**Quantum-Based Group Key Generation for Secure Authentication in WBAN**

**Abstract**

Wireless Body Area Network (WBAN) is an emerging solution that is capable of addressing the requirements of healthcare-related companies located both close to and far away. A newly produced key is statistically self-reliant to any other system data, an attacker could have used standard nomenclature which has information-theoretic security. Real-time authentication and transmission rely more on mobile technology; thus, it must be safe and efficient. Verification and key distribution systems utilized in the past have network failure and response latency issues. This research suggests quantum-based group key production for WBAN authentication. This system establishes secure communication channels using sensor nodes and the base station. The proposed technique might reduce travel time, energy utilization, and communication costs by using a group-based node. The analysis compares the following cases: the generic scheme with no group node, the suggested scheme with a group node, and earlier with the Quantum Key Distribution (QKD) protocol. The suggested approach is tested with mobility and non-mobility and with and without group nodes. It comes up the result that the proposed approach has the most accurate results, with low energy consumption of 0.24369 by using group node, and it is lower in QKD protocol that is 0.236443 while comparison with the existing scheme in which group node is not present. This approach improves security and energy efficiency.

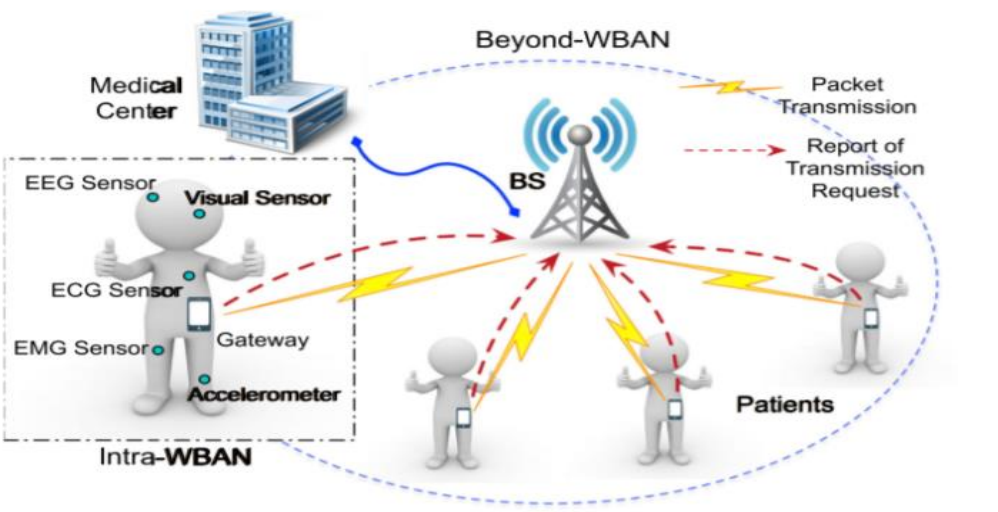
**Keywords** WBAN, Real-time authentication, Group key generation, EMR, QKD, Group node.

# **Introduction**

The advent of Informational and Communication Technology (ICT) has made it possible to personalize medical facilities, observe patients in real-time, and administer more appropriate therapy [1]. Implantable medical equipment, such as pacemakers, cervical nerve insulin pumps, and other similar devices, can analyze a patient's health characteristics and transfer information to a server through the Internet via a gateway gadget [2]. The term digital healthcare system refers to this particular network infrastructure for the exchange and archiving of data [3]. In recent years, a vast number of research have been conducted to establish safe authentication frameworks for electronic healthcare that also protect patients' confidentiality [4].

The WBAN is a type of wireless sensor that is used for a particular purpose [5]. WBAN is an emerging solution that is capable of satisfying the requirements of healthcare-related establishments located both close to and far away [6]. It does this by integrating a large number of wireless networks and devices, which enables it to perform remote surveillance of a wide range of different scenarios [7]. Continuous monitoring is made significantly easier and more effective by its use, which in turn makes it feasible to arrive at precise diagnoses and supply information in real-time to medical professionals [8].

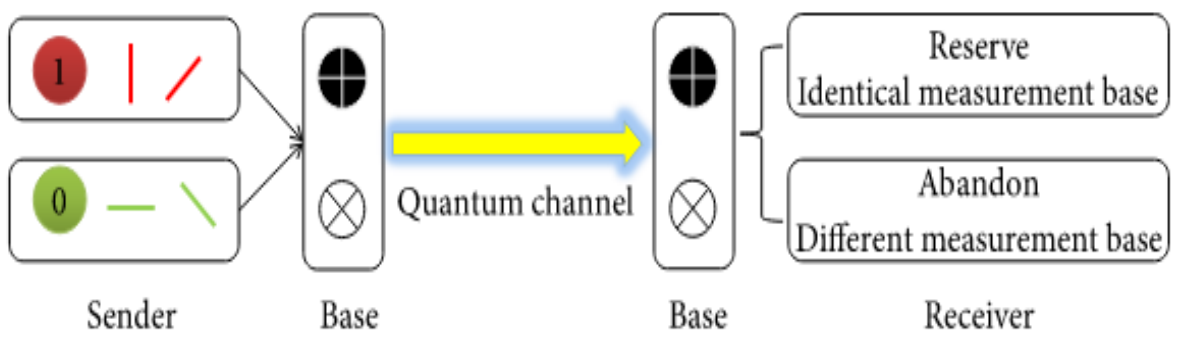
It is a new way of thinking about technology that allows devices from various industries to be connected via the Internet [9]. As more wearable devices hit the market, the WBAN is gaining popularity in medical applications [10]. It is a link between an inter-connected device like a mobile phone, a home automation system, or something worn [11]. Figure 1 demonstrated the electronic health network in which data of multiple patients is monitored as given below.



