SHODH SAMAGAM

ISSN : 2581-6918 (Online), 2582-1792 (PRINT)

Comprehensive Study of Wearable IoT Devices in Healthcare: Applications and Future Directions

Mukesh Kumar, Research Scholar, **Navin Kumar,** Ph.D., Department of Computer Science
Capital University, Koderma, Jharkhand, INDIA

ORIGINAL ARTICLE

Authors

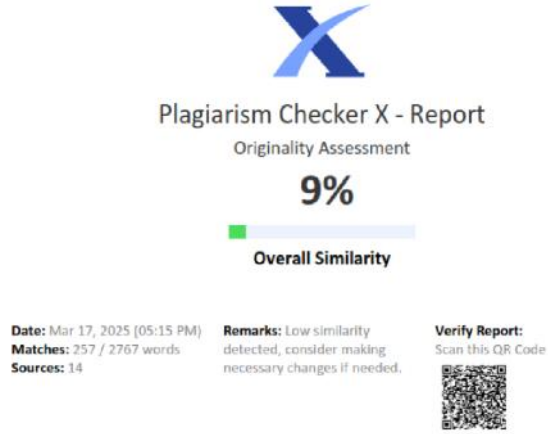
Mukesh Kumar, Research Scholar

Navin Kumar, Ph.D.

E-mail : mukesh.xavierpat@gmail.com

shodhsamagam1@gmail.com

Received on : 16/01/2025
Revised on : 15/03/2025
Accepted on : 25/03/2025
Overall Similarity : 09% on 17/03/2025



ABSTRACT

The Internet of Things (IoT) has been integrated into various sectors, including healthcare, smart homes, entertainment, transportation, and education. New technologies have always been developed by human civilization to improve the comfort, effectiveness, and utility of its way of life. In recent years, there have been a lot of inventions in technology that have significantly transformed the healthcare sector. It has enabled more efficient, accurate, and real-time patient monitoring. The exponential growth of IoT wearable devices leads to the requirement to process results in real time and a better way to store data. However, the significant increase in IoT devices and the large amount of data they generate at the network's edge have added extra challenges that conventional cloud architecture with central repository is not able to handle properly. As a result, Edge Computing (EC) based IoT is becoming a modern strategy that offers data processing and storage closer to the end-users. It results in real-time response and the patient's life could be saved in critical situations. It has opened new avenues for continuous health monitoring, data collection, and analysis through the employment of various wearable devices. Although this paradigm offers unique features and improved quality of service, it also introduces tremendous data security and privacy risks. In healthcare, providing users with a high level of security is crucial since health and location data are sensitive. In this paper, researcher tried to conduct a comprehensive investigation into security and privacy issues in the context of Edge based health monitoring system, and explored possible solutions.

KEY WORDS

IoT in Healthcare, Wearable Devices, Edge Computing (EC), Cloud vs Edge Computing, Security and Privacy Concerns.

INTRODUCTION

The Internet of Things (IoT) is a collective network of interconnected devices that are embedded with sensors, software, and other technologies to collect and exchange data over the Internet. In recent years, the efficient integration of the IoT with healthcare systems has brought new avenues for continuous health monitoring. The IoT architecture for healthcare is a multi-layered architecture designed to ensure efficient data collection, data processing, data analysis, and secure transmission to improve patient care. The major components of multi-layered architecture are as following:

i. **Device Layer**: It consists of wearable devices such as smartwatches, fitness trackers, and other sensors to monitor vital signs.

ii. **Network Protocol Layer**: It consists of various communication protocols such as Zigbee, Bluetooth, Wi-Fi, and LTE. It ensures smooth and efficient connectivity to the cloud or edge servers.

iii. **Cloud Computing Layer**: It consists of centralized cloud servers that provide scalable storage and computational power for data processing and analysis.

iv. **Application Layer**: It consists of user interfaces for healthcare providers, patients, and others to interact with the system.

v. **Security and Privacy Layer**: It consists of various mechanisms and algorithms to encrypt data during transmission and storage.

These devices collect real-time data on vital signs such as glucose levels, heart rates, and other critical health metrics, and allow healthcare providers for real time interventions and more accurate diagnoses. The wearable sensor system is traditionally connected to the cloud and the data can be retrieved and analysed from the cloud [Figure 1].

Once data is collected, it undergoes processing and analysis to extract valuable insights. Medical sensors could be connected to external gateways through wireless networks and information stored in the cloud could be accessible to all medical staff. A remarkable portion of India's population lives in rural areas where frequent access to quality health services is limited. IoT-based patient health monitoring can bridge this gap by providing remote monitoring and consultations.

