Journal Pre-proof

Role of IOT in healthcare: Applications, security & privacy concerns

Akshay Parihar, Jigna B. Prajapati, Bhupendra G. Prajapati, Binti Trambadiya, Arti Thakkar, Pinalkumar Engineer

PII: S2949-866X(24)00003-0

DOI: https://doi.org/10.1016/j.ipha.2024.01.003

Reference: IPHA 89

To appear in: *Intelligent Pharmacy*

Received Date: 11 December 2023

Revised Date: 11 January 2024

Accepted Date: 12 January 2024

Please cite this article as: Parihar A, Prajapati JB, Prajapati BG, Trambadiya B, Thakkar A, Engineer P, Role of IOT in healthcare: Applications, security & privacy concerns, *Intelligent Pharmacy* (2024), doi: https://doi.org/10.1016/j.ipha.2024.01.003.

Role of IOT in Healthcare: Applications, Security & Privacy Concerns

Akshay Parihar[1], Jigna B. Prajapati[3*], Bhupendra G. Prajapati[2*], Binti Trambadiya[4], Arti Thakkar[5], Pinalkumar Engineer[6]

Affiliation details:

1. Faculty of Pharmaceutical Sciences, The ICFAI University, Baddi, 174103, Himachal Pradesh, India Akshay.parihar20@gmail.com

2. Dept. Of Pharmaceutics and Pharmaceutical Technology Shree S. K. Patel College of Pharmaceutical Education & Research, Ganpat University, Ganpat Vidyanagar, Mahesana-Gozaria Highway, 384012, Gujarat, India
bhupen27@gmail.com (Corresponding Author)

3. Faculty of Computer Applications, Ganpat University,
Faculty of Computer Applications, Ganpat University, Ganpat Vidyanagar, Mahesana-Gozaria Highway, 384012, Gujarat, India
Jignap15@gmail.com

4. Binti Trambadiya, Research Scholar, School of Applied Sciences, Edinburgh Napier University, Edinburgh, Scotland, United Kingdom, bintitrambadiya0971@gmail.com

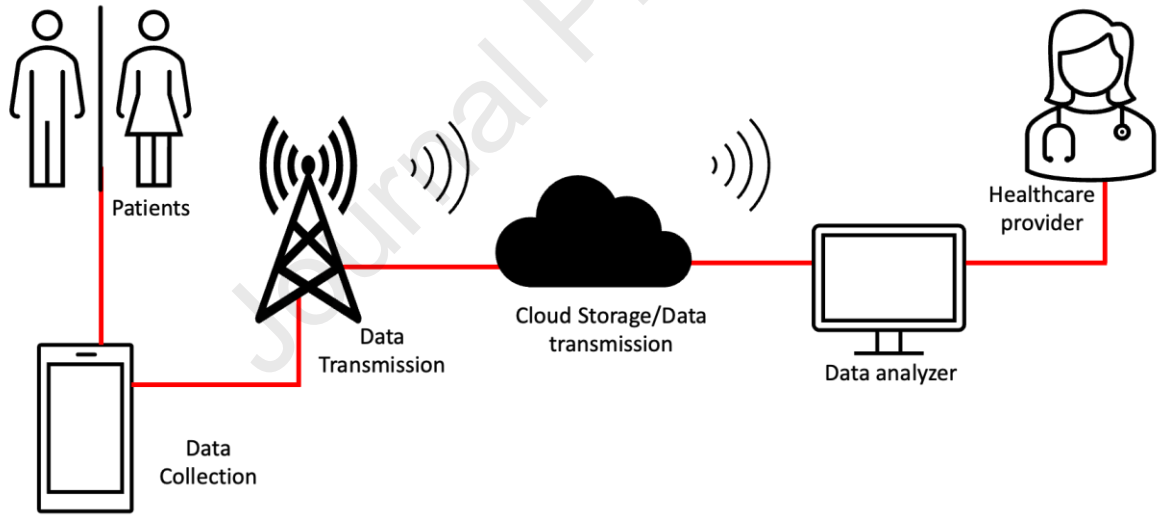
5. Dr. Arti Thakkar, Amity Institute of Pharmacy, Amity University Uttar Pradesh, Noida 201313, UP, India, artirthakkar@gmail.com

