International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 03 March 2024
Page No: 425 - 430
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0062

Opportunities and Challenges in the Implementation of IoT Applications for Health Monitoring of Elderly People in the Indian Scenario

Mukesh Kumar[1*]
[1]*Assistant Professor, Computer Science, St. Xavier's College of Management & Technology, Patna, Bihar, India.*
Emails: *mukeshkumar@sxcpatna.edu.in*[1]
***Orcid ID**: https://orcid.org/0009-0005-3983-0786*

Abstract
The Internet of Things (IoT)-based health monitoring has emerged as a transformative paradigm in healthcare, especially when it comes to tracking the health of senior citizens. The aging population in India is on the rise, necessitating the development of effective and scalable solutions to address the healthcare needs of the elderly. In this regard, IoT applications present promising prospects by facilitating early identification of medical problems, timely intervention, and continuous, real-time health monitoring. IoT applications can be customized to suit the varying needs of rural and urban population. However, the implementation of IoT applications in the healthcare sector in India comes with its own set of challenges. Issues related to infrastructure, data security, and the privacy concerns need to be carefully addressed to ensure the successful deployment and sustained effectiveness of these technologies. The majority of the Indian population resides in villages; therefore, cost effectiveness is also a major concern for rural population. This paper explores the opportunities and challenges associated with the implementation of IoT applications for health monitoring and aim to provide insights for policymakers, healthcare professionals, and technologists to design and implement IoT-based health monitoring systems tailored to the specific needs of the elderly population in India.

Keywords: *Internet of Things (IoT), Health Monitoring, Data Security and Privacy, Healthcare Infrastructure*

1. Introduction

The Internet of Things (IoT) is quickly taking over the modern, digitally connected world. Human civilization has always been inventing new technologies that can make its way of living comfortable, efficient, and useful. We are entering a new phase of technological evolution, a phase where the Internet is integrating every part of our lives. From smart homes to industrial automation, IoT is poised to redefine the way devices communicate, collect, and exchange data, heralding a new era of connectivity and innovation. The Internet of Things refers to a vast network of interconnected devices embedded with sensors, software, and other technologies, enabling them to collect and exchange data over the Internet. The Internet of Things could be better understood with the knowledge of its key components. IoT has four key components:

Sensors and Actuators: IoT devices use sensors as their eyes and ears to gather information from their surroundings, such as temperature, humidity, motion, and more. Actuators, on the other hand, enable devices to perform actions based on the data received, such as adjusting thermostat settings or controlling machinery.

Connectivity: To send data to other devices or central servers, Internet of Things devices use a variety of communication protocols. These may include Wi-Fi, Bluetooth, Zigbee, cellular networks, and even satellite communication, depending on the application's requirements.

Data Processing and Analytics: Once data is collected, it undergoes processing and analysis to extract valuable insights. This may involve edge computing, where data is analyzed locally on the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 03 March 2024
Page No: 425 - 430
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0062

device itself, or cloud-based solutions, leveraging the power of remote servers for more extensive data processing.

User Interface: Numerous Internet of Things applications come with user interfaces that let users communicate with devices, keep an eye on performance, and change settings from a distance. These interfaces can take the form of mobile apps, web dashboards, or voice-controlled assistants, offering seamless control and accessibility. IoT (Internet of Things) devices work by connecting physical objects to the internet, enabling them to send and receive data. The data received from IoT devices is typically sent to a cloud platform or server for further processing, storage, and analysis. Finally, end-users' access IoT data and control devices through applications or services [1]. These could be mobile apps, web dashboards, or dedicated software platforms Figure 1. The Internet of Things (IoT) is connecting everything across the world. Healthcare is one of the major concerns for smart cities in India. The Indian healthcare system comprises of public and private healthcare establishments. In India, where access to healthcare facilities can be challenging, the sudden emergence of COVID-19 posed a new threat to the already burdened healthcare system.

