Intelligent Internet of Medical of Things: Future Challenges

Vineet Kohli

Gadhwal Technical College, India

Abstract

IIOMT includes medical sensors and other medical devices. The use of this technology helps to improve patient's health outcomes, as well as reduce medical costs. For example, IOMT can help to collect patient data, diagnose conditions and monitor treatment in real-time. Also, it can help to improve operational efficiencies and reduce human errors. By using IOT medical devices, healthcare providers can remotely monitor the health of their patients. This technology can also help to reduce the manpower required in a medical organization, as it can enable automation of some tasks. Additionally, with IOT, medical organizations can receive real-time alerts that can help to detect any potential issues in patient’s health. This technology can also enable researchers and doctors to gain insights on health related matters. Despite its many potential benefits, IOMT also poses potential security and privacy risks. As the data is collected from connected devices, it is vulnerable to malicious attacks. Furthermore, healthcare organizations have a duty to protect patient’s personal and private data. As such, an effective data security strategy must be in place to ensure that all the gathered data is securely transmitted, as well as stored. Additionally, patient-generated data should also be encrypted to ensure privacy. Ultimately, IOMT provides numerous benefits to healthcare organizations, including improved accuracy and productivity. This technology can also help to reduce medical costs and improve patient outcomes. However, to ensure the safety and security of IOMT, healthcare providers must ensure that their systems are properly secured and that their data security protocols are regularly updated. By properly utilizing IOMT and enforcing the necessary security measures, healthcare organizations can be assured that their data remains secure and that their patients are provided with the best possible care.Additionally with this work healthcare practitioners will be able to identify the potential security and data privacy challenges associated with IOT and how to address them.

Keywords: IIOMT, IOT, Sensors, Healthcare

Introduction

IoT devices serve many functions, ranging from collecting and processing data, to controlling systems and devices remotely, to automating tasks [1]. IoT technology can be used in virtually any industry, from healthcare and agriculture to manufacturing and automobiles [2]. It enables businesses to communicate with customers directly and to share data in real time. IoT also has potential to help reduce waste, improve operational efficiency, and eliminate inefficiencies [3].

By enabling electronic devices to exchange data between one another, IoT makes it possible for organizations to automate processes, monitor and control systems, and access real-time information [4]. With specific domain applications, IoT can be used to improve customer experience, reduce costs, and increase efficiency. This includes applications such as tracking products through the supply chain, automating medical and agricultural processes, and collecting and analyzing data for industrial purposes [5].

It has enabled more efficient communication and data sharing across various types of connected devices [6]. It enables the communication and exchange of data between different devices and provides greater convenience, safety, and efficiency in our lives. It also helps in better managing energy and resources, due to its ability to monitor, control and manage the usage of resources [7]. IoT also helps in providing better security, because of its ability to identify situations and alert users in case of any mishap. Moreover, IoT is also helping in providing a better customer experience, as it can provide users with personalized services, as well as help businesses to better understand customer behaviour, which in turn helps them to respond to customer needs more effectively [8].

The demand for personal healthcare applications is expected to increase drastically due to the onset of the Covid-19 pandemic. In addition to providing remote monitoring and diagnostic capabilities, personal healthcare applications are becoming increasingly important for maintaining social distancing measures and providing information on the virus [9]. Additionally, these applications can help individuals monitor their own health and medical status, as well as provide feedback on treatments and therapies. Furthermore, with advancements in biometric technology, such as facial recognition, these applications can provide added security and convenience, allowing users to access their health records with ease. Consequently, the increasing demand for personal healthcare applications is expected to lead to a surge in the adoption of Internet of Things technology [10].This is because with the help of Internet of Things, it is possible to monitor patients remotely and provide individualized health care. This will enable doctors to detect abnormalities in patients more quickly, allowing for timely interventions [11]. Moreover, IoT devices can be used to monitor elderly individuals, ensuring their safety, as well as guaranteeing their comfort and security. Additionally, IoT can also be utilized for decreased energy consumption, as well improved traffic management in urban areas [12].