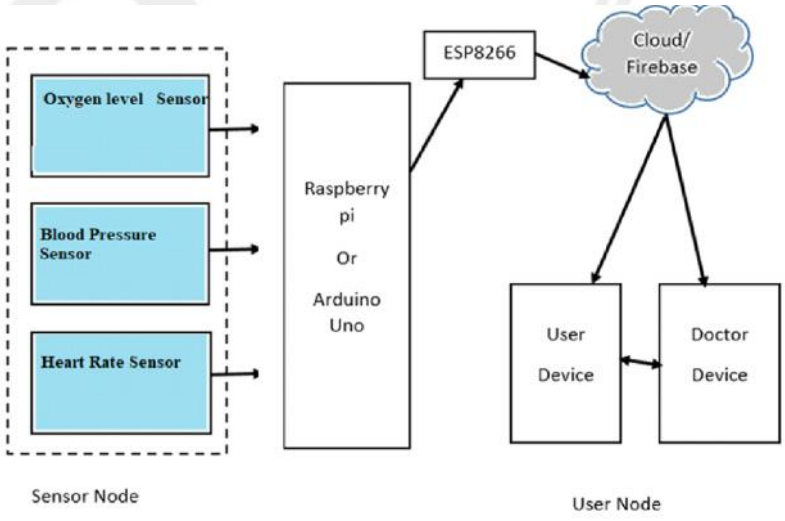


Figure 1: Raspberry Pi model for Health Monitoring System

According to a study report by the Indian Council of Medical Research (ICMR), It is estimated that the percentage of deaths caused by Non-Communicable Diseases (NCDs) in India has risen from 37.9% in 1990 to 61.8% in 2016[1]. The four major NCDs cardiovascular diseases (CVDs), cancers, chronic respiratory diseases (CRDs), and diabetes are basically due to unhealthy diet, physical inactivity, and the use of tobacco and alcohol. Cardiovascular diseases and hypertension are major concerns among the elderly, with prevalence rates of 34.6% and 32%, respectively. According to a report published by A. Minhas, there are very few hospitals available for such a large population in India. It is essential to address these challenges through improved healthcare infrastructure, policies, and support systems to ensure the elderly population receives adequate and timely medical care. The new paradigm of healthcare is adopting IoT devices.

Real Time Health Monitoring with Edge Computing Framework

The amount of information generated by IoT devices is massive; hence cloud computing has virtually infinite storage potential to accommodate such loads efficiently. Cloud storage solutions like Amazon S3, Google Cloud Storage, Azure Blob Storage have been designed specifically for efficient management and placement of huge datasets. The cloud service providers are responsible for faster analysis and further propagation of data to the concerned people. However, this is not always possible to get everything on time in the case of cloud services[2]. The share of Machine-to-Machine (M2M) connections is expected to rise from 33% in 2018 to 50% by 2023. M2M connections will make up 50% of all connections, with a total of 14.7 billion connections projected[3]. In the M2M category, Internet of Things (IoT) devices hold the largest share and are growing rapidly. It may become life-threatening if the system response time is delayed for a few seconds for heart patients. On average, 70-71 milliseconds are required to transfer 1 KB data generated by a sensor with 10 Mbps effective upload speed. Medical sensors generate a vast amount of data. For example, Heart Rate Monitors often collect data around 1 HZ and each heart rate reading might be a single integer, approximately 16-bits (2 bytes).

Therefore,

$$1 \text{ sample/second} \times 2 \text{ bytes/sample} = 2 \text{ bytes/second}$$

It means, approximately 24x60x60x2=172800 bytes of data need to be transferred to the cloud storage in a day. It is obvious that patient monitoring needs more such types of sensors or wearables like temperature sensors, fitness trackers, gyroscopes, etc. GPS sensors may also be attached to detect patients' location and exact position. The data generated can vary from a few megabytes to tens or even hundreds of megabytes depending on the number of sensors, their sampling rates, and the specific use case. In Edge-based or Edge-assisted computing everything related to a patient is not transferred to the central repository. Some processing is done at the edge of the network and then only part of the processed data is sent to the central repository. If something related to a patient needs to be responded to in real-time then that information is directly transferred to the connected hospital or doctor through edge computing [Figure 2]. Edge computing brings computational and processing resources near to the end-users and devices to perform necessary real-time data analysis and decision-making functions and to improve resource efficiency by reducing the amount of data transferred between the end systems and centralized cloud servers.