**Fig 1** Electronic-health networks [12][9]

## **Group Key Generation using the Quantum Approach**

According to the concept, a newly generated key is statistically self-reliant to any other system data that an adversary could have following traditional nomenclature, which possesses information-theoretic security [13]. In the context of cryptography, typical quantitative measures of data theoretic protection have never been clear what their functional or empirical significance is unless it is limited to the restriction of all or some data on a bit pattern [14]. This is undeniably a highly significant problem at the very core, and it manifests itself in all protocols for key generation, whether classical or quantum [15]. Figure 2 shows the model of the Quantum Key Distribution (QKD) protocol as given below.



**Fig. 2** Model of QKD protocol [16]

The difficulty is made worse by the usage of a common secret key through the process of key generation, which is required equally in Key Cryptography Quantum (KCQ) and QKD protocols where an open authentic channel needs to be generated [17].

## **WBAN and Secure Group Key Authentication**

In today's world, WBAN can be put to use in an extremely diverse range of innovative and beneficial ways [18]. Since the WBAN is intrinsically linked to the method of determining biological characteristics, the field of healthcare is where it has had the most success up until this point [19]. The WBAN revolution is changing modern health care in ways that are good for technology, the economic system, and society [20]. Smart objects become the most important building blocks for building smart structures[21-22].

Real-time authentication and transmission have become more dependent on mobile communication technologies, which necessitates that these processes be both secure and efficient [23]. Verification and key distribution methods that have been used in the past are plagued by problems with network breakdown and excessive response delay [24]. It is still difficult to communicate using WBANs due to security and privacy concerns, which limits the scope of their potential uses in the medical field [25]. In this scenario, having an appropriate authentication technique in conjunction with a group key management plan is of utmost importance [26]. Figure 3 demonstrated the general architecture of a WBAN-based system as given below:

**Diagram

Description automatically generated**

**Fig 3** General architecture of a WBAN-based system [27]

# **Review of literature**

The research described the Quantum based group key generation for secure authentication in WBAN. Several researchers provided the following descriptions of their findings:

Yu et al., (2022) [28] stated that the WBAN has made it possible for intelligent sports resources to be integrated and optimally deployed, which has a major influence on the health management of intelligent sports players. Cloud computing offered two of the most significant benefits, were virtualization and distributed storage. In addition to this, the cloud had crucial characteristics such as autonomous administration and broadband internet. Cloud computing was utilized in the building of an intelligent sports health monitoring system. It was the first of its kind to make use of innovative information technology to assist in the management of intelligent sports health.

El-Aziz et al., (2022) [29] analyzed that those patients must be checked regularly and treated in the event of an emergency. An Electronic Medical Record (EMR) is a valuable tool in this situation. The growing popularity of cloud computing must be capitalized on to reap the benefits of data science methodologies for e-healthcare monitoring systems. Many sensor devices captured real-world healthcare data. Scientists applied innovative data science approaches and technology in the Healthcare Monitoring-Data Science Technique (HM-DST). The Improved Pigeon Optimization (IPO) approach was created to combine data in the cloud to improve prediction rates. The Backtracking Search-based Deep Neural Network (BS-DNN) with 93.48 accuracies is deployed to identify human healthcare data. The suggested system was evaluated thoroughly, and the results were compared to those of existing smart healthcare monitoring systems utilizing real-time healthcare information.

Nayak et al., (2022) [30]  determined that health was a fundamental human right and that everyone should have access to it. For corporate use, real-time cloud computing and business applications can be more dependable and cost-effective. If it is wanted to save money and time, cloud computing offered a stable foundation at an affordable cost. Recent developments in sensor communication, sensor sensing, and microelectronics have focused on chronic conditions and crises. One or both of the following elements can be utilized to manage health monitoring. The expense of the most significant challenges or the treatment offered to people. As a consequence, specialists can conduct electronic visits, which removes the need for travel while allowing for complete contact between doctor and patient. The authors explored cloud-based healthcare monitoring frameworks for home hospitalization in their article.

Olatinwo et al., (2021) [31] reported that WBAN is now obtaining a lot of popularity, as a consequence of its capability to be applied to a broad variety of various kinds of systems revealed that sensor gadget is now getting a lot of popularity. One of the many explanations for why this occurrence is taking place is as follows: WBAN is the name of the potentially useful technology, which is now being implemented in the medical sector. Its sole function is that of a healthcare monitoring system, which was the driving motivation for its creation. This has the potential to result in expanded functionality as well as new applications. These kinds of technologies are suitable for medical surveillance, and it can also regulate processes and make decisions without the involvement of humans. It can manage and arrange when mutual connectivity can be utilized, a protocol is known as Medium Access Control (MAC) has lately been receiving a lot of interest in the field of WBAN. In conclusion, the findings show that MAC protocols can be utilized in technology that utilizes WBAN to improve the quality of communications and satisfy necessary criteria. This can be done since the protocols are compatible with the requirements.

