and more crucial due to the deployment and use of devices of all kinds being so widespread. Today, many different kinds of gadgets either operate independently (for automation or control) or are connected to people (for interaction or monitoring). electronics, home appliances, health monitoring, intelligent vehicles, sensors and actuators are among these gadgets. These individually identifiable gadgets can connect to the Internet thanks to the Internet of Things (IoT) ecosystem, sothat they have the ability of sharing information with humans and among themselves. A sophisticated, huge, and quickly growing ecosystem enables universal, seamless device connection. [1]

II. EXISTING IOT COMMUNICATION TECHNOLOGY

Several communication protocols have been developed and are already in use, having been installed in numerous devices all over the world, even though there is currently no centralized location for IoT. Both fixed and short-range means of communication will be employed for the majority of connections, allowing Massive IoT and Critical IoT connectivity via standard cellular IoT or Low Power Wide Area Networks (LPWAN). LPWA technologies are well-suited for Internet of Things applications because to their distinctive attributes such as wide-area coverage, high energy efficiency, channel bandwidth, data throughput, and low power consumption. This technology is an example of the several ways that are currently being used to link sensors and controllers to the Internet without requiring human contact. of recent of modern cellular or Wi-Fi networks. Lora, Sig Fox, and Ingénue RPMA are merely a few of the cutting-edge technologies available. The current and future demand for Internet connectivity of "Things" has prompted cellular technology to develop its own IoT device connectivity landscape solutions, such as LTE Cat-M1 (also known as e MTC), EC-GSM-IoT, and NB-IoT (also known as LTE Cat-NB1), that will enhance and enable future IoT use cases. LPWA networks are currently being implemented for IoT applications such as smart cities, building management networks, asset monitoring, smart agriculture, and so on. This section quickly covers the essential elements of the most prevalent IoT technologies, which are divided into three categories: long-range networks, short-range networks, and cellular technology.

1. **Long-Range Networks:** It is, also known as wide-area networks (WANs), are communication networks that cover extensive geographical areas, often spanning across cities, regions, countries, or even continents. These networks are designed to facilitate data transmission and connectivity over long distances, allowing devices and users located far apart to communicate with each other. Unlike local area networks (LANs), which typically cover a limited physical area like a home, office, or campus, long-range networks are characterized by their ability to provide connectivity across large distances. These networks are crucial for connecting remote locations, enabling communication between geographically dispersed sites, and supporting applications that require broad coverage.

   - **Lora WAN:** Lora WAN operates in the unlicensed Industrial, Scientific, and Medical (ISM) bands, such as 868 MHz in Europe and 915 MHz in North America. It uses a modulation scheme called "Chirp Spread Spectrum" to achieve long-range communication and robustness against interference. One of the significant advantages of Lora WAN is its ability to provide long-range connectivity (up to several kilometers in rural areas and a few hundred meters in urban environments) while maintaining low power consumption. This makes it ideal for applications such as smart cities, environmental monitoring, asset tracking, agriculture, and industrial automation. However, it's essential to consider that Lora WAN's data rates are relatively low compared to other wireless technologies like Wi-Fi or cellular networks. As a result, it is best suited for applications that require intermittent communication of small data packets over long distances and can tolerate latency. Overall, Lora WAN has gained popularity as a reliable and cost-effective solution for various IoT and M2M applications that need long-range and low-power connectivity. [2]