Edge based computing doesn't mean to complete removal of cloud storage. Actually, Edge computing is simply placed in between cloud and IoT devices for most efficient use of the whole system. Wearable devices can detect heart rate abnormalities, blood pressure, body temperature, or glucose levels faster than legacy technologies. Sensor data from an edge computing application is commonly sent longer distances to a server. Edge computing is transforming the conventional method of data gathering and provides notable benefits such as:

- **Lower latency:** Edge based solutions offer a lower latency compared to traditional cloud solutions and some specific elements of the system design allow for this. Data processing at the edge results in eliminated or reduced data travel.

- **Reduced cost:** Using the local area network for data processing grants organizations higher bandwidth and storage at lower costs compared to cloud computing.
- **High Level Security/Privacy:** Due to the confidential nature of health and location information, it is important to guarantee users a high level of security. Some encryption techniques used on edge devices are more energy efficient than others. One very popular encryption technique on smart edge devices is elliptic-curve cryptography (ECC).
- **Model accuracy:** In healthcare systems, they rely on high-accuracy models, especially for edge use cases that require real-time response.
- **Location Awareness:** Location awareness is also a critical requirement for health-related IoT applications, since it allows for the patient to be found in case of a health-related emergency.
- **Wider reach:** Internet access is a must for traditional cloud computing. But edge computing can process data locally, without the need for internet access.

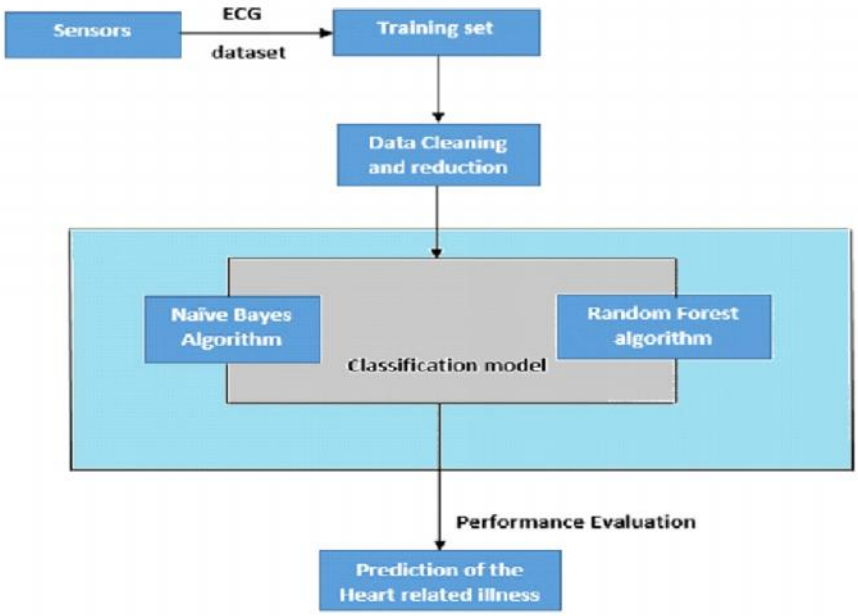


Figure 2: Edge Based Health Monitoring System

Wearable Devices for Health Monitoring

Healthcare providers can use wearable devices for continuous monitoring of patient's health metrics to monitor different health metrics either continuously or periodically. The wearable devices provide personalized data that reflect the unique health status and needs of each user. Recently, CardicSense, a medical grade smartwatch, got approval from the Indian Regulatory Authority Central Drug Standard Control Organization (CDSCO) under the Health Ministry of India[4]. In the diagnosis and treatment of cardiovascular arrhythmias such as tachycardia and bradycardia, the ECG is the initial point of reference. Skin-based devices are wearable technologies designed to capture health parameters directly through the skin. Electronic skins (tattoo) are extensively utilized to detect electrical and physical parameters, including ECG. The ECG is easiest to detect as it has a very high amplitude and can capture electronic frequencies through skin directly. A tattoo-based ECG monitor has electronic components built on graphene [Figure 3]. It is also possible to get blood pressure reading continuously using graphene-based e- tattoos. The graphene has high stretchability and optical transparency. This property makes it light enough to be embossed on skin, like a tattoo. The necessary power could be generated by ultra-thin batteries embedded with tattoos or by techniques such as piezoelectric to convert body movement and heat into electrical energy. The TempTraq is a Class II medical device that has been cleared by the FDA, offering healthcare providers continuous temperature monitoring solution in the