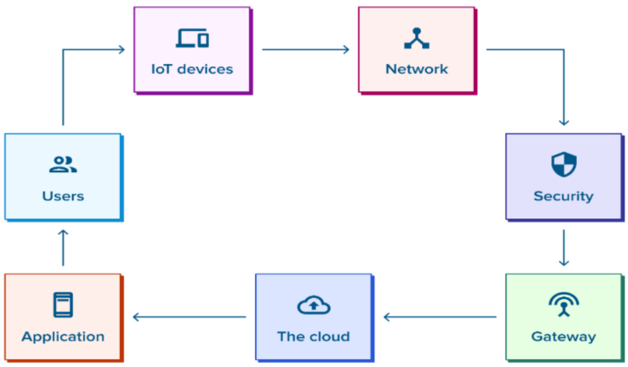

Figure 1 Working of an IoT Application

The pandemic changed the healthcare paradox with newer workplace and societal challenges faced by the healthcare personnel. In any of the smart cities, people want 24/7 health services with efficient and reliable emergency department with real time monitoring. The emergence of IoT and smart sensing technologies revolutionizing the healthcare services. The traditional way of measuring patient health parameters is being replaced by automatic smart sensors. Even for the patient registration to discharge from the hospital we are using several devices to keep track of patient's health records. The future healthcare systems will require more secure, dynamic and personalized services. The future healthcare system should be capable to address sudden challenges such as global pandemics. India has a vast rural population with limited access to healthcare infrastructure. IoT devices can bridge this gap by enabling telemedicine services, where patients can consult with healthcare professionals remotely. Medical sensors could be connected to external gateways through wireless networks and information stored in cloud could be accessible to all medical staff. IoT devices can play a crucial role in monitoring and managing chronic diseases such as diabetes, cardiovascular diseases, and respiratory conditions [2]. IoT technologies can improve the efficiency of healthcare delivery in India by optimizing resource utilization, reducing waiting times, and minimizing administrative overhead. Many IoT solutions are becoming increasingly affordable and scalable, making them suitable for deployment across diverse healthcare settings in India. Moreover, the growing ecosystem of IoT startups and innovation hubs in the country is driving the development of locally relevant solutions tailored to the needs of the Indian healthcare system. In a report published by Ministry of Health and Family Welfare, Govt. of India, 2019-20, India's population is expected to continue growing for the foreseeable future. India's large and growing population will present challenges to the current healthcare system. It can strain resources and infrastructure. IoT (Internet of Things) has the potential to address various challenges associated with a fast-growing population by improving efficiency, resource management, and quality of life. IoT devices can improve access to healthcare services and enhance healthcare delivery for a larger population.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 03 March 2024
Page No: 425 - 430
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0062

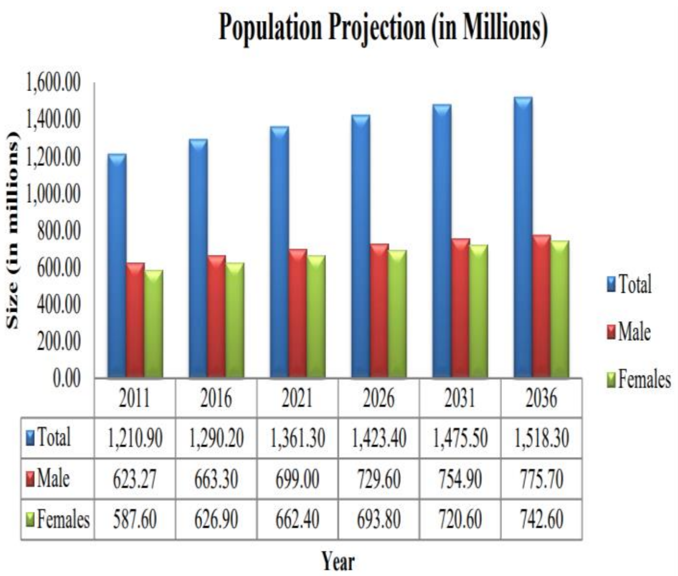

Figure 2 Source: Registrar General & Census Commissioner, India

IoT devices offer numerous benefits for elderly people by providing them with enhanced safety, health monitoring, and assistance in daily living. IoT devices can continuously monitor vital signs such as heart rate, blood pressure, and blood glucose levels. This allows caregivers and healthcare providers to remotely track the health status of elderly individuals and intervene promptly in case of any abnormalities or emergencies. IoT devices can help elderly individuals manage their medications more effectively. Smart pill dispensers [15] can dispense medication doses at scheduled times, remind users to take their medication, and send alerts to caregivers in case of missed doses. Some IoT devices are implanted or attached to the body to monitor specific health conditions continuously. Examples include pacemakers for monitoring heart rhythm, insulin pumps for managing diabetes, and neurostimulators for treating chronic pain or neurological disorders. In Figure 3, a sample IoT device based on Raspberry Pi, could be used efficiently to monitor basic health conditions and send alerts to concerned persons in case of any abnormal condition. However, it's essential to ensure that IoT deployments prioritize privacy, security, and inclusivity to maximize their benefits for all segments of society.