Ullah et al (2021) [32] indicated that the human population has risen rapidly over the past several decades. As a consequence, individuals have been confronting a growing number of obstacles in terms of satisfying their fundamental wants and finding suitable accommodations. People have long had health issues and lost loved ones due to lack of care or treatment. Health care solutions have been getting better over the years, and there have been many medical breakthroughs in the last 200 years. WBAN makes it possible for sensor nodes or controllers to connect with application providers via a variety of open network types. Public Key Infrastructure (PKI) based encryption can provide a solution to the problems that have been outlined above. In the end, it concluded that WBAN was better in terms of privacy, price of calculation, and interaction overhead.

Shaik et al., (2021) [33] revealed that WBAN is both a vital step for long-term purposeful networks and the Internet as well as one of the most current methods that have been developed for healthcare administration. The field of health informatics within the context of a hospital has become increasingly complicated due to the presence of numerous factors that need to be assessed and the requirement for a network that collects data from a large number of patients for analysis at a monitoring station. A specific aspect of each patient's health is evaluated, and the results are referred to as vital signs. It is critical for hospitals to track their patient's health and well-being at all times. Zigbee technology enables the PC to comprehend all parameters. A Micro Controller Board (MCB) is used to assess patient data inputted by the patient. The Zigbee device and the microcontroller on the Arduino board system need to exchange signals. Vital signs are monitored utilizing two sensors. Sensors for the heartbeat and temperature can be found on the device. In the end, it concluded that a ZigBee-based network delivered messages at a high rate, while frequent messages were shared at a lower rate.

Siam et al., (2021) [34] focused on health care professionals and patients alike paying close attention to smart health surveillance technology because it can give an early diagnosis of key abnormalities without the need for direct patient interaction. Multivocal signal monitoring was invented, and the current technology enables simultaneous monitoring of heart rate, blood oxygen saturation, and body temperature. The physiological signals were encrypted and processed using the Advanced Encryption Standard (AES) approach before it is transferred to the cloud. Several market medical devices were compared to the planned system measures.

Lakshmi K et al., (2021) [35] explained that healthcare monitoring systems have grown in importance over the previous decade and are among the most technologically advanced systems available. A lack of medical attention for individuals has resulted in a wide range of health issues, including unexpected deaths. Continuous wireless patient monitoring is made possible with the use of a mobile app and a Global System of Mobile (GSM) communication. Wireless healthcare monitoring systems were available that can deliver real-time internet data on a patient's health status. It was possible for the doctor's mobile device to continuously monitor a patient's temperature, heart rate, Electrocardiogram (ECG), blood pressure, and oxygen saturation (SPO2) levels in an app.

Sahu et al., (2021) [36] analyzed those cardiovascular diseases (CVD) that can be studied using an ECG, which was universally acknowledged as a reliable tool. A cloud-based approach was described in the research. Amazon Web Services (AWS) transmits the ECG data collected from the subject to an S3 bucket for remote monitoring of cardiovascular illness using a mobile gateway. Hyper Text Transfer Protocol (HTTP) and Message Queuing Telemetry Transport (MQTT) servers were used by AWS cloud. Distractions, external noise, and motion artifacts were filtered out of the suggested system using filtering algorithms.

Valsalan et al., (2020) [37] focused on a medical surveillance-based solution that was necessary for the event of such an epidemic. An explosion of these studies is taking place, notably in the healthcare sector, due to a new internet revolution. Remote health care monitoring has improved so quickly because of the growing popularity of wearable sensors and smartphones. An accurate diagnosis can be made even when the attending physician has located at a substantial distance thanks to the e-monitoring of health. A portable monitoring device, such as the one detailed in the study, can keep track of vital physiological indicators including heart rate, room temperature, and others in real-time. This solution would make it possible for anybody with the proper credentials to gain remote access to data stored on an e-health platform to diagnose patients’ ailments using the data collected. There is a wide range of authors who used the technique and presented their discoveries, as given in Table 1.

**Table 1** Comparison of the reviewed literature

|  |  |  |
| --- | --- | --- |
| Author’s Name | Technique used | Outcome |
| Yu et al., (2022) [28] | Cloud computing | It was being utilized to create a smart sports health monitoring system. |
| El-Aziz et al., (2022) [29] | HM-DST | As a result, it was more dependable and cost-effective for corporate use. It provides a solid foundation and a reasonable price. |
| Nayak et al., (2022) [30] | Cloud-based healthcare | Specialists can conduct electronic visits, which removes the need for travel while allowing for complete contact between doctor and patient. |
| Olatinwo et al., (2021) [31] | MAC | MAC protocols can be used to make use of WBAN to enhance the quality of communications and meet essential criteria. |
| Ullah et al (2021) [32] | PKI | WBAN was better in terms of privacy, price of calculation, and interaction overhead. |
| Shaik et al., (2021) [33] | MCB and ZigBee | It was determined that type of network development could increase the percentage of the entire network's life. |
| Siam et al., (2021) [34] | AES | It is used to create a secure, portable, and multivocal signal monitoring system. |
| Lakshmi K et al., (2021) [35] | GSM | Wireless healthcare monitoring systems leverage this technology consequently. Patients' health conditions can be accessed over the internet in real-time. |
| Sahu et al., (2021) [36] | AWS and MQTT | As a result, a cloud-based solution for remote cardiovascular disease monitoring (CVD) was demonstrated. |
| Valsalan et al., (2020) [37] | E-monitoring method | It is used to create a remote health monitoring system, which has the growing popularity of wearable sensors. |

