WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Internet Of Things In Healthcare

Vikash Mall[1],Vikash Kushwaha[2],Vipin Yadav[3], Priyanka Singh[4]

[1,2,3]Student, [4]Assitant Professor

Department of Computer Science and Engineering (IoT), Raj Kumar Goel Institute of Technology, Ghaziabad

[1]vikashmall2004@gmail.com,[2]vikash.ku.2406@gmail.com,[3]vipin16127@gmail.com

A B S T R A C T :

The role of the Internet of Things (IoT) in healthcare is crucial, as it fosters communication between individuals, devices, and the interaction of devices with individuals. IoT is instrumental in improving medical services available to patients, creating a network of interconnected entities through the internet. This paper gives the introduction of IoT in healthcare and its challenges. Additionally, it addresses the importance of encryption techniques for safeguarding sensitive patient health information.

Keywords: Challenges in IoT, Data Protection, Security, Health Monitoring System, IoT Technology.

Introduction

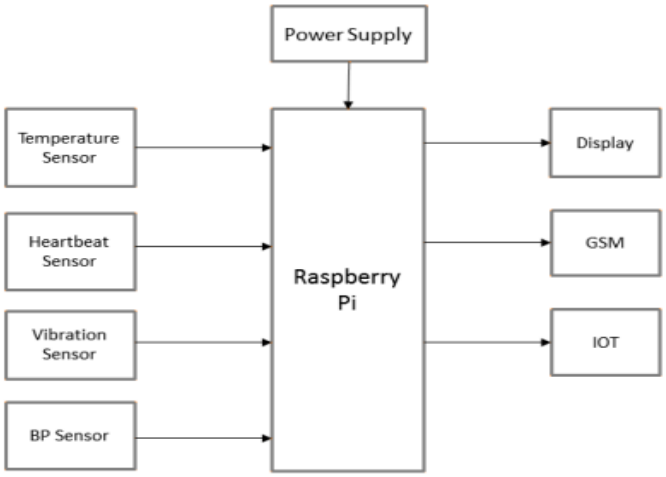
The Internet of Things (IoT) refers to the ever-expanding network of devices that are capable of collecting, storing and exchanging different types of data on the Internet. The term “cloud computing” was introduced by Kevin Ashton in the late 1990s. He used the word to describe a myriad of computer programs, technologies, requirements and initiatives. Ashton's work involved studying radio frequency identification (RFID) which is the technology that uses small radio frequency tags, or RFID tags, attached to objects enabling stored information to be read from a distance. Claims about the growing use of radio frequency identifying (RFID) technology are true, especially with regard to the growing needs of the global population, especially the elderly.

In healthcare, the term “Internet of Clinical Matters” (IOMT) is referred to as devices which continuously monitor and measure VoIP- human physiological parameters. This marks the dawn of intelligent healthcare systems allowing for proactive health monitoring with the help of smart internet connected medical sensors and wearable devices that continuously track patient indicators like heart rate, anticipating heart attacks, and providing timely diagnostics. The demand for personal healthcare services is expected to grow most rapidly.

The blending of IoT in health monitoring systems using cellular phones is known as m-health, which encompasses fact sensing, analysis, and storage from a number of resources, including gadgets, biomedical sensors, and medical uniqueness acquisition structures. IoT applications allow hospitals to monitor patients remotely and monitor their recovery status in real-time, even after discharge. It is done by using IoT-enabled wearable or embedded clinical sensors. The data collected from such sensors is processed and transformed into useful information through the application of learning methods used by devices. Hence, this helps scientific professionals working in hospitals to visualize the modern health environment of out-patients at home, thus enhancing patient well-being and providing caregivers with essential tools and timely data necessary in providing best quality health care to the public at large, traditionally called smart healthcare.

