Journal of Computer Science & Computational Mathematics, *Volume 13, Issue 4, December 2023*
DOI: 10.20967/jcscm.2023.04.002

IoT Communication Technologies in Remote Patient Monitoring: Requirements, Analysis, and Ideal Scenarios

Khalad Agali, Maslin Masrom, Fiza Abdul Rahim

Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia
*Corresponding author email: bkkhalad@graduate.utm.my; maslin.kl@utm.my; fiza.abdulrahim@utm.my

***Abstract*:** Remote patient monitoring (RPM) facilitated by the Internet of Things (IoT) has emerged as a promising approach for efficient and personalised healthcare delivery. Communication technology enables real-time data transmission, ensures reliability and safeguards patients' privacy in RPM system. This paper analyses the various communication technologies used in the IoT. Understanding RPM system-specific requirements, conducting in-depth analysis and emphasising on optimal application scenarios are the primary objectives of this paper. The research methods involve a comprehensive review of the requirements in IoT communication technology by evaluating the IoT communication technology for RPM, using a comprehensive approach as well as focusing on scalability, reliability, data rate, latency, energy efficiency, security and range. The researchers identified its unique strengths and limitations by analysing diverse functionalities of technology. There are also insights of the specific requirements for RPM and its ideal applications. The analysis done reveals that the choice of communication technology underlines the need for a multidimensional understanding of scalability, reliability, data rate, latency, energy efficiency, security and range in its deployment. In short, this paper emphasises on the importance of a tailored approach that can enrich the existing body of knowledge in RPM system in demonstrating the nuanced utilisation of the technology, thus illuminating the pathway to effective implementation of RPM system. This paper also guides the design and selection of IoT communication technology for a better, efficient, reliable and secure RPM, thus promoting personalised healthcare delivery.

***Keywords*:** Internet of things, IoT, patient remote monitoring, RPM, communication technology

1. Introduction

The Internet of Things (IoT) has transformed the modern healthcare landscape, bridging the gap between patients and healthcare providers and enabling remote monitoring; an ability once considered impossible [1]. IoT-based healthcare is lauded for its capacity to increase access to preventative public health services and transform healthcare system to be more proactive, smooth and coordinated [2]. An IoT device's communication technology determines its reach, data transfer rate, energy consumption and effectiveness in healthcare [3]. [4] expanded on this by suggesting IoT is the future of healthcare, in which healthcare professionals will connect and monitor every medical device via the internet. According to Market Data Centre, adopting automation, technology and self-service solutions is predicted to result in an estimated yearly savings of between $24 billion and $48 billion in administrative costs. In another development, the Global Remote Monitoring System Market is anticipated to grow at CAGR of 20%; an increase from $965 million in 2022 to an estimated of $5.1 billion by 2030.

IoT communication technology has significantly improved healthcare outcomes by facilitating efficient data collection and exchange. For example, Wi-Fi and Bluetooth are crucial in facilitating this data transmission. They enable the interconnection of various medical devices, sensors and healthcare professionals [5, 6]. Moreover, the offer is dependable upon the connectivity and support data transmission over short-range to medium-range distances, making it suitable for home applications and hospital settings. LoRaWAN, on the other hand, provides a long-range coverage and minimal power consumption, making it ideal for rural and remote areas with limited infrastructure. The selection of communication technology is contingent upon particular cases, environmental factors, power constraints and scalability requirements [3]. This paper evaluates the specific requirements for IoT communication which include scalability, reliability, data rate, latency, energy efficiency, security and the range for RPM to meet these requirements in constantly evolving industries. By investigating the strengths and limitations of this technology, this paper provides valuable insights to guide the selection of appropriate communication solutions. The analysis considers various emergent technologies and assesses their capabilities to meet the demanding needs of RPM. The findings of this research are crucial for navigating the complexities of selecting the most suitable technology, ensuring secure and reliable data transmission, optimising energy consumption and ensuring compatibility with the existing systems.

RPM system is becoming increasingly essential to meet the increasing global demand for personalised and remote healthcare. In this case, incorporating IoT technology into the system can improve its efficacy and efficiency. In this sense, various IoT communication technologies provide a challenging environment for the healthcare providers and technologists. This paper contributes deeper and vital in-

sights to the existing body of knowledge by analysing the technology's strengths, weaknesses and optimal applications. These insights can guide the development of RPM solutions that are more effective, efficient and tailored to the requirements of patients and healthcare providers.

2. Literature Review

2.1 IoT Communication Technology

IoT communication technology transmits real-time medical data from medical devices, such as wearable devices, to healthcare providers. The collected data is then analysed to make informed decisions about the patient's health and treatment [7]. Figure 1 illustrates that IoT communication technology can use various communication technologies which are categorised into long-range and short-range [8].

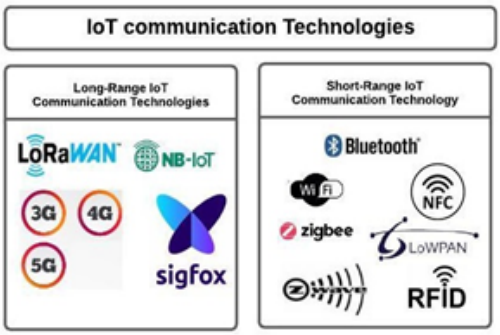

Figure 1. IoT Communication Technologies [5]

2.1.1 Long-Range IoT Communication Technology

Long-range IoT communication technologies enable devices to communicate over long distances, thus providing seamless connectivity across broad geographic areas. These are vital in connecting IoT devices located far away from each other, such as telematics units in vehicles, remote monitoring devices and mobile health devices. Long-range IoT communication technologies include the following:

Cellular Network

Cellular network is one of the most widely used long-range IoT communication technologies. It provides a high-speed and reliable means of connectivity for many IoT devices. It is based on the cellular network infrastructure commonly used for mobile phones and provides widespread coverage across the globe [9]. The technology used in cellular network is based on a standard known as long-term evolution (LTE) that provides high-speed data transfer and low latency [1].