In this research we will also be talking about the advances of IOT in the healthcare sector, such as its remote monitoring capabilities, data security and privacy, and better patient experience [13]. We will also address the potential risks associated with IOT, such as data hacks and privacy violations. Finally, we will discuss the implications of IOT for healthcare stakeholders, such as doctors, hospitals and insurance companies [14].

IoT is described as a network of physical objects connected through internet technology, enabling the exchange of data and information in real time. Therefore, in the healthcare industry, IoT can bring the healthcare sector into the next level by its remote monitoring capabilities, improved data security and privacy, and creation of better patient experience [15].

First, by establishing a secure connection between medical devices and the patient, medical professionals are able to monitor the health status of their patients remotely. IoT-enabled devices can also alert healthcare providers when a patient indicates signs of any medical condition [16]. For example, biometric devices measure the patient’s key vital signs, such as body temperature and heartbeat, and can send an alert to the doctor whenever an abnormality is detected. This kind of technology can greatly improve the quality of care, as well as provide a preventive approach to health management [17].

Second, IoT can help improve data security and privacy for patients. By connecting medical devices to IoT systems, medical data can be collected, transmitted, and stored in a secure way [18]. IoT-enabled medical devices can also help to protect against data theft and unauthorized access, as encrypted communication protocols can be used to make sure data is sent only to authorized sources [19].

Third, IoT can help to create a better patient experience. By providing an interactive platform on mobile devices and computers, patients can access their medical records, contact their physicians, track their health over time, and receive personalized prescriptions [20]. Furthermore, they are able to better manage their own health, as they have access to more data and can better understand the implications of their decisions [21].

Despite the potential of IoT in the healthcare sector, there could be some potential risks when using the technology. Data hacks or privacy violations can occur due to lack of data security or unauthorized access [22]. Furthermore, medical data stored in the cloud can be subject to data breaches. As such, it is important to ensure that measures are taken to protect the security of medical data in order to ensure patient privacy [23].

Finally, stakeholders in the healthcare industry must be aware of the implications of introducing IoT into the healthcare sector [24]. This includes understanding how the technology can improve patient experiences, how data security can be improved, and how patient data can be collected, stored and used in a secure way [25]. Furthermore, healthcare providers must also consider the potential costs associated with incorporating this technology and whether any additional training is needed for healthcare staff in order to use the technology effectively [26].

IoT holds great potential to improve and revolutionize the healthcare sector. By providing remote monitoring capabilities, improved data security and privacy, and better patient experiences [27]. However, responsible implementation of the technology is still necessary in order address potential security and privacy concerns [28]. If stakeholders in the healthcare industry take the appropriate measures to ensure data security and to protect patients’ privacy, they can reap the benefits of using this technology while maintaining the highest standards of healthcare practices [29].

IOT Practices in Healthcare

IoT has become highly important in the healthcare industry due to its potential to improve access to care, increase efficiency, and minimize costs [30]. Using IoT, healthcare providers are able to collect, analyze and share data more efficiently. Additionally, these solutions enable more effective and personalized treatments, as medical professionals can monitor, diagnose and treat patients more accurately [31].

One of the main applications for IoT in healthcare is remote patient monitoring. Devices such as smart watches and sensors can be used to monitor the patient’s vital signs and physical activity levels, providing physicians and nurses with real-time patient information [32]. This type of health monitoring has allowed for greater accessibility and convenience for both patients and healthcare professionals [33].

IoT solutions can also be used to reduce care delivery costs. Healthcare providers can collect data from a variety of sources in order to gain insight into the processes and activities that are associated with providing care, such as hospital utilization, number of patients, diagnostic tests, and symptoms [34]. This data can allow providers to identify areas in which they can improve operational efficiency, such as by streamlining processes or scheduling more efficiently.

IoT solutions are also used to provide better patient care [35]. For example, IoT solutions can provide data on medical imaging results, allowing healthcare providers to make more accurate and timely diagnoses. Additionally, AI technologies can be used to process patient data to predict potential health risks and determine appropriate interventions [36].

In short, IoT solutions have the potential to revolutionize healthcare, providing patients with greater access to care, more personalized treatments, and cost-effective care delivery models [37,38].