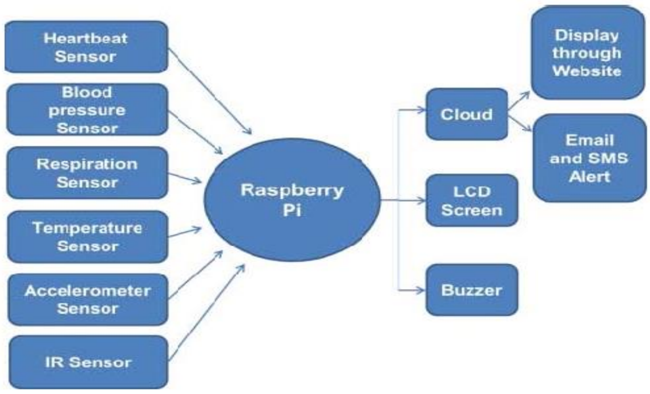

Figure 3 Raspberry Pi Model

2. Challenges in IoT Deployment for Health Services in India

Deploying IoT for health services in India comes with several challenges, and addressing these challenges requires a multi-stakeholder approach involving collaboration between government agencies, healthcare providers, technology vendors, regulatory bodies, and others.

2.1 Infrastructure Limitations

In many parts of India, especially rural areas, there are limitations in infrastructure such as reliable internet connectivity, electricity supply, and access to healthcare facilities. Deploying IoT devices may be challenging in such areas where the basic infrastructure is lacking. As per the Economic Survey 2022-23, 65% of India's population lives in the rural areas and 47% of the population is dependent on agriculture for livelihood [3]. Indian people face problems like availability of pure drinking water, electricity supply and basic health facilities in many areas. Major cities in India generally have well-developed medical facilities, including multi-specialty hospitals, diagnostic centers, and clinics. These facilities often offer advanced medical treatments, state-of-the-art equipment, and access to specialized healthcare professionals. However, many rural areas lack proper healthcare facilities, leading to disparities in healthcare access between urban and rural populations. Mobile health clinics and telemedicine initiatives are being implemented to improve healthcare delivery in remote areas. The Indian government operates a network of primary

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 03 March 2024
Page No: 425 - 430
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0062

health centers (PHCs), community health centers (CHCs), and district hospitals to provide basic healthcare services to the population. While these facilities play a crucial role in delivering healthcare services, they often suffer from underfunding, staffing shortages, and inadequate infrastructure. Registrar General & Census Commissioner, India are shown in Figure 2.

2.2 Data Security and Privacy Concerns

Due to numerous risks, vulnerabilities, cyber-attacks, and threats, security and privacy are among the most significant and difficult IoT issues. IoT devices collect and transmit sensitive health data, including [16] biometric information and medical histories. If these devices are compromised, either through hacking or insecure data transmission, it can lead to data breaches and unauthorized access to personal health information. IoT deployments for health monitoring raise questions about data ownership and consent. Patients may not always be aware of how their data is being collected, stored, and shared, leading to concerns about privacy and consent. Clear policies and consent mechanisms are needed to ensure that patients have control over their health data. It also raises privacy concerns about potential profiling and discrimination based on health data. Compliance with data protection regulations, such as HIPAA in the United States or GDPR in the European Union, is essential for IoT deployments in healthcare. Ensuring compliance with regulatory requirements, [12] such as data encryption, data access controls, and breach notification protocols, is critical to protecting patient privacy and avoiding legal repercussions. One notable example of a data leak in India related to health information is the "Aarogya Setu" app incident. The Aarogya Setu app was launched by the Indian government in April 2020 as a contact tracing tool to help contain the spread of COVID-19. In some of the media publications, it was reported that security vulnerability in the Aarogya Setu app exposed the personal health data of millions of users. The vulnerability allowed attackers to access sensitive user information, including COVID-19 test results, vaccination status, and other personal details. The issue came to light when a French cyber security researcher, Robert Baptiste (also known as Elliot Alderson), discovered the vulnerability and shared it on social media. He demonstrated how an attacker could gain unauthorized access to the health data of users [4].