In recent years, deploying 4G and 5G cellular networks has driven the growth of IoT communication, thus providing improved speed, reliability and lower latency compared to previous generations of cellular networks [10]. The increased speed and improved reliability of 5G networks are expected to drive the growth of remote patient monitoring, as it enables the connection of more devices as well as the collection and analysis of more data. This leads to better and more personalised care for patients [11].

LoRaWAN

Long range wide area network (LoRaWAN) is a protocol for long-range, low-power wireless communication. It is based on the physical layer technology called LoRa which uses a wideband radio frequency to provide long-range connectivity for IoT devices [12]. LoRaWAN is an open protocol managed by the LoRa Alliance. LoRaWAN's ability to provide long-range connectivity with low power consumption is one of its most important characteristics, making it well-suited for IoT applications that require extended battery life. It can cover up to 15km in rural areas and 2-5km in urban areas. Its low power consumption enables devices to operate for years on a single battery [13]. LoRaWAN is also highly scalable, which makes it suitable for large-scale IoT deployment. The network is organised into gateways that receive data from IoT devices and forward the data to a central network server which then forward the data to the intended recipient. The gateways manage the communication between the devices and the network server; both can be deployed flexibly and affordably. Next, LoRaWAN's strong security feature is an additional benefit, in which the networks encrypt data transmitted between devices and gateways with AES-128 and uses a unique device ID and network key to ensure only authorised devices can access [14].

LoRaWAN's main strengths are the abilities to provide inexpensive end devices and to deploy private networks. This eliminates the need for subscriptions and reduces operational expenses for dense IoT application deployment. Furthermore, it has wide coverage with a single gateway and low-power end node operation [13].

NB-IoT (Narrowband IoT)

NB-IoT is a LPWAN communication technology designed for IoT [15]. NB-IoT is a radio communication standard that operates in licensed frequency bands and provides a low-bandwidth, low-power solution for IoT devices that communicate over long distances. NB-IoT uses a narrow frequency band to transmit data, which makes it more spectrally efficient and less prone to interference than other IoT communication technologies [16].

NB-IoT was developed to meet the specific needs of IoT devices, such as minimal power consumption, which is essential for IoT devices deployed in remote areas or in areas where power is not readily available. Its low-cost feature makes it a cost-effective solution for IoT deployment. It does not require expensive infrastructure, can be deployed in existing cellular networks and can support a large number of connected devices [17]. NB-IoT also provides robust security features to safeguard the data transmitted between IoT devices and network. The technology employs encryption algorithms and authentication mechanisms to ensure that only authorised devices can access the network and that all transmitted data is secured [18].

Sigfox

Sigfox is an LPWAN technology that provides low-bandwidth, low-power communication solution that enables IoT devices to operate for extended period without requiring frequent battery replacement or recharging [19]. It operates on unlicensed frequency bands and uses a proprietary

protocol to transmit data between devices over long distance. Sigfox is designed for IoT applications that require low-cost, low-power solution for sending a small amount of data over long distances, such as asset tracking and remote monitoring [20].

Additionally, the signal generated by SigFox tech can easily encompass a large area and locate objects buried underground. The SigFox communication system was designed to connect enormous stretches of land, on the order of tens of kilometres in rural areas and a few kilometres in urban areas [21]. The data transfer rate is modest, supporting 4, 8 or 12 bytes at a maximum data rate of approximately 100bps [22]. Typically deployed in collaboration with mobile operators, the network is implemented with SDR (Software-Defined Radio). In Europe, the SigFox infrastructure is still being constructed, while the largest mobile network operators are negotiating new contracts to attain a larger coverage area than is currently feasible [21].

Sigfox also provides a secured and reliable connection between devices using encryption and authentication mechanisms such as AES 128, SSL and TLS to protect the data transmitted over the network [23]. Sigfox is a secured solution for IoT applications requiring personal health data transmission. However, some challenges are associated with using Sigfox for IoT applications. One of the key challenges is its limited bandwidth which restricts the amount of data transmitted over the network [20]. This is considered as disadvantage for IoT applications that require real-time data transfer or large amount of data, such as video streaming and real-time monitoring.

2.1.2 Short-Range IoT Communication Technology

Short-Range IoT Communication Technology refers to wireless communication technologies that connect devices over short distances, typically within a few hundred meters. These technologies are intended to enable a wide variety of IoT applications, such as smart homes, industrial automation, and wearable devices. A number of the most prevalent IoT short-range communication technologies include:

Bluetooth

Bluetooth is a highly advanced technology that has found its way into various intelligent devices for short-range or personal area network (PAN) data transmission and reception. It operates within the 2.400-2.485GHz frequency band. Bluetooth networks employ a star topology [24]. Bluetooth performs on the unlicensed 2.4GHz frequency band and employs Bluetooth low energy (BLE) to provide IoT devices with low-power, short-range connectivity. BLE was designed specifically to satisfy the needs of IoT devices and offers a cost-effective and power-efficient solution for IoT applications. Bluetooth 5.2 is the most recent iteration of Bluetooth technology and provides IoT devices with increased range, higher data rate and enhanced power efficiency [10]. BLE uses encryption and authentication mechanisms to secure device connection and prevent unauthorised data access. In addition, Bluetooth supports multiple profiles which define the data that can be exchanged between devices and the types of applications that can be run over the connection.