Challenges of IOT in Healthcare

One of the biggest challenges of IoT in healthcare is data privacy and security. Since IoT is an interconnected network of devices, it opens up new opportunities for data breaches and malicious activity. In the healthcare industry, these breaches can be extremely detrimental, as patient information is often very sensitive [39]. As such, implementing security measures such as encryption and authentication is essential. Additionally, healthcare providers must adhere to strict regulations such as HIPAA and GDPR to ensure that patient data is protected.

Another challenge is device compatibility. Different devices and systems may collect and store data in different formats, making it difficult to integrate the data into a unified system. Additionally, some existing healthcare systems are not designed to support the latest technology, and they may not be able to accommodate the integration of new IoT devices and data. Additionally, device connectivity can be an issue, as many healthcare systems rely on wifi and Bluetooth connections [40].

IoT have many advantages which make ease the life of patient, doctor and health care organization. It help in improved treatment decisions, more proactive care, better outcomes, and more efficient operations. It also facilitates patient homes with wearable and assistive technologies. Smart device trackers can alert healthcare providers about the changes in patient health and lifestyle. Most important advances are that IoT supports automation that enhances the connection between patient, care provider and technology [41].

The biggest challenge for IoT in healthcare is data privacy and security. As the healthcare industry deals with sensitive and confidential information, a small compromise in the security of these records can be disastrous. The data collected through IoT devices must be sufficiently encrypted and secure from any potential breaches. The healthcare organizations using these devices must satisfy compliance regulations, like HIPAA and GDPR, to protect patient data.

Another major challenge is the compatibility of different devices and systems. Many of the existing healthcare systems are not designed to be used with the latest technology. It can be difficult to connect IoT devices to them and to ensure the compatibility of data collected and stored by these systems.

Finally, there is the issue of scalability. IoT solutions require vast amounts of data to be stored and analyzed. This can cause a strain on the resources of healthcare organizations and create difficulties in assuring the security of these data [41].

Benefits of IOT in Healthcare

1. On-Time Patient Data: IoT can provide health care professionals with immediate access to patient info, enabling them to decide more effectively and judiciously. This can enable them to track the progress of the patient remotely and deliver more personalized care.

2. Enhanced Patient Experiences: Patients can also benefit from the use of IoT, as it can provide them with more convenient access to their medical records and treatments. Additionally, wearable devices can provide real-time data on changes in the patient’s health and alert them about potential complications.

3. Remote Monitoring: Healthcare professionals can monitor patient data and activity from remote locations, and even remotely administer treatments if necessary. This eliminates the need to visit a patient’s home or facility, which can help decrease costs and improve efficiency.

4. Automation: IoT can automate medical processes, such as the ordering of medical supplies and the functioning of medical equipment, thereby eliminating the need for manual records. This helps to reduce waste, maximize efficiency, and free up resources.

5. Reduced Healthcare Costs: As mentioned earlier,

IoT can help reduce costs by streamlining processes and eliminating the need for manual labour. In addition, it can help reduce the costs associated with hospital stays and visits by enabling care to be delivered at home [42].

Conclusion

We discussed potential practices and benefits of IOT in healthcare, ranging from real-time patient data access to reduced healthcare costs. We also discussed some of the challenges associated with their use, such as the need for data security and privacy, as well as the need for training and education. We concluded that despite these challenges, the use of IoT in healthcare holds great promise, and provides an opportunity to deliver better patient care at a lower cost.

We also discussed the need to ensure the security and data privacy while considering the use of IOT in healthcare. The challenges associated with the use of IOT should be dealt with due to their importance in medical applications. Finally, we concluded that incorporating the use of IOT in healthcare can promise to deliver cost-effective, patient-oriented care.

References

[1]. Rathore, R.S., Sangwan, S. and Kaiwartya, O., 2021. Towards Trusted Green Computing for Wireless Sensor Networks: Multi Metric Optimization Approach. *Adhoc& Sensor Wireless Networks*, *49*.

[2]. Rathore, B., 2023. Textile Industry 4.0: A Review of Sustainability in Manufacturing. *International Journal of New Media Studies (IJNMS)*, *10*(1), 38–43.