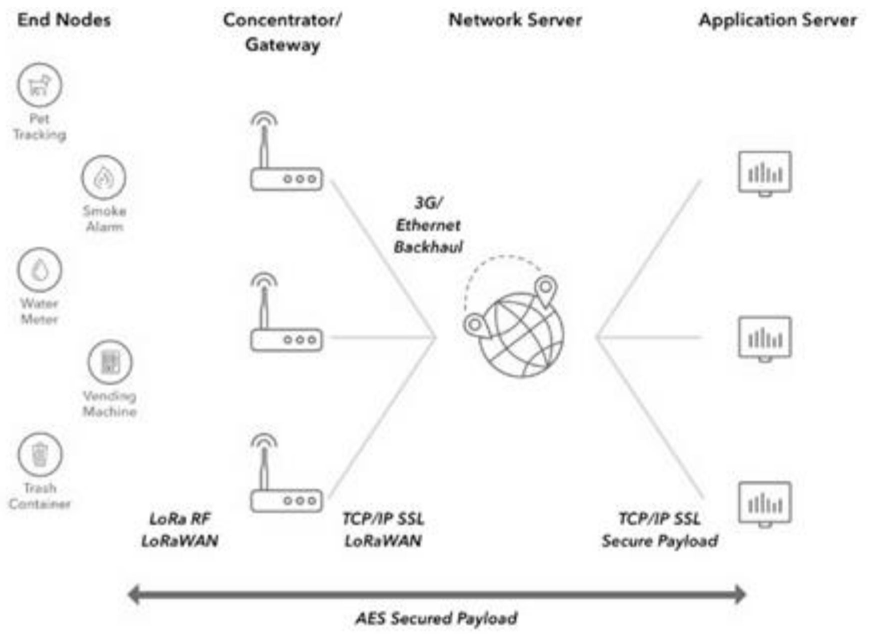

Figure 1: Lora wan Network Architecture (Tech journal.com)[3]

- **SIGFOX:** In the vast landscape of IoT communication technologies, an LPWAN (Low-Power Wide Area Network) technology empowers devices to communicate efficiently over long distances while consuming minimal power. Sigfox operates in unlicensed radio frequency bands, allowing for easy and cost-effective deployment of IoT solutions worldwide. With a unique approach to data transmission, Sigfox employs ultra-narrowband technology to send small data packets securely and reliably. This optimized method not only ensures extended battery life for connected devices but also enables seamless connectivity in challenging environments. Sigfox’s low-cost and low-energy consumption attributes make it a perfect fit for various applications, ranging from smart cities and industrial monitoring to asset tracking and environmental sensing. Its reach extends even to remote and rural areas, opening up new possibilities for IoT implementations in traditionally underserved regions. The simplicity and scalability of Sigfox's ecosystem have sparked innovation and rapid adoption across industries. Companies can now harness the power of IoT to improve efficiency, enhance sustainability, and drive transformative changes in their operations. In this ever-connected world, Sigfox emerges as a promising technology, empowering the Internet of Things to reshape the way we interact with devices and the environment. As we delve deeper into the IoT era, Sigfox's unique characteristics position it as a driving force behind the connected future we envision.

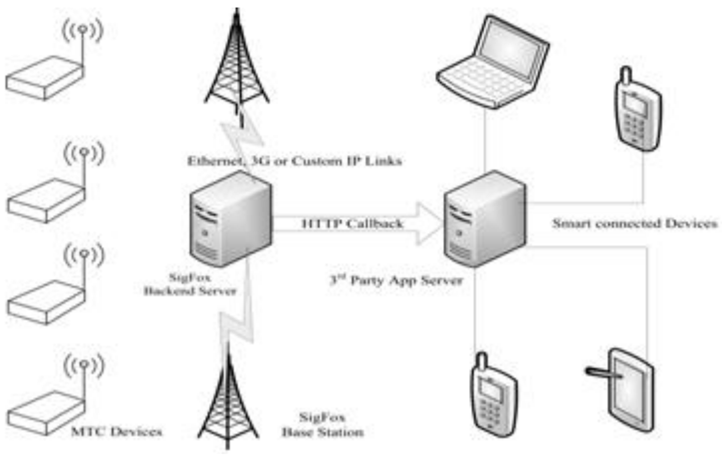

Figure 2: Sigfox(source: Research gate.com) [4]

- **DASH7:** Dash7 is a wireless communication protocol designed for low power, long-range IoT applications. It operates in the sub-GHz frequency bands, typically 433 MHz or 868 MHz, providing excellent range and penetration through obstacles. Dash7 is particularly well suited for remote and outdoor applications where low power consumption is critical for battery-operated devices to achieve long operational lifetimes. One of the key features of Dash7 is its ability to deliver reliable data communication even in challenging environments with high interference or noisy conditions. This makes it ideal for various applications such as smart agriculture, environmental monitoring, asset tracking, and industrial automation. With its focus on long battery life, robustness, and versatility, Dash7 has emerged as a valuable IoT communication technology, contributing to the growth and scalability of the Internet of Things ecosystem.