# **Background Study**

E-healthcare refers to a network that is made up of real-world items that are capable of gathering and exchanging digital data. It incorporates a broad variety of intelligent gadgets and sensors that can communicate with one another and send data via a network. The exponential rise of wireless technology has led to the discovery of the new potential for expansion in a variety of industries, including schooling, aviation, agriculture, and most notably the field of healthcare. However, the increasing usage of intelligent gadgets and sensors, particularly in e-health systems, would increase the number of safety concerns that need to be addressed. These challenges include the authentication of many connected items and information that is being transmitted. Ensuring truthfulness is one of the most crucial difficulties that have to be addressed because of the sensitive nature of e-health applications. As a result, E-health applications call for an authentication mechanism to safeguard the transmission of data, its utilization, and the interchange of information among detector nodes and the Base Station. These programs are vulnerable to a variety of hacking attempts because all communication in e-health apps takes place via a wireless connection. In addition, it has limited capabilities in terms of its computational and energy resources. Therefore, one of the primary objectives of developing protection protocols is to enhance the use of the system. This would enable sensors to conserve energy, which would in turn lead to an extension of the network's lifetime and make it more resistant to a variety of forms of assault. This research proposes a quantum-based group key creation as a method for achieving safe authentication in WBAN networks. Through the use of sensor nodes and the Base Station, this system provides authentication and generates secure communication channels. The suggested method, which includes a group-based node as an element, could cut down on travel time and the amount of energy that must be used, while also lowering the cost of communication [38].

# **Problem Formulation**

WBAN is a specialized form of network that is being developed specifically for the human body to monitor, control, and transmit various vital indications of the human body, such as temperature, blood pressure, and ECG. These vital indicators can be tracked by employing a variety of sensors that can be mounted on clothing, on the body, or even underneath the skin of a person. There are still a lot of problems that need to be solved, and the ones that are needing better solutions can be found in WBAN. WBAN is confronted with both ethical and technological issues, such as the fact that privacy is the most significant and pressing ethical issue that has not yet been resolved, and that the primary technical task is to improve Human-Computer Interaction (HCI). Protection, intrusions, speed, periodic intricacy, invariant meshes, and the adaptable nature of WBAN are just a few of the difficulties that are being tackled in the research gap. Security measures and key distribution are employed so that cyber-attacks can be both avoided and responded to more quickly, a group key is created to ensure secure authentication by utilizing a quantum system, which helps to prevent illegal access.

# **Research Methodology**

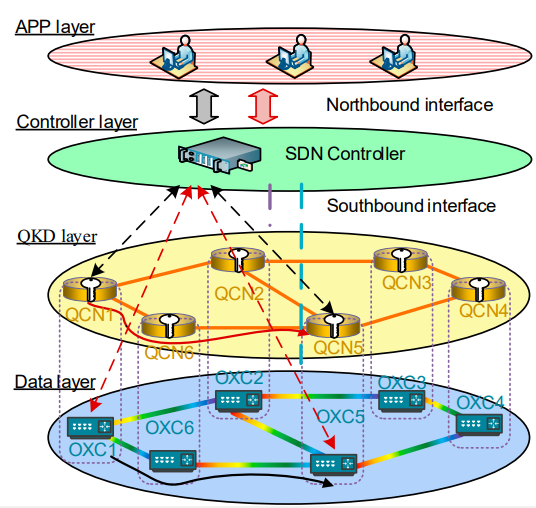
The concept of designed architecture is examined in the context of research methodology. The QKD technique has been studied extensively for the generation of group keys to perform secure authentication in WBAN. In the research methodology, it has been taken patient’s data as the input data, and then transfer to the server via a base station and group node by making secure authentication between source to destination. It is achieved by using two techniques which are explained given below.

## **Technique used**

Two technologies are used in this proposed methodology which are Quantum Key Distribution (QKD) and Layered architecture.

* **Quantum Key Distribution (QKD)**

A technology known as quantum cryptography employs quantum physics to ensure the safety of the deployment of symmetrical encryption keys. QKD is a moniker that more accurately describes quantum cryptography. An optical link is used to transmit photons, also known as quantum particles of light so that the process can take place. Monitoring of a quantum state is known to result in a disturbance, as required by the fundamental principles of quantum physics. The different QKD techniques are designed to assure that any effort by an unauthorized person to view the broadcast photons could disturb the communication if the eavesdropper succeeds in observing the photons [39]. Figure 4 shows the architecture of optical networks secured by QKD as shown below.



**Fig. 4** Network Architecture secured by QKD [40]

The final key's length can't be predicted precisely because of the quantum channel's error rate and Eve's impact. The number of bits that have been leaked and the range of rounds required to find the key's flaws also play a role. An encrypted message can only be decrypted using an encrypted key that is long enough [41]. To predict the length of a raw key following formulae can be summarised:

(1)

Where Q is denoted as the Raw Key, A is denoted as the length of the final key, S is denoted as the percentage of the raw key, and L is denoted as the number of bits leaked during the key reconciliation phase

* **Layered Architecture**

A fuzzy-based multipath routing system creates layers of varying widths depending on the distances between sensor nodes. The sensor node's unique ID is included in messages forwarded to the Base Station (BS). Fuzzy-based multipath routing protocol layer layout is shown in Figure 5.