Zigbee

Zigbee is a low-power, short-range wireless communication technology commonly used in IoT applications. Zigbee operates in the unlicensed 2.4GHz frequency band and utilises a mesh network architecture, enabling IoT devices to communicate and route data to their destination [25]. This makes Zigbee a highly scalable and reliable solution for IoT applications, as the mesh network can be extended to cover larger areas and provide redundant paths for data transmission [26]. Zigbee supports a range of power-saving modes which allow devices to conserve energy when not in use. In addition, Zigbee offers various security features, such as encryption and authentication, to safeguard the data transmitted between devices and prevent unauthorised access [5, 27]. Zigbee also supports a wide range of application profiles which define the types of data that can be exchanged between devices and the applications that run over the connection. This makes Zigbee a highly flexible solution for IoT applications as it can be used for many devices and applications [9].

Wi-Fi

Wi-Fi is a wireless communication technology that enables connectivity and communication between devices over short distance. Wi-Fi operates with multiple protocols, including 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac and 802.11ax—also known as Wi-Fi 6. Each bar provides a unique set of features and capabilities, such as increased speed, enhanced security and enhanced power efficiency. Wi-Fi operates on multiple frequency bands, including 2.4GHz and 5GHz, and supports various data rates which can affect network performance and dependability [9]. Wi-Fi is one of the most widely used wireless communication technologies. It provides high-speed connectivity for many devices, including IoT devices, smartphones and laptops.

Wi-Fi is ideal for IoT applications requiring real-time data transfer, such as intelligent home systems, smart cameras, and wearable technology [28]. One of the critical benefits of Wi-Fi for IoT applications is its high speed and bandwidth, allowing for quickly transmitting large amounts of data. In addition, Wi-Fi provides robust security features to protect the data transmitted between IoT devices [29]. However, some challenges are associated with using Wi-Fi for IoT applications. First is power consumption, which is higher than other short-range wireless communication technologies, such as Zigbee and Bluetooth [30]. This is considered as a disadvantage of IoT devices powered by batteries as they require frequent charging or replacement. Another challenge of Wi-Fi for IoT applications is its limited range compared to other wireless communication technologies such as LPWANs [13].

Radio Frequency Identification (RFID)

RFID uses radio waves to transmit a small amount of data from an RFID tag to readers within short distance [5]. RFID is a wireless technology for identifying and tracking objects using radio waves. RFID technology uniquely identifies devices and assets in IoT-enabled remote monitoring systems, thus enabling real-time tracking and monitoring of their loca-

tion and status. RFID technology, which is primarily used for automatically identifying objects and people, has garnered considerable attention due to its extensive application in various industries, including toll payment, healthcare, agriculture, libraries, national security and proximity cards. The primary components of this technology are RFID tags, which come in two kinds, namely active reader tags and passive reader tags. Passive tags, powered by batteries, employ high radio frequencies, whereas passive tags, which do not possess their own power sources, use a narrower range of frequencies. In both situations, the crucial role of RFID in IoT applications is evident, and the typical structure of the RFID network is based on a peer-to-peer topology [31].

Z-Wave

Z-Wave is a wireless communication technology that provides a secured and reliable connection between IoT devices. It operates in the unlicensed 908.42MHz frequency band and uses low-power, low-bandwidth communication protocol to support data transmission between devices[5]. Z-Wave is designed for smart homes and other IoT applications which requires low power consumption and low-bandwidth connection. Z-Wave also provides a secured connection between devices using encryption and authentication mechanisms to protect the data transmitted over the network [8]. In addition, Z-Wave supports mesh networking that allows devices to route data to each other to reach their destinations. This enables Z-Wave devices to communicate with each other even if they are out of range of the central hub or controller. This feature makes Z-Wave a highly scalable solution for IoT applications, as new devices can be easily added to the network[5].

Z-Wave is also an interoperable technology, meaning that devices from different manufacturers can work together on the same network. This makes it easy for consumers to mix and match devices from different brands to create a customised, innovative system. However, some challenges are associated with using Z-Wave for IoT applications. One of the key challenges is its limited bandwidth that confines the amount of data transmitted over the network. This is perceived as a drawback of IoT applications; requiring real-time data transfer, such as video streaming and monitoring [8].

Near Field Communication (NFC)

NFC is a short-range wireless communication technology that facilitates the exchange of data over a short distance between two devices. It operates at the frequency of 13.56MHz and communicates between devices via magnetic field induction [1]. NFC is commonly used for contactless payment system, device pairing and data exchange between smartphones, tablets and other IoT devices [5]. The advantage of NFC is its ease of use that makes NFC an ideal solution for IoT applications that require fast and easy device setup, such as wearable devices [32]. NFC is a low-power technology, thus making it an energy-efficient solution for battery-powered IoT devices. This enables NFC-enabled devices to operate for extended period without frequent charging or battery replacement [8]. However, using NFC for IoT applications has its own limitations, for example its short range limits the distance between devices that can be used for data exchange. In this situation, a more extended range is required, such as monitoring and control system [3]. Figure 2 shows the IoT communication technologies classified by data rate and coverage range.

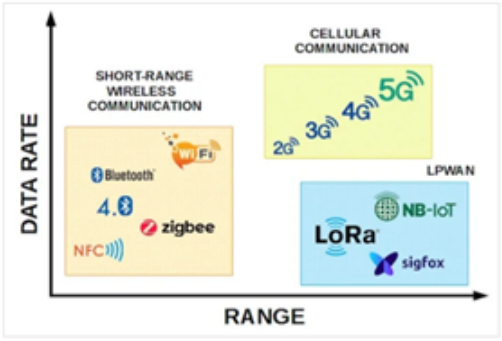

Figure 2. IoT communication technologies are classified by data rate and coverage range

Next, Table 1 compares various IoT communication technologies, which include their network topology, data rate, network, frequency band, standard, coverage range and power consumption.