6. Department of Electronics Engineering, SVNIT, Surat, India, pje@eced.svnit.ac.in

***Corresponding author:**
Name: Prof. Bhupendra G. Prajapati
Designation: Professor
Department: Pharmaceutical Technology
Affiliation & Address: Shree S.K.Patel College of Pharmaceutical Education & Research Ganpat University, Gujarat
Mobile: +917990533373/9429225025
Email ID: bhupen27@gmail.com
ORCID ID: https://orcid.org/0000-0001-8242-4541

Abstract

Employing the Internet of Things (IoT) in healthcare provides many advantages for patient monitoring and analysis of the patient's health with the help of generated data. The basic role of IoT in healthcare is to ease the patient's life by giving them a monitor over their medical condition. The use of IoT in medical devices requires a focus on the end-user. Medical devices such as glucose meters are designed to record the data of the patient and their vital signs. The generated information can be used to enhance decision-making for the physician. The collected information about the patient can be at risk due to certain security issues during the transferring of information can compromise the identity and social life of the patient. This review explores the IoT regarding its structural requirement and its role in various fields with special emphasis on healthcare. The security and privacy issues than can hinder the utilization of IoT at its potential and ways to overcome these issues are being addressed.



Graphical Abstract

1. Role of IoT in Medical Devices

Medical Devices (MDs) are any instrument, reagent, apparatus, implement, machine or any other *in-vitro* reagent or calibrator, software which is intended to be used alone or in combination for the diagnosis, mitigation, prevention, treatment or alleviation of diseases in human beings [1]. Generally, MDs are classified based on the risk associated with them. As per USFDA MDs are classified into three categories I, II, III where category I has lowest risk and category III has highest risk as shown in Table 1 [2].

Table 1: Classification of Medical Devices in US

CLASS	RISK LEVEL	DEVICE EXAMPLES
I	Low risk	Elastic Bandage, Gloves
II	Medium risk	Catheter, Needle
III	High risk	Pacemakers, Heart Valves

A report from Fortune Business Insights states that from 2018-2025 the Medical Device Industry will experience major investment in Research & Development of new technology from pharmaceutical players, approvals from regulatory authorities will also contribute to increase this number. The medical device global market was USD 42.5 Billion in 2018 and is estimated to reach USD 612.7 Billion by 2025. CAGR is expected at 5.4% from 2018 to 2025 [3].

Further Medical Devices have been showing an increasing growth in the previous decade and with promising technology and innovations being made, it will keep growing more. Although there is conventional research and development being done by existing companies. With the entry of giants like Apple and Google, new technological advancements in the form of Artificial Intelligence, Data Analytics and Internet of Things (IoT) are being implemented in this sector [4].

In today's era, Internet has become inevitable in our daily life. Proper and smart use of internet makes our life simple, fast and easy. Amongst the many uses of the internet, one of the important technologies is "IoT (Internet of Things)". IoT provides "an integration approach for all these physical objects that contain embedded technologies to be coherently connected and enables them to communicate and sense or interact with the physical world, and also among

themselves"[5]. So, basically it is to connect the smart “things” or objects to the internet in the easiest and transparent way. Further, with the “IoT” there is the exchange of the information between all the all things and the end user gets all the information and data in the most secured way [6].