III. EMERGING IOT COMMUNICATION TECHNOLOGY: QUANTUM COMMUNICATION

A quantum mechanics-based correspondence framework that permits moment data exchanges. Not at all like radio waves restricted to light speed, quantum entrapment permits an exchange speed that is at present not quantifiable. Quantum correspondence is a new and emerging field that can possibly upset the manner in which we convey. Quantum correspondence involves the laws of quantum mechanics to send data in a secure and rugged manner. This makes it ideal for applications where security is paramount, like the IoT.

There are various emerging IoT correspondence advances that utilize quantum mechanics. Probably the most encouraging innovations include:

1. **Quantum key circulation** (QKD): QKD is a strategy for communicating an irregular key between two gatherings in a manner that is secure against snooping. This implies that the key can be utilized to encode information without fear of it being blocked or perused. The meaning of quantum is because of its better security and reliability over conventional key dispersion. Valuable cryptography strategies are utilized to send and test the old-style key appropriation. An old-style key circulation depends on registering intricacy and numerical conditions, and it utilizes symmetric and off-kilter essential dissemination methodologies separately. At the point when both the source and the beneficiary utilize a similar safe, secret, safeguarded key, symmetric techniques are utilized. Then again, the lopsided procedure offers a kept-up-to-date and secure public and confidential key. The confidential key is utilized to keep up with each party's authenticity and secrecy through correspondence. Those safety efforts were OK, and much of the time was utilized before Shor's calculation, which is a quantum cryptography approach intended to work on the security of any organization's association, was presented. Moreover, quantum was put forward as a powerful numerical cycle that would undermine RSA security. The Elliptic Bend Cryptography approach, which is predicated on giving lower key sizes with a similar RSA cryptographic strength, was likewise harmed by quantum's capacity to dodge the discrete logarithm issue. The quantum key dissemination, which depends on quantum mechanics and actual rationale, shows its dependability, protection of safety, and elevated degree of privacy by forestalling listening in and offering an exhaustive, unmistakable, and new idea on encryption systems. It very well may be considered an imaginative mechanical advance that advances an inventive technique for sending photon lights between the transmitter and the collector to make a protected association. The Heisenberg Vulnerability Standard and the quantum no-cloning hypothesis are the two significant standards of quantum mechanics on which quantum cryptography is fabricated. A few advantages of carrying out QKD have to do with the security that was implemented to supplant an unavoidably weak numerical calculation with secure correspondence. Moreover, the QKD is practically the quantum key conveyance, which depends on quantum mechanics and actual rationale, exhibits its steadfastness, protection of safety, and elevated degree of privacy by forestalling snooping and giving a complete, exceptional, and new idea for an encryption system. As portrayed in figure 3.