Cellular networks (GSM, CDMA, 3G, LTE (4G) and 5G) provide high data rate of up to 600Mbps for 4G over a large coverage area of up to 5km. However, they have high power of consumption which limit their use in environments with limited power. LoRaWAN and NB-IoT provide lower data rates over large coverage areas while consuming short and low power. These are ideal for IoT applications that require long-range communication but do not require transmitting significant amounts of data. Sigfox offers meagre data rate but at an impressive range, making it suitable for data-light applications that require long-range communication. Bluetooth, RFID, Zigbee, Z-Wave and NFC are designed for short-range (from a few centimetres to a few hundred metres) communication with low power consumption. Typical applications include device-to-device communication, intelligent dwellings and assets tracking. Wi-Fi provides high data rate of up to 105Mbps over a comparatively short range (10-100m) and is commonly used in homes, offices and public hotspots for internet access. However, its energy consumption is significant.

2.2 IoT-Based Remote Patient Monitoring

Remote patient monitoring (RPM) has revolutionised the healthcare industry by enabling the monitoring and evaluation of real-time patient data, regardless of the geographical distance between patients and healthcare providers [33]. According to [34], IoT-RMS enables healthcare providers to monitor their patients' health and status while being away from the hospitals or clinics. [35] stated that IoT-RPM improves patient care through the utilisation of digitally transmitted health-related data. This shared information allows for early detection and treatment of disease symptoms, patient education and patient-physician relationship improvement. This digital transformation fosters improved patient-physician relationships, enables early detection of disease de-

Table 1. A table with an example caption goes here

Parameter	**Network Topology**	**Data Rate**	**Network**	**Frequency band**	**Standard**	**Cover range**	**Power consumption**
Cellular Network	NA	21 Mbps (3G+), 600 Mbps (4G)	WNAN	Cellular band	GSM, CDMA, 3G, LTE (4G), 5G	5km	High
LoRaWAN	Star-0f-star	0.3-50 Kbps	LPWAN	Various, sub-gigahertz	LoRa-Alliance	1-10 Km in rural, 1-5 Km in urban	Very Low
NB-IoT	Star	200 Kbps	LPWAN	Various, Uses sub-6 GHz spectrum]	3GPP	10 Km in rural, 1 Km in urban	Low
Sigfox	Star, Mesh, and	1 Mbps	LPWAN	868 or 902	Sigfox	30-50 Km in rural, 3-10 Km in urban	Low
Bluetooth	Star, Mesh, and P2P	1 Mbps	WPAN	2.4 Ghz	IEEE 802.15.4	15-30 M	Low
RFID	P2P	4 Mbps		902-928 MHz	RFID	1.5 m	Low
Zigbee	Star, Mesh cluster network	250 Kbps	WPAN	868/915 MHz-2.4 GHz	IEEE 802.15.4	10-300 m	Very Low
Wi-Fi		11-105 Mbps		2.4 GHz, 5.8 GHz	Wi-Fi Alliance		
Z-Wave	Mesh	40 Kbps	WPAN	868.42 MHz	Z-wave	30 Indoor, 100 outdoor	Very Low
NFG	P2P	424 Kbps	P2P network	860 MHz	ISO/IEC 14443 ISO/IEC 18092	Up To 10 cm	Low

compensation and expedites the intervention required, thus significantly enhancing patient care [36].

However, robust and dependable connectivity is necessary for RPM's successful implementation and operation. Connectivity is the foundation of RPM system that allows for the seamless transmission of patients' health information from electronic devices to healthcare providers. Without dependable connectivity, RPM system becomes ineffective and impedes the transmission and analysis of patients' health data in real-time [35].

2.2.1 IoT-Based RPM Communication Requirements

The evaluation of IoT communication technology considers several factors. While the internet is the primary connectivity medium, RPM devices may also use Bluetooth or Zigbee for device-to-device communication. Additionally, they must support standard data transmission protocols and be compatible with the home network environment of the patients [8]. Furthermore, the quality of care these systems provide can be compromised but limit their potential benefits [10]. Therefore, it is essential to highlight the uniqueness of the feature of the communication technology for IoT-based RPM that must be considered while designing a new system. Table 2 illustrates these criteria.

The requirements for IoT Communication in RPM are comprehensive, interdependent and focus on addressing specific healthcare issues.

Scalability: This refers to the system's ability to manage an increasing number of devices or a growing volume of data without sacrificing functionality or performance [3]. Scalability has become a significant concern with the proliferation of IoT devices in healthcare, especially in RPM [35]. The scalability of RPM system communication is crucial for the purpose of expansion [43]. The scalability can be critically analysed from multiple angles, such as data transmission and device compatibility [44]. *Data Transmission*: Scalability directly impacts the efficiency of data acquisition and transmission, which are essential components of RPM. Without scalable IoT communication, the data transmission process may become slower and data may be lost or delayed as the number of monitored patients increases [44]. *Device Compatibility:* Supporting various IoT devices may include wearable sensors, implanted equipment and portable instruments; each generating data in a unique format and communicating using distinct protocols [1]. A scalable IoT communication infrastructure must support interoperability between these disparate devices, thus enabling them to communicate and exchange data effectively [44].

Reliability: The relationship between IoT communication and RPM reliability is crucial. Since remote healthcare monitoring heavily depends on accurate and timely communication between IoT devices and healthcare providers, the efficacy of RPM is inextricably linked to the reliability of IoT communication [38].