Due to a lot of health challenges and advanced availability of the technologies like IoT, it has created a possibility of many medical applications based on the IoT technology. Specifically, various devices addressing remote health monitoring, elderly care, chronic diseases and different fitness programs [7]. IoT is the smartest solution for making healthcare related medical products more consumer friendly and redefined the usage of technology and various devices can connect with each other. It can provide best of the outcome, reduced costs and care. Further, IoT can transform the healthcare products by data analytics and automation [8]. It can even collect and transmit the data in the real-time activity using networking. So overall, IoT can improve [9]:

- Patient care,
- Optimize the services,
- Collect more information about patient’s preferences and convenience,
- Make hospital services smarter,
- Can provide safer wearable medical devices and monitoring devices,
- Electronic ID enabled security doors in hospital set-up,
- Medical asset tracking,
- Preventive maintenance solution for medical equipment and devices

1.2 Concepts of IoT

Concepts of IoT started with the development of a monitoring the soda machine using the internet by computer science student at Pittsburgh in 1982. Followed by in 1989, a British scientist invents the World Wide Web (WWW) to share the research. In 1990, a toaster was developed which can be turned off and on over internet. Further, in 1999, IoT as a terminology was invented by the British researcher Kevin Ashton. He was the co-founder of the Auto-ID Center at the Massachusetts Institute of Technology, USA and used IoT to explain the Radio-Frequency Identification (RFID) technology in which the device can read and store the data from a tag in a non-contacting manner. In year 2000, LG Ltd. presented the idea of internet refrigerator which notifies the owner when certain things have been run out [10, 11]. Since then, lot of expansion in technology and connectivity has been observed, it has been even predicted that around 75 billion devices will be based on internet in 2025 [12].

1.3 Architecture of IoT Device Development

There are some basic features of the IoT technology such as, wireless technology, remote monitoring, tracking of the objects, real-time solutions worldwide [13]. Further, IoT have few dimensions such as (Figure 1)

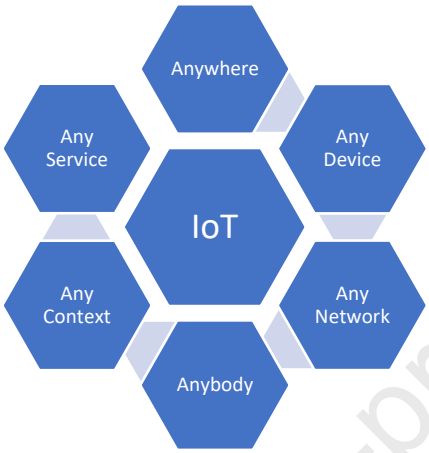


Figure 1. Dimensions of the IoT

Basically, IoT functions with physical devices, advanced data analytics, wireless networking technology and cloud computing. The fundamental method [14] of how IoT works in following manner:

Step 1 – Physical devices are wired or wirelessly linked to each other and/or a central area.

Step 2 – These devices will collect the data through sensor from the external data sets or information networks.

Step 3 – These data is stored in a cloud or intermediary network or within the device itself.

Step 4 – In the next stage the data is processed, by means of machine learning or artificial intelligence.

Step 5 – These processed data will be used by the physical device to perform the predefined task.

2. Medical devices and the need for IoT

Machinery has always been playing an important role in the life of everyone. The availability, productivity, and performance of equipment are now considered a major task for manufacturers. [15] Healthcare organizations have been considering the management program of medical equipment so that the performance level of medical devices can be ensured. Big data is associated with the diversity and updating rate of the data. This can be used to predict

real-world events. The data generated is divided into three categories such as traditional medical data, Omics data, and communication data [16, 17]. The medical devices connected to the internet provide an environment that is capable of giving quick access to information. The vital information of the patient is can be transmitted over the cloud to the healthcare providers for analysis and giving real-time and evidence-based medicines [18]. The fostering of technology has provided the development of mobile applications. These applications can cater the services such as measuring metabolic activities, watching diet, or management of calories. The devices are usually wearable types on the wrist or fingers linked to the mobile phones. Multiple device access is also being offered over a common platform. This kind of development has been filling the gap for free sharing of personal healthcare device [19]. IoT incorporation in medical devices such as RFID can help in anti-counterfeiting, emergency and medical waste management along with drug identification. The medical records and equipment and drug storage can also managed properly. IoT enabled medical devices supports time based monitoring of patients in addition to study the progression of disease. It helps in faster access for physician [20].