2.3 User Acceptance and Adoption

Acceptance and adoption of IoT-enabled health services by healthcare providers and patients are crucial for the success of deployments. However, resistance to change, lack of awareness, and cultural factors may hinder adoption and behavior change, requiring targeted education and training initiatives. [5] Awareness about the benefits of IoT health monitoring and education about how to use these technologies are crucial for acceptance and adoption. Public awareness campaigns, training programs for healthcare professionals and community outreach initiatives can help improve understanding and acceptance of IoT health monitoring solutions. In regions with limited access to healthcare facilities, [7] IoT health monitoring can fill gaps in healthcare delivery by enabling remote monitoring and telemedicine services. The level of healthcare accessibility and availability of primary care services can influence the demand for IoT health monitoring solutions. Trust in the security and privacy of IoT health monitoring solutions [6] is essential for adoption. Patients need assurance that their health data will be kept confidential and secure. Cost is another significant barrier to the adoption of IoT devices, particularly for healthcare services in India. Many IoT devices are expensive, making them inaccessible to a large segment of the population, especially those from low-income backgrounds.

3. Opportunities and Benefits of Implementing IoT for Health Monitoring

In a country like India, IoT-based health monitoring presents several opportunities to address some of the unique healthcare [8] challenges and improve healthcare delivery. India has a vast rural population with limited access to healthcare facilities. IoT-based health monitoring can bridge this gap by enabling remote patient monitoring in rural areas.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 03 March 2024
Page No: 425 - 430
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0062

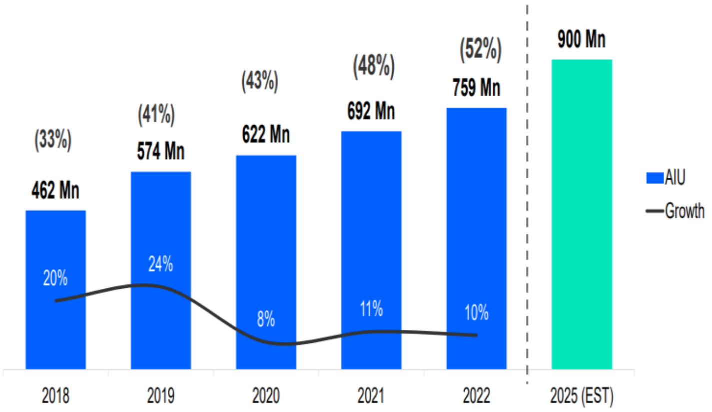

Figure 4 Active Internet Users

3.1 Chronic Disease Management

India is experiencing a growing burden of chronic diseases such as diabetes, hypertension, and cardiovascular diseases. IoT devices can help in the continuous monitoring of patients with chronic conditions, enabling [11] early detection of complications and facilitating personalized disease management strategies. This can lead to better health outcomes and reduced healthcare costs in the long term. The number of internet users in India has been increasing steadily [9] over the years. India has one of the largest and fastest-growing internet user bases globally. According to a report published by Kantar ICUBE [5], 52% Indians are active internet users and it is predicted that 900 million people will have internet access in year 2025 Figure 4. Even rural India continues to drive internet adoption in the country, surpassing urban India and still growing at double rate. IoT-based solutions can monitor maternal health parameters during pregnancy, track fetus development, and provide real-time alerts in case of complications. India faces periodic outbreaks of infectious diseases such as dengue, malaria, influenza and recently Covid-19. IoT-based surveillance systems [13] can monitor environmental factors, track disease vectors, and detect disease outbreaks in real-time. This early warning system can help public health authorities implement timely interventions to control the spread of diseases and prevent epidemics. IoT generates vast amounts [10] of data that can be analyzed to gain insights into population health trends, disease patterns, and healthcare outcomes. By leveraging advanced analytics and machine learning algorithms, healthcare providers can derive actionable insights from IoT data to inform decision-making, improve clinical outcomes, and optimize healthcare delivery. [14]

Source: Kantar ICUBE 2022, All India Population, 1473 million Numbers in bracket indicate Internet Penetrations, AIU=Active Internet Users