Data Rate: In IoT communication technology, the data rate is a crucial parameter that influences the effectiveness and reliability of the RPM system. Higher data rate facilitates rapid and seamless transmission of data, ensures real-time monitoring and is highly advantageous in healthcare settings where any delay can lead to severe consequences. Decreasing data rate, on the other hand, may lead to lags, delays and data loss, thus resulting in inefficient monitoring and potentially jeopardising patients' health.

Latency: Reduced latency in IoT communication technology can revolutionise RPM system. Reduced latency means quicker data transmission, which in turn means quicker responses to changes in a patient's health status. Simultaneously, technologies such as message queuing telemetry transport (MQTT) are used to receive and analyse patients' vital signs and reduce signal transmission latency. However, the primary obstacle is network reliability. Although technologies like MQTT seek to reduce latency, network reliability remains crucial [45].

Energy Efficiency: This affects the stability and relia-

Table 2. IoT-based RPM communication requirements

Requirements	IoT Communication for Remote Patient Monitoring (RPM)
Scalability	Highly scalable, as RPM systems need to manage a significant amount of patient data across various locations [37].
Reliability	Extremely high reliability is required because these systems deal with critical health data. Any failure in transmission or analysis can have serious consequences [38].
Data Rate	The data rate required can be high, especially for devices that monitor patients' health in real-time [39].
Latency	Low latency is necessary, particularly for critical monitoring and real-time applications [40].
Energy Efficiency	High energy efficiency is essential, especially for wearable and implanted devices that run on batteries [41].
Security	Since this system handles sensitive health data, it must be highly secured to protect patients' confidentiality and data integrity [42].
Range	The required range can be extensive so that the patients can be monitored from anywhere including their homes [33].

bility of RPM system that relies heavily on IoT devices. These devices, which are frequently battery-powered and portable, must efficiently manage energy consumption to operate for extended periods. RPM system utilises IoT technology, chiefly LPWAN such as LoRaWAN, Sigfox and NB-IoT due to their low-power consumption and long-range capabilities [46]. These power-efficient technologies enable reliable data transmission between remote sensors and healthcare providers. Energy efficiency should be considered when selecting the communication technology for RPM system. Energy performance metrics become essential in this regard. Specifically, the study cited in [39] discovered that LoRaWAN and DASH7 are more energy-efficient than Sigfox and NB-IoT. Therefore, selecting the most suitable technology can optimise the energy efficiency of the complete system, allowing for efficient RPM. However, with the introduction of newer technologies such as 6G, the energy efficiency of IoT communications is anticipated to increase considerably [47]. This development directly improves the efficacy of RPM system by increasing device stability, data transmission rate and overall reliability.

Security: Providing data privacy and security is one of the most challenging aspects of implementing IoT-based healthcare system [48, 49]. The interdependence of vital medical devices with other systems in different network layers presents opportunities for remote adversaries, thus making security an urgent concern [49].

Range: RPM entails the collection, exchange, evaluation and transmission of patient's health information from electronic devices such as ubiquitous sensors, implanted equipment and portable instruments [50]. The data is collected remotely and transmitted to healthcare providers in different locations in order for this technology to be effective [33]. In this context, range refers to the distance over which IoT devices can effectively transmit the collected health data to the required receiving end, for example data centre of a healthcare provider [12]. The greater the range, the further away the patients can be tracked and monitored while transmitting their health information. Greater range ensures that data can be collected and transmitted consistently and uninterruptedly. This is essential in monitoring patients' health status and conditions [9].

3. Methodology

This paper employed secondary research which is a standard method of investigation that relies solely on the collection of previous research data. It began with a comprehensive review of secondary literature on IoT communication technologies emphasising on identifying the main features or characteristics of each communication instrument. The next step involved identifying the main requirements of these technologies when implementing the RPM system. Publications were gathered from diverse secondary sources, including academic journals, conferences and technical reports. Additionally, several databases, including IEEExplore, Google Scholar and Scopus were consulted throughout the review.

4. Results and Discussion

RPM involves electronic devices to collect, transmit, evaluate and communicate patients' health data. These devices consist of wearable sensors, implantable apparatus or handheld instruments. Healthcare providers can evaluate the collected data and patients can be notified on the relevant, data-driven insights and interventions. Thus, the optimal communication technology for this purpose depends on the circumstances and patients' requirements including range, data rate, reliability and energy efficiency.

Cellular Network 3G, 4G and 5G cellular networks are optimal for densely populated urban areas with solid cellular coverage. These networks support cardiac, glucose and respiratory monitoring applications that require real-time data transmission [51]. They provide high data rate and dependability, thus efficiently transmitting a large amount of medical data. LoRaWAN is suitable for the transmission of non-real-time data in large rural areas. It can be effectively utilised for monitoring the movement and activities of elderly patients in order to monitor their health. This technology provides the requisite range and coverage for remote areas. NB-IoT is well-suited for infrequent, dependable communication, making it suitable for rural daily vital sign monitoring applications. It provides a cost-effective solution for RPM and disease management such as patients with chronic diseases.