form of a soft, comfortable, disposable patch[5]. There is one more skin patch, FreeStyle Libre, it is the most effective and painless way to monitor blood glucose levels. A very thin patch is applied under your skin, preferably on back of your upper arm, and measures your interstitial fluid. Your blood glucose level can be monitored without having to prick your finger every time. Polymer-based microfluidic devices, paper-based microfluidic devices, and micro sized needles known as microneedles are frequently used for this purpose. Sensors that are self-powered, such as piezoelectric nanogenerators (PENG) and triboelectric nanogenerators (TENG) are revolutionizing the healthcare devices.

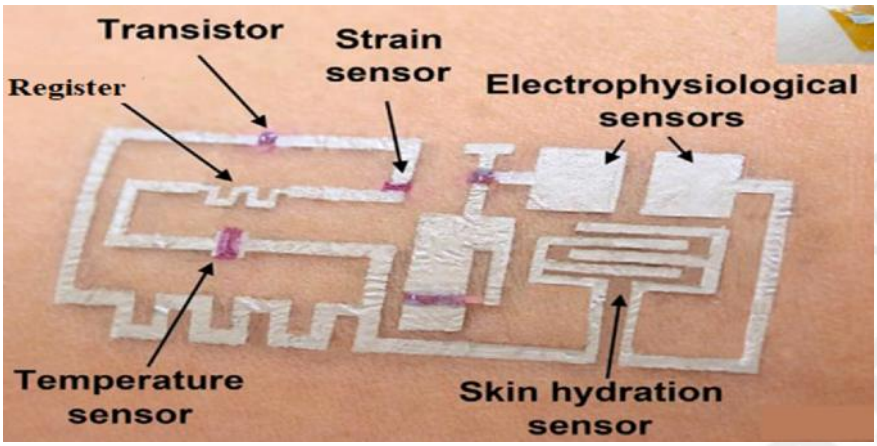


Figure 3: Graphene Tattoo Based Sensors

Now we discuss the main desirable features of wearable devices required for standard healthcare systems:

- **Wireless Mobility:** The wearable devices come with wireless technologies like Bluetooth, Wi-Fi, and occasionally cellular connectivity, allowing them to transmit data to other devices. Patients can wear these devices and move freely without being tethered to stationary equipment.
- **Interactivity and Intelligence:** The wearables must have user interfaces (like touch screens or physical buttons) that allow users to interact with the device, input data, receive feedback, and adjust settings. The wearable devices are typically designed to be easy to use, with intuitive interfaces and minimal setup required.
- **Sustainability and Durability:** The wearable gadgets necessitate durability and reliability. They must be capable of managing daily wear and tear. The devices are generally water resistant with robust casing and with energy efficient functioning.

Privacy and Security Challenges in Edge-Centric Health Monitoring Systems

Edge-Centric (EC) IoT based health monitoring systems offer real-time data analysis and reduced latency, but they also present several security concerns. These systems collect sensitive health data, making them a prime target for cyberattacks such as data breaches, unauthorized access, and ransomware. Attackers may also change the training process of machine learning models of EC nodes by injecting misleading data sets. The healthcare industry is the most targeted industry for data breaches, with over 470 healthcare breaches reported in 2020[6] , exposing over 37.5 million sensitive records. Anthem, one of the largest health insurers in the United States, suffered a cyberattack resulting in the exposure of personal information of approximately 78.8 million individuals, including names, social security numbers, and medical IDs. Anthem will pay a $39.5 million[7] settlement in connection with the state Attorney Generals' investigation. The year 2023 witnessed an unrelenting surge in cyberattacks targeting healthcare organizations, resulting in two significant milestones: the highest number of reported data breaches and the largest volume of breached records. During this period, a total of 725 data breaches were reported to the OCR, compromising or unlawfully exposing over 133 million

records[8]. Edge-Centric IoT based Health Monitoring Devices are vulnerable to security risks at various layers like perception layer, network layer and application layer.

- **Perception Layer:** This layer is responsible for collecting data through sensors, RFID tags, GPS or other smart sensors. Unencrypted data at this layer can be intercepted easily. IoT health devices have limited power supply and resources for processing. Encrypting data before transmission may slow down the communication speed.
- **Network Layer:** This layer handles the transmission of collected data to other devices or the cloud via communication protocols like Wi-Fi, Bluetooth, Zigbee, NFC or 5G. Attackers may intercept data during transmission or disrupt communication by overloading the network (DoS). In medical IoT devices, each device is capable of re-routing and amplifying, and therefore it creates new opportunities for attackers[9].
- **Application Layer:** This layer processes the data and provides user interfaces like dashboards, mobile apps, or alerts. In this layer, attackers may inject false data to be shown on user's dashboard. The human factor is also very important at this layer.