Conclusion

In Indian context, the opportunities presented by IoT-based health monitoring are vast and promising. From remote patient monitoring to epidemic surveillance and telemedicine, these technologies have the potential to revolutionize healthcare delivery, improve patient outcomes, and enhance healthcare access across urban and rural areas. However, along with these opportunities, there are significant challenges that need to be addressed. Issues such as data privacy and security, infrastructure limitations, regulatory frameworks, and socioeconomic disparities must be carefully navigated to ensure the successful implementation and adoption of IoT-based health monitoring solutions. Data Security and privacy could be achieved by implementing strong encryption protocols to secure data transmission between IoT devices, gateways, and cloud servers. End-to-end encryption ensures that data remains encrypted throughout its journey, protecting it from unauthorized access or interception. Ensure that IoT devices are securely provisioned and on boarded onto the network. Use secure boot mechanisms and unique device identifiers to verify the authenticity and integrity of devices before allowing them to connect to the network. Despite these challenges, the momentum towards leveraging IoT in healthcare is undeniable, driven by a growing recognition of its transformative potential and the urgent need to address healthcare gaps in India. By addressing these challenges through collaborative efforts involving government, industry, healthcare providers, and communities, India can harness the full potential of IoT-based health monitoring to build a more

e ISSN: 2584-2137
Vol. 02 Issue: 03 March 2024
Page No: 425 - 430
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0062

resilient, accessible, and effective healthcare system for the future.

References

[1]. https://www.oracle.com/in/internet-of-things/what-is-iot/ Accessed on 10 Feb 2024.

[2]. Varshney U. Pervasive Healthcare and Wireless Health Monitoring. Mobile Networks and Applications 2007; 12(2): 113–127. doi: 10.1007/s11036-007-00171

[3]. https://pib.gov.in/PressReleasePage.aspx?PRID=1894932#:~:text=The%20Union%20Minister%20for%20Finance,in%20real%20terms%20in%20FY24. Accessed on 13 Feb 2024.

[4]. https://www.thequint.com/tech-and-auto/tech-news/aarogya-setu-data-breach-reported-by-shadow-map. Accessed on 13 Feb 2024.

[5]. https://economictimes.indiatimes.com/tech/technology/52-of-indian-population-had-internet-access-in-2022-says-report/articleshow/ Accessed on 12 Feb 2024.

[6]. Olivier F, Carlos G, Florent N. New security architecture for IoT network. In: International workshop on big data and data mining challenges on IoT and pervasive systems (BigD2M 2015), procedia computer science, vol. 52; 2015. p.1028–33

[7]. Mamdiwar S.D., Shakruwala Z., Chadha U., Srinivasan K., Chang C.-Y. Recent advances on IoT-assisted wearable sensor systems for healthcare monitoring. Biosensors. 2021; 11:372. Doi: 10.3390/bios11100372.

[8]. Pal A., Visvanathan A., Choudhury A.D., Sinha A. Improved heart rate detection using smart phone; Proceedings of the 29th Annual ACM Symposium on Applied Computing; Gyeongju, Korea. 24–28 March 2014; pp. 8–13.

[9]. Goyal S., Sharma N., Bhushan B., Shankar A., Sagayam M. Cognitive Internet of Medical Things for Smart Healthcare. Springer; Berlin/Heidelberg, Germany: 2021. IoT enabled technology in secured healthcare: Applications, challenges and future directions; pp. 25–48.

[10]. Zanella A, Bui N, Castellani A, Vangelista L, Zorgi M. Internet of things for smart cities. IEEE IoT-J. 2014; 1(1):22–32.

[11]. IoT application areas. https://iot-analytics.com/top-10-iot-project-application-areas-q3-2016/. Accessed 12 Feb 2024.

[12]. Li Y, et al. IoT-CANE: a unified knowledge management system for data centric internet of things application systems. J Parallel Distrib Compute. 2019; 131:161–72.

[13]. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for internet of things. J Netw Compute Appl. 2014; 42:120–34.

[14]. Pereira C, Aguiar A. Towards efficient mobile M2M communications: survey and open challenges. Sensors. 2014; 14(10):19582–608.

[15]. Colacovic A, Hadzialic M. Internet of things (IoT): a review of enabling technologies, challenges and open research issues. Compute Netw. 2018; 144:17–39.

[16]. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, Oct 2017.