Sigfox is efficient at transmitting small quantities of data, making it ideal for simple alert system, fall detection and rural activity monitoring. Its minimal power consumption and extensive range makes it ideal for remote monitoring applications. Bluetooth is best adapted for short-range, high-data rate applications. It can be applied to ubiquitous medical devices such as heart rate monitors, fitness trackers and sleep monitors. These devices can transmit data for further analysis and monitoring to a patient's smartphone or a local gateway device. RFID technology is suitable for close-range applications in a hospital environment. It can be used for medication usage monitoring and patient's identification. RFID enables accurate and efficient monitoring of medical assets and patient's data within a limited range. Zigbee and Z-Wave can create mesh network monitoring devices in a home or hospital setting. These technologies balance range, power con-

Table 3. IoT communication technologies and their examples of applications

Communication Technology	Application	References
Cellular Network (3G, 4G, 5G)	Urban Areas	[51–53]
LoRaWAN	Rural Areas	[54, 55]
NB-IoT	Chronic Disease Management	[56]
Sigfox	Alert Systems	[57, 58]
Bluetooth	Wearable Devices	[59, 60]
RFID	Hospital Settings	[31, 61]
Zigbee and Z-Wave	Home Health Monitoring	[62, 63]
Wi-Fi	Home Monitoring	[64, 65]
NFC	Short-Range Communication	[66]

sumption and data rate, thus making them suitable for home health monitoring applications. Wi-Fi technology is appropriate for RPM in a patient's residence. It enables various health monitoring devices to transmit real-time data to healthcare providers. Wi-Fi offers dependable and rapid data transmission for continuous monitoring and prompt intervention. NFC is used in situations that require short-range communication, such as transmitting data from wearable device to smartphone, or reading data from implanted device. In clinical setting, NFC technology also facilitates patient's identification.

5. Conclusion

This paper emphases on the importance of IoT communication technology in advancing the healthcare industry, particularly RPM. Researchers' evaluations have demonstrated that selecting and designing IoT communication technology for RPM requires a comprehensive understanding of multiple factors, including scalability, reliability, data rate, latency, energy efficiency, security and range. As discovered, these factors are crucial towards a successful deployment of RPM system. Nonetheless, this paper also demonstrates that mere comprehension of these technological characteristics is insufficient. Effective implementation of RPM system requires a set of well-balanced factors; each contributing to the system's overall performance and effectiveness. This conclusion calls attention to the scope of additional research in IoT communication technology with intent to advance remote patient care in healthcare to unheard-of heights, thereby contributing to a healthier global community.

References

[1] S. S. Shree and J. F. G. Poovathy, "Communication technologies in iot and related concepts: A review," in *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*. IEEE, 2022, pp. 310–314.

[2] J. T. Kelly, K. L. Campbell, E. Gong, and P. Scuffham, "The internet of things: Impact and implications for health care delivery," *Journal of medical Internet research*, vol. 22, no. 11, p. e20135, 2020.

[3] M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik, and Y. Le Moullec, "A survey on the roles of communication technologies in iot-based personalized healthcare applications," *IEEE Access*, vol. 6, pp. 36 611–36 631, 2018.

[4] S. Razdan and S. Sharma, "Internet of medical things (iomt): Overview, emerging technologies, and case studies," *IETE technical review*, vol. 39, no. 4, pp. 775–788, 2022.

[5] A. A. Bahashwan, M. Anbar, N. Abdullah, T. Al-Hadhrami, and S. M. Hanshi, "Review on common iot communication technologies for both long-range network (lpwan) and short-range network," in *Advances on Smart and Soft Computing: Proceedings of ICACIn 2020*. Springer, 2021, pp. 341–353.

[6] B. Pradhan, S. Bhattacharyya, and K. Pal, "Iot-based applications in healthcare devices," *Journal of healthcare engineering*, vol. 2021, pp. 1–18, 2021.

[7] M. O. Qays, I. Ahmad, A. Abu-Siada, M. L. Hossain, and F. Yasmin, "Key communication technologies, applications, protocols and future guides for iot-assisted smart grid systems: A review," *Energy Reports*, vol. 9, pp. 2440–2452, 2023.

[8] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of things (iot) communication protocols," in *2017 8th International conference on information technology (ICIT)*. IEEE, 2017, pp. 685–690.

[9] A. Čolaković, A. H. Džubur, and B. Karahodža, "Wireless communication technologies for the internet of things," *Science, Engineering and Technology*, vol. 1, no. 1, pp. 1–14, 2021.

[10] N. Verma, S. Singh, and D. Prasad, "A review on existing iot architecture and communication protocols used in healthcare monitoring system," *Journal of The Institution of Engineers (India): Series B*, vol. 103, no. 1, pp. 245–257, 2022.

[11] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5g in the internet of things era: An overview on security and privacy challenges," *Computer Networks*, vol. 179, p. 107345, 2020.

[12] F. S. D. Silva, E. P. Neto, H. Oliveira, D. Rosário, E. Cerqueira, C. Both, S. Zeadally, and A. V. Neto, "A survey on long-range wide-area network technology optimizations," *IEEE Access*, vol. 9, pp. 106 079–106 106, 2021.

[13] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, "A survey of lorawan for iot: From technology to application," *Sensors*, vol. 18, no. 11, p. 3995, 2018.

[14] M. Wooldridge, "Introduction to lora," 2003.

[15] A. Brdulak, "Characteristics of narrowband iot (nb-iot) technology that supports smart city management, based on the chosen use cases from the environment area," *Journal of Decision Systems*, vol. 29, no. sup1, pp. 489–496, 2020.