1. Strengthening Security in Edge-Centric IoT Devices

Here, researcher discuss the strategies and solutions that could be used for security enhancement and to avoid privacy attacks. First, we should detect hardware/software intrusion with edge devices. It could be done by observing unusual behaviour of nodes like significant increase in their execution time, power consumption or heat emission. We can also embed physically unclonable function (PUF) into the circuit which detects trojan activities. Other mechanisms that could be employed are listed below:

a) Frequent updates for the firmware.
b) Authentic and reliable routing protocol.
c) Use of energy efficient encryption/decryption techniques especially designed for edge devices.
d) Decentralisation of information or even combining edge computing with blockchain technology.
e) Multifactor Authentication.

2. Safeguarding Privacy in Edge-Centric IoT Devices

The next bigger concern is related to privacy. Edge devices that constantly monitor our activities can create detailed profiles of our behaviour, preferences, and routines. Health-related data is highly sensitive and subject to strict privacy regulations. 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[10], it was reported that a security vulnerability in the Aarogya Setu app exposed the personal health data of millions of users. The incident raised concerns about the security and privacy of health-related data in digital health platforms and the potential for unauthorized access or misuse [18]. Manufacturers of health monitoring edge devices should prioritize transparency and provide clear and explicit consent mechanisms.

CONCLUSION

Edge-based healthcare monitoring devices have revolutionized the industry by enabling real-time data analysis, personalized insights, and better patient care. These benefits come with security risks that require careful attention. As technology advances, cyber threats such as data breaches, malware attacks, and unauthorized access become more prevalent. Protecting sensitive health data is crucial, as these devices can have vulnerabilities that may expose patient information and compromise privacy. Ensuring transparency in data handling, enforcing clear privacy policies, and educating users play a key role in safeguarding edge-based healthcare monitoring devices. Awareness and proactive strategies are essential to manage these risks and ensuring a secure digital environment. Artificial Intelligence (AI) and machine learning algorithms can

greatly enhance security by detecting patterns, identifying anomalies, and predicting vulnerabilities in systems. There should be continuous improvements, stronger collaboration, and robust regulations to protect patient privacy and data instead of discouraging the use of such a transformative technology.

REFERENCES

1. PIB Delhi, (2022, February 8), Status of Non-Communicable Diseases (NCDs) in India, retrieved from: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1796435, Accessed on 27/12/2024.
2. A. Minhas, (2023, Jul 12), Estimated number of public and private hospitals in India 2019, retrieved from: https://www.statista.com/statistics/1128425/india-number-of-public-and-private-hospitals-estimated/, Accessed on 27/12/2024.
3. Cisco Annual Internet Report (2018–2023) White Paper, March 9, 2020, retrieved from: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, Accessed on 28/12/2024.
4. Retrieved from: https://www.financialexpress.com/business/healthcare-medical-grade-smartwatch-cardiacsense-receives-approval-in-india-2983982/ Accessed on 28/12/2024.
5. Retrieved from: https://temptraq.healthcare/ Accessed on 29/12/2024.
6. Identity Theft Resource Center, "2020 End-of-Year Data Breach Report": https://www.idtheftcenter.org/2020-data-breaches/ Accessed on 29/12/2024.
7. https://www.fiercehealthcare.com/tech/anthem-to-pay-39m-to-state-ags-to-settle-landmark-2015-data-breach, Accessed on 27/12/2024.
8. https://www.hipaajournal.com/healthcare-data-breach-statistics/Posted by Steve Alder on 30/12/2024, Accessed on 02/01/2025.
9. Richmond, S. Stopping the Attacks: Cybersecurity In Healthcare Manufacturing, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/08/17/stopping-the-attacks-cybersecurity-in-healthcare-manufacturing/?sh=4db312231a8d, Accessed on 01/01/2025.
10. https://www.thequint.com/tech-and-auto/tech-news/aarogya-setu-data-breach-reported-by-shadowmap Accessed on 23/12/2024.
11. Joyia, Gulraiz J.; Liaqat, Rao M.; Farooq, Aftab; and Rehman, Saad (2017) Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain, *Journal of Communications*, Vol. 12, No. 4, April 2017.
12. Salah, K.; El Kafhali, S. (2017) 'Performance modelling and analysis of hypoexponential network servers', *J. Telecommun. Syst.*, 65, (4), p. 717–728
13. Zhang, J.; Chen, B.; Zhao, Y.; Cheng, X.; and Hu, F. (2018) "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, p. 18 209–18 237.
14. Jeong, IC; Bychkov, D; Searson, PC (2019) Wearable devices for precision medicine and health state monitoring, *IEEE Trans Biomed Eng*, 2019 May;66(5):1242-1258.
15. Guk, K; Han, G; Lim, J; Jeong, K; Kang, T; Lim, E; et al. (2019) Evolution of wearable devices with real-time disease monitoring for personalized health care, *Nanomaterials (Basel)* 2019 May 29; 9(6).
16. Yapici, M. K.; & Alkhidir, T. E. (2017) Intelligent medical garments with graphene functionalized smart-cloth ECG sensors, *Sensors* 17, 1–12.
17. Kabiri, Ameri S.; et al. (2017) Graphene electronic tattoo sensors, *ACS Nano* 11, 7634–7641.