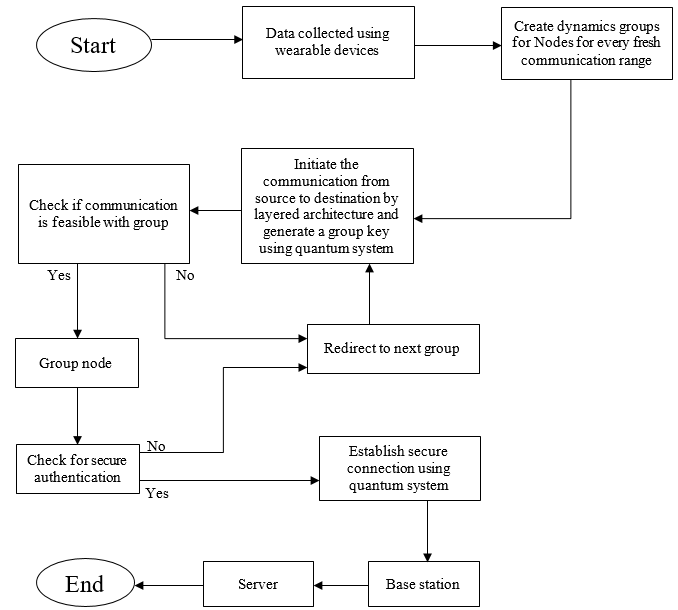


**Fig. 5** Fuzzy-based multipath routing protocol layer [42]

The comparative space between each device point and BS is calculated centered on the intensity of the indicator from each node, and the identification of the device is saved. The BS creates sheets of varied sizes based on the space between the closest and farthest sensors. The device connections that are nearby to the support location are positioned on top, while the connections that are farthest gone from the support location are on the bottom. This decreases from the upper layers to the lowest layers in device connection density [42].

## **Proposed methodology**

The methodology is based on Quantum based group key generation for secure authentication in WBAN and detailed step are given below. Figure 6 shows the proposed methodology in pictorial representation as shown below.



**Fig. 6** Flow diagram of research methodology

**Step 1: Collection of data from wearable devices.**

In this step, several sensor nodes collect distinct types of data from a patient such as body temperature, heart rate, blood pressure, sugar level, etc., and further transmitted it.

**Step 2: Create node dynamics groups for each new communication range.**

In step 2, dynamic group nodes are created for every fresh communication range for collected data, which stores all the collected data of the patient and further transmits it for producing the group key.

**Step 3: Initiate communication from source to destination and produce a group key by a quantum system.**

In this step, communication is initiated between source to destination by using layered architecture and produces a group key by using the quantum system and sending the communication to check whether it is feasible with the group or not.

**Step 4: Condition check for group communication**

In this step, the condition is checked whether the communication is feasible with the group or not. If the condition is true, then the data is transferred to the group node to further check the secure authentication and if the condition is false then it is redirected to the next group.

**Step 5: Verify secure authentication**

In this step, the data transferred to the group node is directed to verify whether the authentication is secured or not. If the authentication is not secured it is redirected to the next group and if the authentication is secured, then it is allowed to proceed further.

**Step 6: Establish a quantum secure connection**

This step is used for establishing a secure connection and using a quantum system a secured connection is established between the group node and base station to transmit the collected data.

**Step 7: Transferring data to the base station and then to the server**

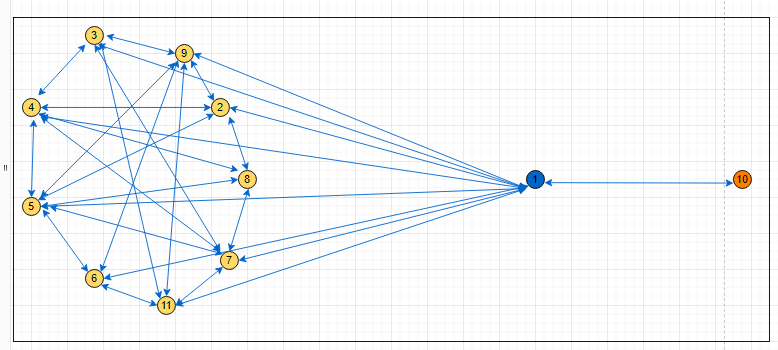
In this step, finally after establishing a secure connection between using the quantum system, the data is transferred to the base station from the group node and then the data is transmitted to the server from the base station.

# **Results and Discussion**

In this section, an analysis of how the suggested plan would consume energy is demonstrated. The investigation would comprise a comparison of the following cases: a general approach with no group node; the suggested approach with the presence of a group node with both mobility and no mobility condition and the QKD protocol with both mobility and no mobility.

* **Result 1**

A patient was shown in this situation resting on the bed without the group node being utilized on them. In this particular instance, nine ultra-sensor nodes were strategically placed all over the patient's body to monitor a variety of vital indicators. Figure 7 shows the simulator scenario of no group node.