[16] C. B. Mwakwata, H. Malik, M. Mahtab Alam, Y. Le Moullec, S. Parand, and S. Mumtaz, "Narrowband internet of things (nb-iot): From physical (phy) and media access control (mac) layers perspectives," *Sensors*,

vol. 19, no. 11, p. 2613, 2019.
[17] H. Malik, M. M. Alam, Y. Le Moullec, and A. Kuusik, "Narrowband-iot performance analysis for healthcare applications," *Procedia computer science*, vol. 130, pp. 1077–1083, 2018.
[18] V. Kumar, R. K. Jha, and S. Jain, "Nb-iot security: A survey," *Wireless Personal Communications*, vol. 113, pp. 2661–2708, 2020.
[19] F. Pitu and N. C. Gaitan, "Surveillance of sigfox technology integrated with environmental monitoring," in *2020 International Conference on Development and Application Systems (DAS)*. IEEE, 2020, pp. 69–72.
[20] A. Lavric, A. I. Petrariu, and V. Popa, "Long range sigfox communication protocol scalability analysis under large-scale, high-density conditions," *IEEE Access*, vol. 7, pp. 35 816–35 825, 2019.
[21] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of lpwan technologies for large-scale iot deployment," *ICT express*, vol. 5, no. 1, pp. 1–7, 2019.
[22] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovács, P. Mogensen, and M. Sorensen, "Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot," in *2017 IEEE 85th vehicular technology conference (VTC Spring)*. IEEE, 2017, pp. 1–5.
[23] R. Fujdiak, P. Blazek, K. Mikhaylov, L. Malina, P. Mlynek, J. Misurec, and V. Blazek, "On track of sigfox confidentiality with end-to-end encryption," in *Proceedings of the 13th international conference on availability, reliability and security*, 2018, pp. 1–6.
[24] I. Sergi, T. Montanaro, A. T. Shumba, M. C. Gammariello, E. Imperiale, and L. Patrono, "A literature review on outdoor localization systems based on the bluetooth technology," in *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)*. IEEE, 2022, pp. 1–5.
[25] R. A. Gheorghiu and V. Iordache, "Analysis of the possibility to implement zigbee communications in road junctions," *Procedia engineering*, vol. 181, pp. 489–495, 2017.
[26] A. S. Deese and J. Daum, "Application of zigbee-based internet of things technology to demand response in smart grids," *IFAC-PapersOnLine*, vol. 51, no. 28, pp. 43–48, 2018.
[27] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "Iot: Communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, 2023.
[28] Y. Cui, F. Liu, X. Jing, and J. Mu, "Integrating sensing and communications for ubiquitous iot: Applications, trends, and challenges," *IEEE Network*, vol. 35, no. 5, pp. 158–167, 2021.
[29] H. Pirayesh, P. K. Sangdeh, and H. Zeng, "Coexistence of wi-fi and iot communications in wlans," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7495–7505, 2020.
[30] A. Souri, A. Hussien, M. Hoseyninezhad, and M. Norouzi, "A systematic review of iot communication strategies for an efficient smart environment," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3736, 2022.
[31] L. Profetto, M. Gherardelli, and E. Iadanza, "Radio frequency identification (rfid) in health care: where are we? a scoping review," *Health and Technology*, vol. 12, no. 5, pp. 879–891, 2022.
[32] D. K. Singh and R. Sobti, "Wireless communication technologies for internet of things and precision agriculture: A review," in *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*. IEEE, 2021, pp. 765–769.
[33] F. A. C. d. Farias, C. M. Dagostini, Y. d. A. Bicca, V. F. Falavigna, and A. Falavigna, "Remote patient monitoring: a systematic review," *Telemedicine and e-Health*, vol. 26, no. 5, pp. 576–583, 2020.
[34] A. N. Barakat, T. M. Ambark, and K. A. Bozed, "Remote healthcare monitoring system using iot platform," in *The 7th International Conference on Engineering & MIS 2021*, 2021, pp. 1–5.
[35] E. E. Thomas, M. L. Taylor, A. Banbury, C. L. Snoswell, H. M. Haydon, V. M. G. Rejas, A. C. Smith, and L. J. Caffery, "Factors influencing the effectiveness of remote patient monitoring interventions: a realist review," *BMJ open*, vol. 11, no. 8, p. e051844, 2021.
[36] L. Bezerra Giordan, H. L. Tong, J. J. Atherton, R. Ronto, J. Chau, D. Kaye, T. Shaw, C. Chow, and L. Laranjo, "The use of mobile apps for heart failure self-management: systematic review of experimental and qualitative studies," *JMIR cardio*, vol. 6, no. 1, p. e33839, 2022.
[37] M. M. H. Mia, N. Mahfuz, M. R. Habib, and R. Hossain, "An internet of things application on continuous remote patient monitoring and diagnosis," in *2021 4th international conference on bio-engineering for smart technologies (BioSMART)*. IEEE, 2021, pp. 1–6.
[38] A. Rghioui, A. Naja, J. L. Mauri, and A. Oumnad, "An iot based diabetic patient monitoring system using machine learning and node mcu," in *Journal of Physics: Conference Series*, vol. 1743, no. 1. IOP Publishing, 2021, p. 012035.
[39] O. S. Albahri, A. Zaidan, B. Zaidan, M. Hashim, A. S. Albahri, and M. Alsalem, "Real-time remote health-monitoring systems in a medical centre: A review of the provision of healthcare services-based body sensor information, open challenges and methodological aspects," *Journal of medical systems*, vol. 42, pp. 1–47, 2018.
[40] S. S. Kazi, G. Bajantri, T. Thite *et al.*, "Remote heart rate monitoring system using iot," *Techniques for Sensing Heartbeat Using IoT*, vol. 5, no. 04, 2018.
[41] K. L. S. S. v. L. A. J. J. D. L. N. C. O. A. Jarrin R, Barrett MA, "Need for clarifying remote physiologic monitoring reimbursement during the covid-19 pandemic: a respiratory disease case study," *NPJ Digital Medicine*, vol. 4, no. 1, pp. 1–5, 2021.
[42] C. Y. B.-A. L. O. M. Nait Hamoud O, Kenaza T, "Implementing a secure remote patient monitoring system," *Information Security Journal: A Global Perspective*, vol. 32, no. 1, pp. 21–38, 2023.
[43] A. I. Paganelli, P. E. Velmovitsky, P. Miranda, A. Branco, P. Alencar, D. Cowan, M. Endler, and P. P. Morita, "A conceptual iot-based early-warning architecture for remote monitoring of covid-19 patients in wards and at home," *Internet of Things*, vol. 18, p. 100399, 2022.
[44] Y. Liao, C. Thompson, S. Peterson, J. Mandrola, and M. S. Beg, "The future of wearable technologies and remote monitoring in health care," *American Society of Clinical Oncology Educational Book*, vol. 39, pp. 115–121, 2019.
[45] H. H. Alshammari, "The internet of things healthcare monitoring system based on mqtt protocol," *Alexandria Engineering Journal*, vol. 69, pp. 275–287, 2023.
[46] R. K. Singh, P. P. Puluckul, R. Berkvens, and M. Weyn, "Energy consumption analysis of lpwan technologies and lifetime estimation for iot application," *Sensors*, vol. 20, no. 17, p. 4794, 2020.
[47] A. H. Sodhro, S. Pirbhulal, Z. Luo, K. Muhammad, and N. Z. Zahid, "Toward 6g architecture for energy-efficient communication in iot-enabled smart automa-