18. Someya, T.; & Amagai, M. (2019) Toward a new generation of smart skins, *Nat. Biotechnol*, 37, 382–388.
19. Williams, P.A.; Woodward, A.J. (2015) Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem, *Med. Devices*, 8, 305.
20. Aghili, S.F.; Mala, H.; Kaliyar, P.; Conti, M. (2019) SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT, *Future Gener. Comput. Syst.*, 101, 621–634.
21. Lin, J.; et al., (2017) A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications, *IEEE Internet Things J.*,vol. 4, no. 5, p. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.
22. Hassija, V.; et al. (2019) A survey on IoT security: Application areas, security threats, and solution architectures, *IEEE Access*, vol. 7, p. 82721–82743, doi:10.1109/ACCESS.2019.2924045.
23. Ni, J.; Lin, X.; and Shen, X. S. (2019) Toward edge-assisted internet of things: From security and efficiency perspectives, *IEEE Network*, vol. 33, no. 2, p. 50–57, March 2019.
24. Health Statistics of India, Report of the National Commission on Macroeconomics and Health, Ministry of Health & Family Welfare, Govt. of India August 2005, retrieved from: https://www.indushealthplus.com/health-statistics-of-india.html Accessed on 26/12/2024.
25. PIB Delhi, (2022, February 8), Status of Non-Communicable Diseases (NCDs) in India, retrieved from: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1796435 Accessed on 27/12/2024.
26. A. Minhas, (2023, Jul 12), Estimated number of public and private hospitals in India 2019, retrieved from: https://www.statista.com/statistics/1128425/india-number-of-public-and-private-hospitals-estimated/ Accessed on 27/12/2024.
27. Cisco Annual Internet Report (2018–2023) White Paper, March 9, 2020, retrieved from: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html , Accessed on 28/12/2024.
28. Amft, O; Lukowicz, P. (2009) From backpacks to smartphones: past, present, and future of wearable computers, *IEEE Pervasive Comput*, 2009 Jul;8(3):8-13.
29. Medical-grade Smartwatch CardiacSense receives approval in India, February 17, 2023, retrieved from: https://www.financialexpress.com/business/healthcare-medical-grade-smartwatch-cardiacsense-receives-approval-in-india-2983982/ Accessed on 28/12/2024.
30. Identity Theft Resource Center, "2020 End-of-Year Data Breach Report", retrieved from:https://www.idtheftcenter.org/2020-data-breaches/ Accessed on 29/12/2024.
31. Anthem to pay $39M to state AGs to settle landmark 2015 data breach, September 30, 2020, retrieved from: https://www.fiercehealthcare.com/tech/anthem-to-pay-39m-to-state-ags-to-settle-landmark-2015-data-breach Accessed on 28/12/2024.
32. Richmond, S. Stopping the Attacks: Cybersecurity In Healthcare Manufacturing, (2021) https://www.forbes.com/sites/forbestechcouncil/2021/08/17/stopping-the-attacks-cybersecurity-in-healthcare-manufacturing/?sh=4db312231a8d Accessed on 01/01/2025.
33. Healthcare Data Breach Statistics, Posted by Steve Alder on 3oth December 2024, https://www.hipaajournal.com/healthcare-data-breach-statistics/, Accessed on 4/01/ 2025.

****