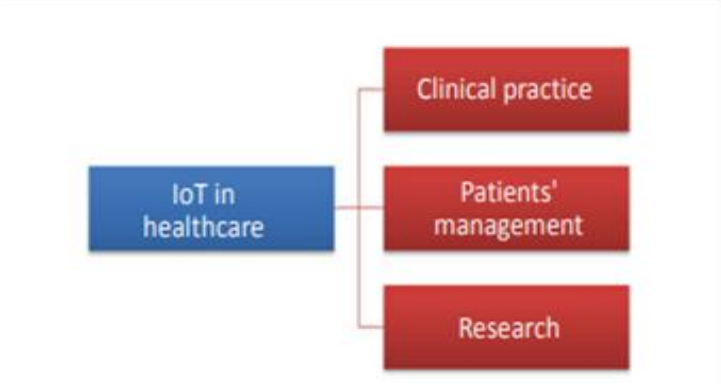
IoT In Healthcare

The IoT allows medical professionals to monitor individuals through online platforms. The method allows intelligent devices, including mobile phones, sensors, and Raspberry Pi, to sense, monitor, and respond to changes in the environment in real-time. The method allows for a personalized manner of taking care of patients, and it's possible to store health conditions and create personalized treatment plans. Healthcare professionals can monitor patients' health remotely using portable sensors and respond to changes in real-time. Processing is done in a cloud data center, where data is converted into meaningful information for healthcare professionals and approved patients. The growth of smart healthcare is also driven by the belief that patients want access to quality and timely services from healthcare professionals irrespective of time and location. The healthcare management system, made possible through IoT technology, is heterogeneous computing, as it uses many wireless communication systems to link patients with healthcare professionals. The services provided include the detection, analysis, monitoring, and protection of critical medical and statistical information.



Application Of IoT In Healthcare

The use of IoT in healthcare greatly enhances research, clinical practice, and patient care. This is accomplished from four fundamental pillars. The first pillar is gathering data, which is achieved through networked devices such as sensors, monitors, detectors, and cameras. The second pillar is transforming data, which is focused on converting analog signals acquired from sensors and ancillary devices into digital signals to facilitate processing. The third pillar is storing data, which is achieved through cloud system. The fourth pillar is processing data, which is achieved through sophisticated analytics techniques that give users vital information to assist them in making informed choices. In patient care, the infrastructure of iot is primarily made up of wearable devices. The wearable devices can monitor diverse indicators of health such as oxygen saturation, blood pressure, heart rate, and blood glucose level, depending on the patient's history and the necessity of observation. These devices can provide personalized care in case of acute disease or progressive worsening of health. Applications include real-time systems for observing health that can measure ecg indications, heart rates, body temperatures, blood pressures, oxygen saturation levels, and blood glucose levels, thus detecting abnormalities easily. This infrastructure, therefore, allows healthcare providers to monitor the health condition of patients and provide appropriate care. Under this category of application, most studies and models possess the same functionalities and characteristics, such as collection, capture, storage, and transmission of vital signs. These applications also encounter the same challenges.



4. Challenges In IoT Enabled Healthcare

I. Security and Privacy

Exchange of information through the internet poses a threat to patient data confidentiality. A conventional network has five basic building blocks: availability, integrity, confidentiality, access control, and authentication. Medical monitoring systems have the same security requirements as conventional networks. Security is a top priority in medical monitoring systems. There is a need to employ current cryptographic methods to safeguard patient data from attack, as medical monitoring systems are vulnerable.

II. Power Consumption

The level of energy that a system or machine uses in a bid to operate at its best is called power consumption. Power consumption is especially relevant to the IoT since most IoT devices are actually designed to be small, energy-efficient, and battery-driven.

III. Accurate and continuous monitoring

Chronic illness patients must be checked periodically to determine any alterations or irregularities that may occur.

IV. Storage Capacity

Installation of IOT technologies is also challenging with regard to limited storage capacity for patient data. While storage capacities are improving day by day, it is crucial to make sure that a lot of patient data is stored in a compact area efficiently.