[3]. Fabijan A. Corneal endothelium image segmentation using feedforward neural network: Proceedings of the Federated Conference onComputer Science and Information Systems; IEEE Cataloge Number, 2017:629-637.

[4]. Rathore, B., 2023. Future of Textile: Sustainable Manufacturing & Prediction via ChatGPT. *International Journal of New Media Studies (IJNMS)*, *10*(2), 58–69.

[5]. Rathore, R.S., Sangwan, S., Kaiwartya, O. and Aggarwal, G., 2021. Green communication for next-generation wireless systems: optimization strategies, challenges, solutions, and future aspects. *Wireless Communications and Mobile Computing*, *2021*, pp.1-38.

[6]. Singh, U.P. and Rathore, R.S., 2012. An efficient distributed group key management using hierarchical approach with ECDH and symmetric algorithm. *J. Comput. Eng. Intel. Syst*, *3*(7), pp.32-41.

[7]. Rathore, B., 2021. Fashion Transformation 4.0: Beyond Digitalization & Marketing in Fashion Industry. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *10*(2), pp.54-59.

[8]. Rattan, V., Sinha, E.M., Bali, V. and Rathore, R.S., 2010. E-Commerce Security using PKI approach. *International Journal on Computer Science and Engineering*, *2*(5), pp.1439-1444.

[9]. Rathore, R.S., Sangwan, S., Mazumdar, S., Kaiwartya, O., Adhikari, K., Kharel, R. and Song, H., 2020. W-GUN: Whale optimization for energy and delay-centric green underwater networks. *Sensors*, *20*(5), p.1377.

[10]. Rathore, R.S., Kaiwartya, O., Qureshi, K.N., Javed, I.T., Nagmeldin, W., Abdelmaboud, A. and Crespi, N., 2022. Towards enabling fault tolerance and reliable green communications in next-generation wireless systems. *Applied Sciences*, *12*(17), p.8870.

[11]. Rathore, B., 2022. Textile Industry 4.0 Transformation for Sustainable Development: Prediction in Manufacturing & Proposed Hybrid Sustainable Practices. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *11*(1), pp.223-241.

[12]. Rathore, R.S., Hewage, C., Kaiwartya, O. and Lloret, J., 2022. In-vehicle communication cyber security: challenges and solutions. *Sensors*, *22*(17), p.6679.

[13]. Khasawneh, A.M., Singh, P., Aggarwal, G., Rathore, R.S. and Kaiwartya, O., 2022. E-Mobility Advisor for Connected and Autonomous Vehicles Environments. *Adhoc& Sensor Wireless Networks*, *53*.

[14]. Kumar, S., Rathore, R.S., Mahmud, M., Kaiwartya, O. and Lloret, J., 2022. BEST—Blockchain-Enabled Secure and Trusted Public Emergency Services for Smart Cities Environment. *Sensors*, *22*(15), p.5733.

[15]. Jha, S.K., Prakash, S., Rathore, R.S., Mahmud, M., Kaiwartya, O. and Lloret, J., 2022. Quality-of-service-centric design and analysis of unmanned aerial vehicles. *Sensors*, *22*(15), p.5477.

[16]. Kumar, M., Kumar, S., Kashyap, P.K., Aggarwal, G., Rathore, R.S., Kaiwartya, O. and Lloret, J., 2022. Green communication in internet of things: A hybrid bio-inspired intelligent approach. *Sensors*, *22*(10), p.3910.

[17]. Rathore, R.S., Sangwan, S., Adhikari, K. and Kharel, R., 2020. Modified echo state network enabled dynamic duty cycle for optimal opportunistic routing in EH-WSNs. *Electronics*, *9*(1), p.98.

[18]. Rathore, R.S., Sangwan, S., Prakash, S., Adhikari, K., Kharel, R. and Cao, Y., 2020. Hybrid WGWO: whale grey wolf optimization-based novel energy-efficient clustering for EH-WSNs. *EURASIP Journal*

on Wireless Communications and Networking, *2020*(1), pp.1-28.

[19]. Singh, U.P. and Rathore, R.S., 2013. Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function. *International Journal of Computer Applications*, *61*(19).