**Fig. 7** Simulator scenario of no group node

Figure 8 depicts the outcomes that occurred as a result of figure 7. The outcomes revealed that the energy usage is higher in no group node- no mobility. The energy consumption is larger, dependent on the range from the nodes to the base stations. As the length is directly related to the energy utilization as shown below.

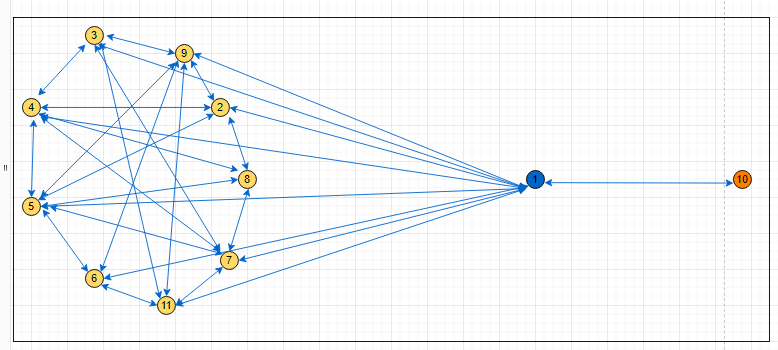
**Chart, line chart

Description automatically generated**

**Fig. 8** No Group Node – No Mobility

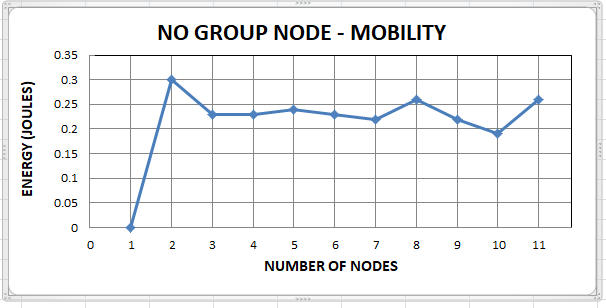
* **Result 2**

In result 2, a patient was seated in a wheelchair that can travel freely among rooms and does not require the use of the group node program. This case was evaluated using nine ultra-sensor nodes that were placed in various locations on the patient's body to measure various vital indicators. In a typical scenario, all ultra-sensors would gather the necessary data, transmit it to the base station, and then send it on to the healthcare server. This process can be shown in figure 8.



**Fig. 9** Simulator scenario of No group node – Mobility

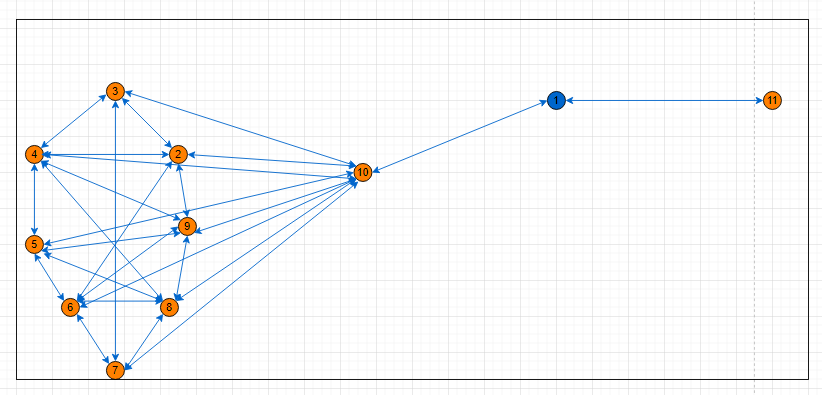
Figure 10 depicts the outcomes that occurred as a result of figure 9. The outcomes revealed that the energy usage is higher in no group node with mobility. The energy consumption is larger, dependent on the range from the nodes to the base stations. As the length is directly related to the energy utilization as shown below.



**Fig. 10** No group node –Mobility

* **Result 3**

In this result, a patient was seen lying on a bed while being monitored by a group node. At the same time, eight ultra-sensor nodes were dispersed across the patient's body to monitor various vital signs in addition to the group node. In a typical scenario, all ultra-sensors would gather the necessary data and transmit it to the group node. The group node would then transmit all of the data to the Base Station, and finally to the server as seen in figure 10.



**Fig. 11** Simulator scenario of group node – No Mobility

Figure 12 depicts the outcomes that occurred as a result of figure 11. The outcomes revealed that the usage is lower when it uses a group node with no mobility i.e., a patient is on the bed. The group node key would transmit the same key between all ultra-sensor nodes, so there would be no need for the individual nodes to communicate with one another to obtain their authentication key. This help to decrease the average energy consumption.

Chart, line chart

Description automatically generated

**Fig. 12** Group node – No Mobility

* **Result 4**

In this result, a patient is seated in a wheelchair that can travel among rooms. The group node technology is being used, and eight ultra-sensor nodes have been distributed to various parts of the patient's body to monitor their vital signs. The group node would track the movements of the patient, and as a result, both the wearable sensor nodes and the group node would be able to move about freely.

Chart

Description automatically generated

**Fig. 13** Simulator scenario of group node – Mobility

Figure 14 depicts the outcomes that occurred as a result of figure 13. The outcomes revealed that the usage is lower when it uses a group node in mobility i.e., a patient is in a wheelchair. The group node key would transmit the same key between all ultra-sensor nodes, so there would be no need for the individual nodes to communicate with one another to obtain their authentication key. This help to decrease the average energy consumption.