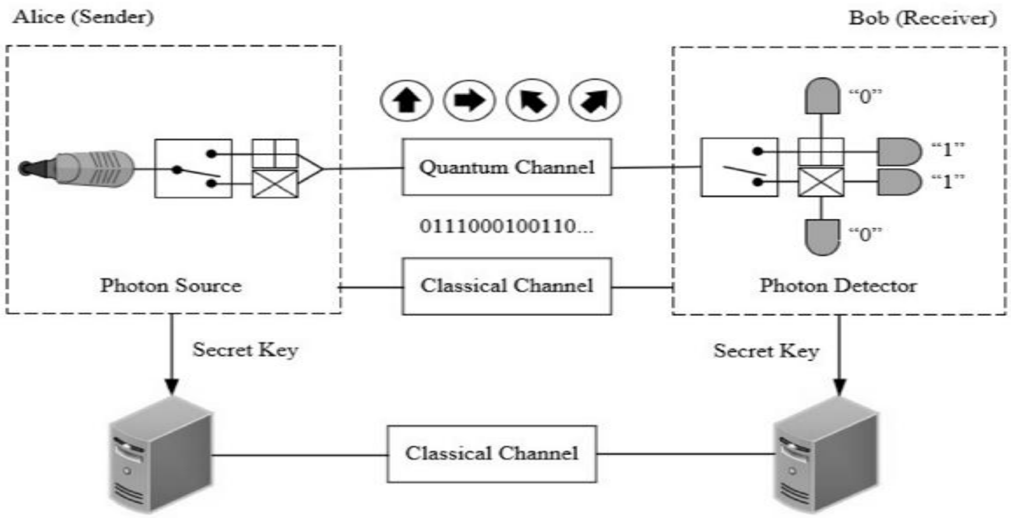

Figure 3: QKD [5]

2. **Quantum sensor networks**: Quantum sensor networks are a type of technological infrastructure that leverages the principles of quantum mechanics to provide ultra-precise measurements and detections. These networks use qubits, the basic units of quantum information, to process and transmit data with unprecedented accuracy and speed. Quantum sensor networks have a wide range of potential applications, from enhancing GPS systems to improving medical imaging and drug discovery. However, the development of such networks is still in its early stages, and requires significant advances in both hardware and software before it can be commercialized on a large scale. It uses quantum technology to detect and measure a range of physical properties such as temperature, magnetic and electric fields, and gravity. These networks consist of interconnected sensors that can communicate using quantum communication protocols, enabling secure communication and transmission of information. Quantum sensors have significant advantages over traditional sensors, including higher sensitivity, faster response times, and lower noise levels. They have the potential to revolutionize fields such as materials science, biology, medicine, and national security. However, further research is needed to develop more affordable and scalable quantum sensor networks. It has the potential to greatly improve sensing technologies and enable new applications such as more precise navigation, improved medical imaging, and more efficient and secure communication networks. The inherent nature of quantum mechanics allows these sensors to detect very minute changes in a system, making them highly accurate and sensitive. With the rapid development of quantum technologies, quantum sensor networks are becoming more viable and may revolutionize many fields in the future.

3. **Quantum correspondence satellites**: Quantum correspondence satellites are another sort of satellite that utilization quantum data to send secure interchanges. Not at all like conventional satellites, they use quantum signs to encode data, making it practically difficult to block or break. This innovation has critical applications in enterprises that require high-security correspondences, like monetary foundations, government organizations, and military tasks. With the rising interest for secure correspondences, the improvement of quantum correspondence satellites is probably going to turn into a basic

part of worldwide broadcast communications framework before very long. Correspondence satellites utilize the standards of quantum mechanics to trade secure data between focuses on the planet and in space. They use quantum key appropriation (QKD) innovation to produce and trade cryptographic keys that can't be caught or hacked, guaranteeing a definitive security of data being sent. QKD includes sending an irregular succession of photons over a fiber optic link, with the polarizations of the photons addressing the 1s and 0s of the key. As the collector estimates the photons, any endeavor to capture or notice them adjusts their polarization and alarms the source to the presence of a snoop.

These satellites use quantum entanglement to ensure that the information being transmitted cannot be intercepted or tampered with without detection. The technology is still in its initial stages, but it has the potential to revolutionize the way we communicate, particularly when it comes to financial and government transactions. Current quantum communication satellite projects include China's Micius satellite, which has successfully demonstrated quantum key distribution over long distances.