V. Standardization

Standardization Most suppliers provide a wide variety of goods and devices, with more and more new firms entering this unstable realm of innovation. However, they do not pay attention to the existing standards and regulations of compatible protocols and interfaces for devices, which makes it difficult to exchange and convert data.

VI. Data Protection

Data Protection It is of prime significance to secure health data collected using a range of sensors and devices. Data protection challenges are ensuring physical devices are secure, ensuring data channels are secure for passing data, ensuring data processing is transparent, and ensuring security for processing vast quantities of IoT data.

VII. Increased number of IoT devices

In recent times, cybersecurity experts have made significant advancements in enhancing the security protocols for computers and mobile devices. Furthermore, the adoption of IoT technology is expanding among both private and public organizations. Currently, there are approximately seven billion devices in use, and projections indicate that this number could surpass 20 billion by the year 2021. The growing number of internet of things (IoT) devices is expected to lead to more security risks for businesses, making it harder for security experts to address these challenges.

VIII. Need for encryption

While encryption strategies are essential for safeguarding sensitive information from unauthorized access, they also pose substantial challenges for iot security. The devices in question typically have limited storage and processing power compared to standard computers, making them more susceptible to attacks. Hackers can easily find the bugs in IoT devices because it security algorithm is weak. Therefore, encryption can only serve as a security measure if this issue is successfully resolved.

IX. Inability to predict threats

Certain organizations may lack a management system that efficiently tracks activities and conducts simultaneous inspections to identify potential threats, despite the efforts of security professionals to prevent attacks on iot. Without implementing these proactive measures, organizations will likely encounter difficulties in identifying potential breaches at an early stage.

Conclusion

Modern advancements are swiftly becoming crucial in the healthcare industry, utilizing devices that regularly observe health metrics or track timely health data. The recommended system can be deployed in hospitals, facilitating the collection and storage of extensive data in an online database. This paper analyzes the various applications of IoT that enhance human life and the vulnerabilities it encounters. Furthermore, the system can be improved by integrating components of artificial intelligence to aid both medical practitioners and patients.

Acknowledgements

I would like to thank my supervisor, Ms. Priyanka Singh, for their guidance and valuable suggestions. Their expertise, constructive feedback, and patience were instrumental in shaping this research and helping me navigate through the complexities of the topic.

I am deeply grateful to the faculty members of the CSE - IOT at Raj Kumar Goel of Institute for providing a conducive learning environment and for their constant motivation throughout my academic journey.

A special thanks to my family, whose unwavering love, support, and understanding kept me motivated throughout my studies. Without their encouragement and belief in me, this research would not have been possible.

Thank you to all who have contributed, directly or indirectly, to the completion of this project.

REFERENCES

1. Greengard, S.: The Internet of Things. The MIT Press, Cambridge, MA (2015)
2. Figueroa CA, Harrison R, Chauhan A, Meyer L (2019) Priorities and challenges for health leadership and workforce management globally: a rapid review. BMC Health Serv Res 19(1):239
3. Devi MK, Vemuri VP, Arumugam M, UmaMaheswaran SK, Acharjee PB, Singh R, Kaliyaperumal K (2022) Design and implementation of advanced machine learning management and its impact on better healthcare services: a multiple regression analysis approach (MRAA). Comput Math Methods Med 2022:2489116

4. Esther OA, Jantan A, Abiodun OI, Arshad H, Dada KV, Emmanuel E (2020) HoneyDetails: a prototype for ensuring patient's information privacy and thwarting electronic health record threats based on decoys. Health Inform J 26:2083–2104

5. B. G. Ahn, Y. H. Noh, and D. U. Jeong. Smart chair based on multi heart rate detection system. In 2015 IEEE SENSORS, pages 1–4, Nov 2015.

6. S. H. Almotiri, M. A. Khan, and M. A. Alghamdi. Mobile health (m-health) system in the context of iot. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pages 39–42, Aug 2016.