Chart, line chart

Description automatically generated

**Fig. 14** Group node –Mobility

## **Comparison results**

The findings demonstrate that the energy usage is higher in both of the scenarios, mobility or without mobility. It tested the same situations of the person for both cases of mobility, and non-mobility, utilizing the proposed approach where interaction with the base station might be accomplished by utilizing the concept of a group node key. In both cases, it was found that the proposed solution worked effectively. The Group Node key would transmit the same key between all ultra-sensor nodes, so there would be no need for the individual nodes to communicate with one another to obtain their authentication key. Based on the findings that were reached for the amount of energy that was consumed by each node, which is reflected in the graphs that are shown below. Compare with other methods, such as those in which no group node is deployed for either the patient being in bed (having no mobility) or the patient being in a wheelchair (having mobility), the QKD protocol, finds that proposed smethod is superior. Table 2 shows the value of average energy consumption for mobility and no-mobility.

**Table 2** Average energy consumption for mobility and no mobility

|  |  |  |
| --- | --- | --- |
|  | Mobility (Average energy consumption) | No mobility (Average energy consumption) |
| No group Node | -0.23623 | -0.24765 |
| Group node | -0.23375 | -0.24369 |
| QKD | -0.224149 | -0.236443 |

Figure 15 depicts the comparison between group node and no group node in the WBAN-based health monitoring system.

**Fig. 15** Average Energy consumption comparison between group node and no group node

# **Conclusion and Future Scope**

This system checks sensor nodes, the Base Station, and E-health channels. This strategy improves energy efficiency and security. The approach was tested with mobile and non-mobile patients, as well as with and without GN. After that, these findings were acquired from various situations, and it was discovered that there was a considerable difference in energy efficiency and secure communication. According to the findings, the suggested method produces the most accurate outcomes, has a low energy consumption of 0.24369 by utilizing group nodes, and has a lower QKD protocol value of 0.236443 when compared to an existing scheme in which a group node is not present.

Utilizing quantum cryptography in applications that deal with information transfer in the real world can be the focus of future efforts and the next major technological advance. Quantum computing speeds up information processing in every circumstance, and quantum cryptography meets information security criteria. As a result, investigating the quantum IoT integrated environment for solving industry-specific problems might be an attractive direction to go in the future.

# **References**

1. Althebyan, Q., Yaseen, Q., Jararweh, Y., & Al-Ayyoub, M. (2016). Cloud support for large-scale e-healthcare systems. Annals of Telecommunications, 71(9), 503-515.
2. Almulhim, M., Islam, N., & Zaman, N. (2019). A lightweight and secure authentication scheme for IoT-based e-health applications. International Journal of Computer Science and Network Security, 19(1), 107-120.
3. Dey, J., & Mukherjee, S. (2021). Wireless COVID-19 telehealth: Leukocytes encryption guided by amino acid matrix. Wireless Personal Communications, 120(2), 1769-1789.
4. Kumari, S., Khan, M. K., & Kumar, R. (2013). Cryptanalysis and improvement of a privacy-enhanced scheme for telecare medical information systems. Journal of medical systems, 37(4), 1-11.
5. Singla, R., Kaur, N., Koundal, D., & Bharadwaj, A. (2022). Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. Wireless Personal Communications, 122(2), 1767-1806.
6. Soni, M., & Singh, D. K. (2021). LAKA: lightweight authentication and key agreement protocol for internet of things based wireless body area network. Wireless Personal Communications, 1-18.
7. Jegadeesan, S., Azees, M., Babu, N. R., Subramaniam, U., & Almakhles, J. D. (2020). EPAW: Efficient privacy-preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). IEEE Access, 8, 48576-48586.
8. Mukati, N., Namdev, N., Dilip, R., Hemalatha, N., Dhiman, V., & Sahu, B. (2021). Healthcare assistance to COVID-19 patients using internet of things (IoT) enabled technologies. Materials today: proceedings.
9. Marudhai, V., Prince, S., & Kumari, S. (2022). Design and Simulation of Physical Layer Security for Next Generation Intelligent Optical Networks. Wireless Personal Communications, 1-20.
10. Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the energy sector. Energies, 13(2), 494.
11. Doyu, H., Morabito, R., & Brachmann, M. (2021, April). A tinymlaas ecosystem for machine learning in IoT: Overview and research challenges. In 2021 International Symposium on VLSI Design, Automation and Test (VLSI-DAT) (pp. 1-5). IEEE.
12. Mary, A. V., & Jerine, S. (2020, November). Wireless body area network transmissions for IoT-based healthcare network: a review. In IOP Conference Series: Materials Science and Engineering (Vol. 983, No. 1, p. 012017). IOP Publishing.
13. Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, 8(8), 595-604.
14. Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, 2(1), 1-12.

Dhanaraj, R. K., Rajasekar, V., Islam, S. H., Balusamy, B., & Hsu, C. H. (Eds.). (2022). Quantum Blockchain: An Emerging Cryptographic Paradigm. John Wiley & Sons.