[20]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Routing Protocol for MANETs: A Survey. *IUP Journal of Computer Sciences*, *4*(3).

[21]. Bali, V. and Rathore, R.S., 2010. A NEW HIERARCHICAL TRANSACTION MODEL FOR MOBILE ADHOC NETWORK ENVIRONMENT. *International Journal on Computer Science and Engineering*, *2*(3).

[22]. Singhal, S. and Rathore, R.S., 2015. Detailed Review of Image Based Steganographic Techniques. *IJCST*, *6*, pp.93-95.

[23]. Kumar, V. and Rathore, R.S., 2018, October. Security issues with virtualization in cloud computing. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 487-491). IEEE.

[24]. Sharma, P. and Rathore, R.S., 2015. Three Level Cloud Computing Security Model. *International Journal of Computer Applications*, *119*(2).

[25]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, August. Information Technology Architectures for Grid Computing and Applications. In *2009 Fourth International Multi-Conference on Computing in the Global Information Technology* (pp. 52-56). IEEE.

[26]. Bali, V., Rathore, R.S. and Sirohi, A., 2010. Performance analysis of priority scheme in ATM network. *International Journal of Computer Applications*, *1*(13), pp.26-31.

[27]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009, December. A Framework to Provide a Bidirectional Abstraction of the Asymmetric Network to Routing Protocols. In *2009 Second International Conference on Emerging Trends in Engineering & Technology* (pp. 1143-1150). IEEE.

[28]. Rathore, B., 2022. Impact of Green Marketing on Sustainable Business Development. Cardiff Metropolitan University. Presentation.

[29]. Dixit, R., Gupta, S., Rathore, R.S. and Gupta, S., 2015. A novel approach to priority based focused crawler. *International Journal of Computer Applications*, *116*(19).

[30]. Tomar, R. and Rathore, R.S., 2016. Privacy Preserving in TPA using Secured Encryption Technique for Secure Cloud. *International Journal of Computer Applications*, *138*(8).

[31]. Tomar, R. and Rathore, R.S., 2016. A Survey on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud. *International Advanced Research Journal in Science, Engineering and Technology*, *3*(4), pp.83-86.

[32]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Clustering Technique Approach to Detect the Special Patterns for Medical Video Mining. *Advances in Data Management*, p.140.

[33]. Bali, V., Rathore, R.S., Sirohi, A. and Verma, P., 2009. Architectural Options and Challenges for Broadband Satellite ATM networks. *Recent Developments in Computing and Its Applications*, p.155.

[34]. Rathore, B., 2023. Digital Transformation 4.0: A Case Study of LK Bennett from Marketing Perspectives. *Eduzone: International Peer Reviewed/Refereed MultidisciplinaryJournal*, *12*(1), pp.40-49.

[35]. Bhusan, M., Rathore, R.S. and Jamshed, A., 2018. *Fundamental of Cyber Security: Principles, Theory and Practices*. BPB Publications.

[36]. Srivastava, S.N., Kshatriya, S. and Rathore, R.S., 2017. Search Engine Optimization in E-Commerce Sites. *International Research Journal of Engineering and Technology (IRJET)*, *4*(5), pp.153-155.

[37]. Rathore, B., 2023. Integration of Artificial Intelligence & It's Practices in Apparel Industry. *International Journal of New Media Studies (IJNMS)*, *10*(1), pp.25-37.

[38]. Bali, V., Rathore, R.S. and Sirohi, A., Adaptive Analysis of Throughput in Mobile Admhoc Network (IEEEm802. 11).

[39]. Saxena, S., Rathore, R.S., 2013. *Compiler Design*. S. Chand Publishing.

[40]. Kumar, V. and Singh Rathore, R., 2016. A Review on Natural Language Processing. *International Journal Of Engineering Development And Research*.

[41]. Rathore, B., 2022. Supply Chain 4.0: Sustainable Operations in Fashion Industry. *International Journal of New Media Studies (IJNMS)*, *9*(2), pp.8-13.

[42]. Rathore, B., 2023. Digital Transformation 4.0: Integration of Artificial Intelligence & Metaverse in Marketing. *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal*, *12*(1), pp.42-48.