tion systems," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5141–5148, 2020.
[48] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in iomt communications: A survey," *Sensors*, vol. 20, no. 17, p. 4828, 2020.
[49] M. I. Ahmed and G. Kannan, "Secure and lightweight privacy preserving internet of things integration for remote patient monitoring," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6895–6908, 2022.
[50] L. P. Malasinghe, N. Ramzan, and K. Dahal, "Remote patient monitoring: a comprehensive study," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 57–76, 2019.
[51] P. Kakria, N. Tripathi, and P. Kitipawang, "A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors," *International journal of telemedicine and applications*, vol. 2015, pp. 8–8, 2015.
[52] V. D. Funtanilla, T. Caliendo, and O. Hilas, "Continuous glucose monitoring: a review of available systems," *Pharmacy and Therapeutics*, vol. 44, no. 9, p. 550, 2019.
[53] K. Bayoumy, M. Gaber, A. Elshafeey, O. Mhaimeed, E. H. Dineen, F. A. Marvel, S. S. Martin, E. D. Muse, M. P. Turakhia, K. G. Tarakji *et al.*, "Smart wearable devices in cardiovascular care: where we are and how to move forward," *Nature Reviews Cardiology*, vol. 18, no. 8, pp. 581–599, 2021.
[54] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Viñas, M.-D. Cano, and A. F. Skarmeta, "Performance evaluation of lora considering scenario conditions," *Sensors*, vol. 18, no. 3, p. 772, 2018.
[55] P. Boonyopakorn and T. Thongna, "Environment monitoring system through lorawan for smart agriculture," in *2020-5th International Conference on Information Technology (InCIT)*. IEEE, 2020, pp. 12–16.
[56] Y. Cheng, X. Zhao, J. Wu, H. Liu, Y. Zhao, M. Al Shurafa, and I. Lee, "Research on the smart medical system based on nb-iot technology," *Mobile Information Systems*, vol. 2021, pp. 1–10, 2021.
[57] R. W. Marar, "A sigfox-based blockchain network for electronic health records," in *Proceedings of the 6th International Conference on Algorithms, Computing and Systems*, 2022, pp. 1–5.
[58] T. A. Bach, L.-M. Berglund, and E. Turk, "Managing alarm systems for quality and safety in the hospital setting," *BMJ open quality*, vol. 7, no. 3, p. e000202, 2018.
[59] Z. Li, L. Lian, J. Pei, and Y. She, "Design and implementation of wearable medical monitoring system on the internet of things," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–14, 2021.
[60] F. Subhan, A. Mirza, M. B. M. Suud, M. M. Alam, S. Nisar, U. Habib, and M. Z. Iqbal, "Ai-enabled wearable medical internet of things in healthcare system: A survey," *Applied Sciences*, vol. 13, no. 3, p. 1394, 2023.
[61] D. Mcgonagle, "Since january 2020 elsevier has created a covid-19 resource centre with free information in english and mandarin on the novel coronavirus covid-19," *The COVID-19 resource centre is hosted on Elsevier Connect, the companys public news and information*, 2020.
[62] H. Fernandez-Lopez, J. A. Afonso, J. H. Correia, and R. Simoes, "Remote patient monitoring based on zigbee: Lessons from a real-world deployment," *Telemedicine and e-Health*, vol. 20, no. 1, pp. 47–54, 2014.
[63] M. B. Yassein, W. Mardini, and A. Khalil, "Smart homes automation using z-wave protocol," in *2016 International Conference on Engineering & MIS (ICEMIS)*. IEEE, 2016, pp. 1–6.
[64] S. Iranpak, A. Shahbahrami, and H. Shakeri, "Remote patient monitoring and classifying using the internet of things platform combined with cloud computing," *Journal of Big Data*, vol. 8, pp. 1–22, 2021.
[65] F. Dahan, R. Alroobaea, W. Alghamdi, M. K. Mohammed, F. Hajjej, K. Raahemifar *et al.*, "A smart iomt based architecture for e-healthcare patient monitoring system using artificial intelligence algorithms," *Frontiers in Physiology*, vol. 14, p. 1125952, 2023.
[66] H. R. Hossein, "Sphms: Smart patient m-healthcare monitoring system with nfc and iot," *Int. J. Comput. Appl. Technol. Res*, vol. 4, no. 12, pp. 956–959, 2015.