1. Murugan, G. (2020). An Efficient Algorithm on Quantum Computing with Quantum Key Distribution for Secure Communication. International Journal of Communications, 5.
2. Kues, M., Reimer, C., Lukens, J. M., Munro, W. J., Weiner, A. M., Moss, D. J., & Morandotti, R. (2019). Quantum optical micro combs. Nature Photonics, 13(3), 170-179.
3. Chen, Y., & Li, S. (2019). A lightweight anomaly detection method based on SVDD for wireless sensor networks. Wireless Personal Communications, 105(4), 1235-1256.
4. Hasan, K., Biswas, K., Ahmed, K., Nafi, N. S., & Islam, M. S. (2019). A comprehensive review of wireless body area network. Journal of Network and Computer Applications, 143, 178-198.
5. Kumari, S. (2022). Enhancing the Quantum Communication Channel Using a Novel Quantum Binary Salt Blowfish Strategy. Wireless Personal Communications, 123(2), 1085-1102.
6. Kashani, M. H., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques, and trends. Journal of Network and Computer Applications, 192, 103164.
7. Hussain, S. J., Irfan, M., Jhanjhi, N. Z., Hussain, K., & Humayun, M. (2021). Performance enhancement in wireless body area networks with secure communication. Wireless Personal Communications, 116(1), 1-22.
8. Saritha, A., Reddy, B. R., & Babu, A. S. (2021). QEMDD: Quantum Inspired Ensemble Model to Detect and Mitigate DDoS Attacks at Various Layers of SDN Architecture. Wireless Personal Communications, 1-26.
9. Xu, G., Li, X., Jiao, L., Wang, W., Liu, A., Su, C., ... & Cheng, X. (2020). Bagkd: a batch authentication and group key distribution protocol for vanets. IEEE Communications Magazine, 58(7), 35-41.
10. Kumar, V., Jayapandian, N., & Balasubramanie, P. (2021). Improving routing data security in wireless sensor networks using clustering range indicators is essential in the SMDSRNGs method. Wireless Personal Communications, 1-12.
11. Tan, H., & Chung, I. (2019). Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor. IEEE Access, 7, 151459-151474.
12. Liu, B., Yan, Z., & Chen, C. W. (2013). MAC protocol in wireless body area networks for E-health: Challenges and a context-aware design. IEEE Wireless Communications, 20(4), 64-72.
13. Yu, H., Cai, Z., Xie, W., Xiao, H., Zhang, S., & Wang, F. (2022). Research on the Construction of Intelligent Sports Health Management System Based on Internet of Things and Cloud Computing Technology. Wireless Communications and Mobile Computing, 2022.
14. M Abd El-Aziz, R., Alanazi, R., R Shahin, O., Elhadad, A., Abozeid, A., I Taloba, A., & Alshalabi, R. (2022). An Effective Data Science Technique for IoT-Assisted Healthcare Monitoring System with a Rapid Adoption of Cloud Computing. Computational Intelligence and Neuroscience, 2022.

Nayak, M., & Barman, A. (2022). A Real-Time Cloud-Based Healthcare Monitoring System. In Computational Intelligence and Applications for Pandemics and Healthcare (pp. 229-247). IGI Global.

Olatinwo, D. D., Abu-Mahfouz, A. M., & Hancke, G. P. (2021). Towards achieving efficient MAC protocols for WBAN-enabled IoT technology: a review. EURASIP Journal on Wireless Communications and Networking, 2021(1), 1-47.

Ullah, I., Zeadally, S., Amin, N. U., Khan, M. A., & Khattak, H. (2021). Lightweight and provable secure cross-domain access control scheme for the internet of things (IoT) based wireless body area networks (WBAN). Microprocessors and Microsystems, 81, 103477.

Shaik, M. F., Subashini, M. M., & Swathi, N. (2021, March). Implementation of a ZigBee Based Network for WBAN. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 188-192). IEEE.

Siam, A. I., Almaiah, M. A., Al-Zahrani, A., Elazm, A. A., El Banby, G. M., El-Shafai, W., ... & El-Bahnasawy, N. A. (2021). Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications. Computational Intelligence and Neuroscience, 2021.

Sangeethalakshmi, K., Preethi, U., & Pavithra, S. (2021). Patient health monitoring system using IoT. Materials Today: Proceedings.

Sahu, M. L., Atulkar, M., Ahirwal, M. K., & Ahamad, A. (2021). IoT-enabled cloud-based real-time remote ECG monitoring system. Journal of Medical Engineering & Technology, 45(6), 473-485.

Valsalan, P., Baomar, T. A. B., & Baabood, A. H. O. (2020). IoT-based health monitoring system. Journal of critical reviews, 7(4), 739-743.

Almulhim, M., Islam, N., & Zaman, N. (2019). A lightweight and secure authentication scheme for IoT-based e-health applications. International Journal of Computer Science and Network Security, 19(1), 107-120.

Yulianti, L. P., & Surendro, K. (2022). Implementation of Quantum Annealing: A Systematic Review. IEEE Access.

He, X., Li, L., Han, D., Zhao, Y., Nag, A., Wang, W., ... & Zhang, J. (2022). Routing and secret key assignment for secure multicast services in quantum satellite networks. Journal of Optical Communications and Networking, 14(4), 190-203.

Mehic, M., Niemiec, M., & Voznak, M. (2015). Calculation of the key length for quantum key distribution. Elektronika ir Elektrotechnika, 21(6), 81-85.

Noh, K. M., Park, J. H., & Park, J. S. (2020). Data transmission direction-based routing algorithm for improving network performance of IoT systems. Applied Sciences, 10(11), 3784.