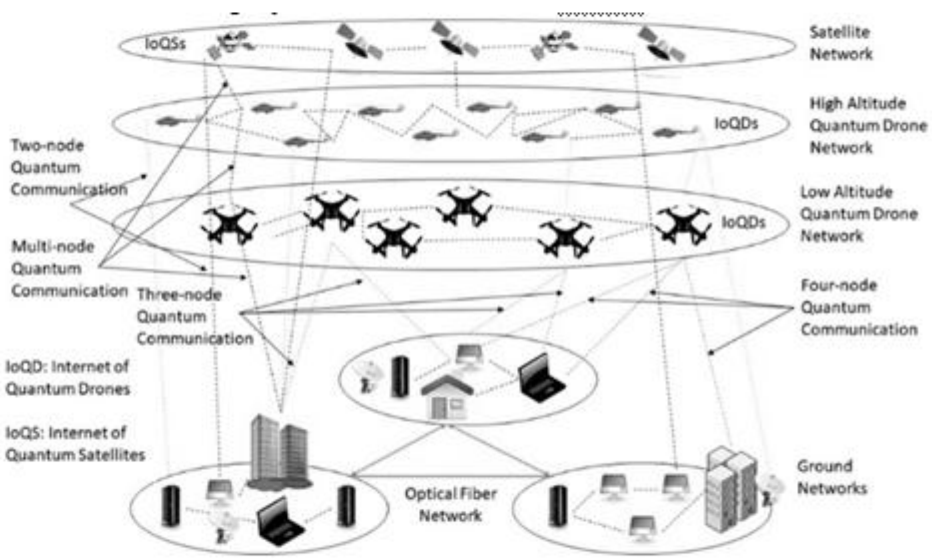

Figure 4: Quantum communication satellites (source:science direct.com)[6]

Some of the benefits of using quantum communication in IoT include:

- **Enhanced security:** Quantum communication is inherently secure, as it is based on the laws of quantum mechanics. This makes it ideal for applications where security is paramount, such as the IoT.
- **Increased bandwidth:** Quantum communication can hypothetically accomplish a lot higher data transfer capacities than conventional correspondence innovations. This could consider the transmission of a lot of information between IoT gadgets progressively.
- **Improved accuracy:** Quantum sensors can be used to measure physical quantities with unprecedented accuracy. This could lead to new applications for IoT, such as environmental monitoring and medical diagnostics.

IV. INTEGRATING QUANTUM COMMUNICATION IN DRONES AND IOT DEVICES

The low-power arrangements depended on IoT and had high accuracy in laying out the robot's situation. A couple of trial of long-range, low-power innovations that depended on the IoT pinpointing drone positions with outrageous accuracy were viable. The discoveries demonstrated that robot positions in regions where Wi-Fi and different advancements probably will not be accessible ought to be expeditiously detailed. For example, surveillance robots can use these IoT advancements to track down other severed drones in far or hazardous regions. As IoQDs networks develop, various continuous applications are additionally conceivable. Low power working utilization while keeping up with greatest awareness and observing is conceivable with quantum radars. However, hindrance shortcomings, abrogation calculation, and genuine examination of inactive space should be generally handled in ensuing review. Military and common uses of quantum radar frameworks are average. A trial on the all-inclusive portrayal of quantum radar cross-areas for complex articles with 3D math, like B2 airplane, additionally yielded positive outcomes. The quantum impedance that side curves of biostatic quantum radar cross-segments in dispersing much of the time display is an issue for the field, but. The goal would should be expanded past two-layered focuses in future examination to foster pragmatic application IoQDs networks in applications for traffic designing. The on-ground vehicle information will be traded with significant distance traffic the executives based information handling units with the help of multitudes of IoQDs. These gadgets can investigate traffic information and change vehicle courses to stay away from gridlocks. [7]