7. T. S. Barger, D. E. Brown, and M. Alwan. Healthstatus monitoring through analysis of behavioral patterns. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 5(1):22–27, Jan 2005. ISSN 1083-4427.

I. Chiuchisan, H. N. Costin, and O. Geman. Adopting the internet of things technologies in health care systems. In 2014 International Conference and Exposition on Electrical and Power Engineering (EPE), pages 532– 535, Oct 2014.

A. Dwivedi, R. K. Bali, M. A. Belsis, R. N. G. Naguib,P. Every, and N. S. Nassar. Towards a practical healthcare information security model for healthcare institutions. In 4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine, 2003., pages 114–117, April 2003.

8. Atawneh SH, Ghaleb OAM, Hussein AM, Al-Madi M, Shehabat B (2020) A time series forecasting for the cumulative confirmed and critical cases of the covid-19 pandemic in Saudi Arabia using autoregressive integrated moving average (ARIMA) model. J Comput Sci 16:1278–1290

9. Yogaraj A, Ezilarasan MR, Anuroop RV, Sivanthiram CS, Thakur SK (2017) IOT based smart healthcare monitoring system for rural/isolated areas. Int J Pure Appl Math 114(12):679–688

10. Psiha, M.M., Vlamos, P.: IoT applications with 5G connectivity in medical tourism sector management: third-party service scenarios. Adv. Exp. Med. Biol. 989, 141–154 (2017). https:// doi.org/10.1007/978-3-319-57348-9_12

11. O'Brolcháin, F., de Colle, S., Gordijn, B.: The ethics of smart stadia: a stakeholder analysis of the Croke Park project. Sci. Eng. Ethics 25, 737–769 (2019). https://doi.org/10.1007/s11948- 018-0033-5

12. Gupta, Akhil and Jha, Rakesh Kumar.2015." Security Threats of Wireless Networks: A Survey", International Conference on Computing, Communication and Automation, pp. 389-395.

13. Nisha, Shireen and Farik, Mohammed.2017. "RSA Public Key Cryptography Algorithm – A Review". International Journal Of Scientific & Technology Research, Vol. 6,(pp. 187-191).

14. Ilyas ,Mohammad.2018. "Wireless Sensor Networks for Smart Healthcare" IEEE, (pp. 1-5).

15. Talpur, Mir Sajjad Hussain.2013. "The Appliance Pervasive of Internet of Things in Healthcare Systems," International Journal of Computer Science Issues, vol. 10, (pp. 419–424.)

16. Dziak, Damian, Jachimczyk, Bartosz and Kulesza, Wlodek J.2017." IoT-Based Information System for Healthcare Application: Design Methodology Approach", Applied Science Journal, (pp. 1-17)

17. Stefano, G.B., Kream, R.M.: The micro-hospital: 5G telemedicine-based care. Med. Sci. Monit. Basic Res. 24, 103–104 (2018). https://doi.org/10.12659/MSMBR.911436

18. Garcia-Morchon, O., Falck, T., Wehrle, K.: Sensor network security for pervasive e-health. Secur. Commun. Netw. 4, 1257–1273 (2011). https://doi.org/10.1002/sec.247

19. Backman, W., Bendel, D., Rakhit, R.: The telecardiology revolution: improving the management of cardiac disease in primary care. J. R. Soc. Med. 103, 442–446 (2010). https://doi.org/ 10.1258/jrsm.2010.100301

20. Li, S., Li, M., Xu, H., Zhou, X.: Searchable encryption scheme for personalized privacy in IoT-based big data. Sensors 19 (2019). https://doi.org/10.3390/s19051059

21. Brey, P.: Freedom and privacy in ambient intelligence. Ethics Inf. Technol. 7, 157–166 (2005). https://doi.org/10.1007/s10676-006-0005-3

22. International Journal of Engineering Applied Sciences and Technology, 2019 Vol. 4, Issue 1, ISSN No. 2455-2143, Pages 49-53 Published Online May 2019 in IJEAST (http://www.ijeast.com)