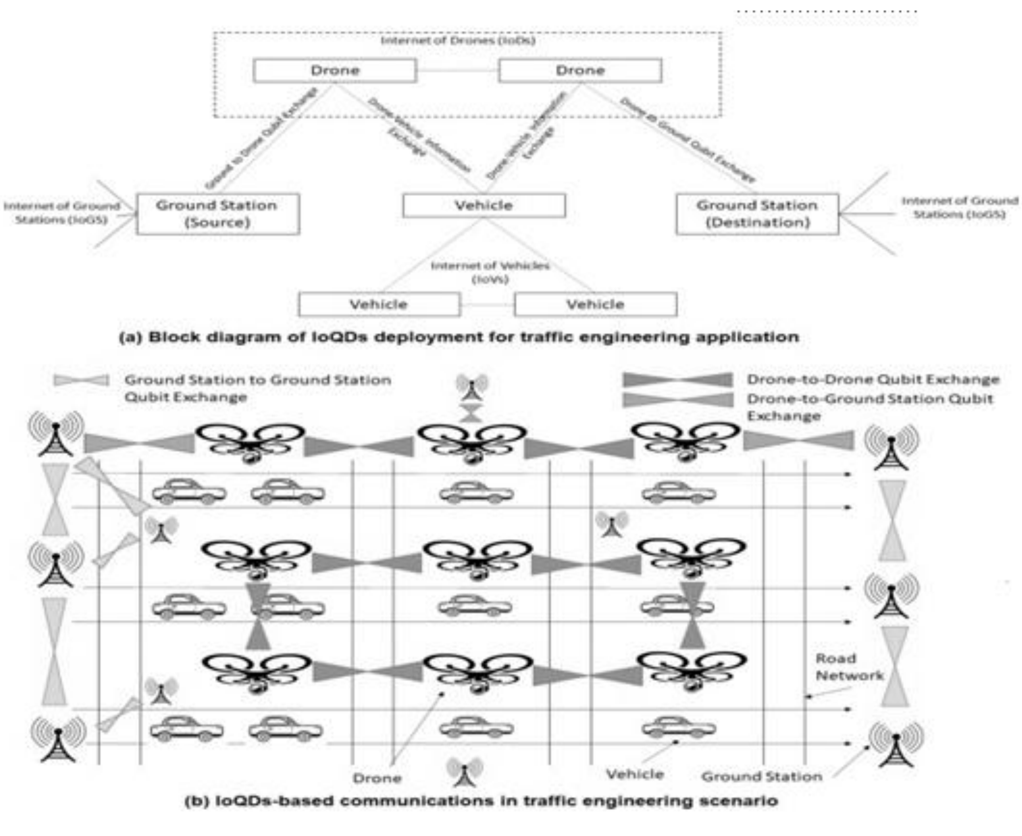

Figure 5: IoQDs-based Communication (source: science direct.com) [8]

V. CONCLUSIONS

The use of Quantum Communication in IoT for drones improves long-distance communication and data transmission. Because quantum processing and related angles are expected to hold enormous potential in the future, this study will be useful in investigating the many heads in the quantum region. As a result, this work depicts several examination orientations, obstacles, and cutting-edge aspects of quantum drones, designs, computations, satellites, IoQDs, a star grouping of satellites, long-distance correspondence, assaults on quantum organizations and correspondence, and PQC. (Post-quantum cryptography) Quantum communication enables efficient transmission and significant demand in emerging sectors.

REFERENCES

[1] “Security and Privacy in Device-to-Device (D2D) Communication”, Michael Haus. Available :https://ieeexplore.ieee.org/abstract/document/7809147
[2] “A Review on existing IoT Architecture and Communication Protocols used in Healthcare Monitoring System” ,Navneet Verma .Available:https://link.springer.com/article/10.1007/s40031-021-00632-3
[3] “Lora wan” Available: https://www.cardinalpeak.com/blog/setting-up-a-lora-gateway-to-view-iot-device-data
[4] SigFox-based Internet of Things Network Planning for Advanced Metering Infrastructure Services in Urban Scenario Available:https://www.researchgate.net/publication/343777129_SigFox
[5] “Quantum-Based Lightweight Transmission Mechanism against Eavesdropping for IoT Networks” Available : https://www.hindawi.com/journals/wcmc/2022/4809210/
[6] “Futuristic view of the Internet of Quantum Drones” Adarsh Kumar. Available: https://www.sciencedirect.com/science/article/pii/S2214209622000341
[7] https://wiforum.org/concept-innovations/
[8] “IoQDs for radar and traffic management” Available : https://www.sciencedirect.com/science/article/pii/S2214209622000341