3. Applications of IoT in Medical Devices & Diagnosis

Today, the need for linked devices may be found in a variety of businesses. IoT has a wide range of applications in healthcare, including remote monitoring of patients' health, tracking patients and equipment within healthcare organisations, smart beds that detect occupancy, smart pill dispensers that monitor patients' medication intake and sending alert messages to caregivers, and so on [21, 22].IoT can also identify specific health issues in people and respond quickly to medical crises when the patient is on the go. IoT technology, such as equipment tracking systems, can assist healthcare businesses in lowering costs. Furthermore, it may give patients with tailored treatment, therefore boosting the quality of healthcare services [23].

3.1 Remote Monitoring of Patient’s Health

While the patient is at home, Remote Physiological Monitoring (RPM) (also known as remote patient monitoring) employs digital technology to watch their vital signs and intervene if necessary. Sensor advances, the widespread availability of cellular technology, and the falling prices of embedded communication devices are all paving the way for new RPM possibilities [24]. Clinical outcomes and service quality may be improved cost-effectively by organizations. It's a huge aid to the elderly, as it reduces the amount of time they spend travelling to hospitals. Weight, blood pressure, heart rate, glucose level, and other vital physiological characteristics may be monitored remotely, and necessary medical advice could be offered [25].

3.1.1 Components of technology

Recent advancements in technology including RFID, cloud computing, embedded sensors, actuator nodes and microcontrollers and smartphones all have altered the way patients are traditionally monitored [26].

3.1.2 Various Tools used for remote monitoring

The health monitoring tools track the patient's vital signs, gather the information, and send it electronically to a healthcare practitioner in another location for evaluation and medical advice in the form of suggestions to maintain track of the patient's physical activity, remote monitoring equipment such as a glucose meter for assessing diabetes, a pulse meter for checking the patient's pulse rate, and an accelerometer (a movement tracking sensor) are employed. Data is sent to a central database via smartphones, tablets, PDAs, and PCs, where it may be accessed and evaluated by the healthcare professional [27, 28].

3.1.3 Sensors

The sensors can be worn by patients, integrated into watches, shoes, clothes, mattresses, and other items, or positioned in the home as a motion sensor [29]. A sensor that assesses physiological factors and a sensor that detects the external environment, often known as ambient sensors, are two types of medical sensors. The physiological sensors can be worn or implanted and detect vital indicators like temperature, blood oxygen saturation, heart rate, and blood pressure. The environmental sensors monitor variables such as room temperature, light, and sound, as well as to detect falls [21, 30].

A device that monitors the acceleration of a moving body is known as an accelerometer. It is utilized in healthcare applications to examine and record the patient's body poster. It's also used to detect falls, particularly in individuals who are confined to their beds. Humidity and temperature sensor: This sort of sensor may be used to detect the patient's or the surrounding/external environment's body temperature. Sensors for monitoring temperature can be either contact or contactless [31]. Sweat sensor: Sweat biomarkers give a plethora of information about sodium, chloride, potassium, glucose, amino acids, and other substances. It is highly useful for diagnosing disorders like cystic. fibrosis. Athletes and patients have employed wearable sensors built into textiles to obtain information from their bodily fluids in several cases [32]. A respiration sensor is an optical sensor that is used to monitor a patient during magnetic resonance imaging scanning. Respiratory rate monitoring is particularly useful for ambulatory measures and is frequently used to monitor disorders like sleep apnoea and COPD. Blood glucose sensor: Glucose monitoring sensors are essential for diabetic patients to

monitor glucose levels in interstitial fluids continuously [33]. These devices can be bio-implants that are inserted beneath the skin or non-invasive devices that use infrared, optical sensors, or ultrasonic technology. High blood pressure causes heart attacks, strokes, and other problems, and blood pressure can vary every minute, necessitating continual monitoring. Wearable sensors that employ the pulse wave approach provide reliable readings without the requirement for an examiner, as is the case with standard examination methods. ECG sensors monitor the electrical impulse that travels through the cardiac muscles. Electrodes in ECG sensors must contact the skin. Pulse oximetry sensor: Pulse oximetry is a sensor that measures oxygenated haemoglobin in the blood using a non-invasive approach. It is linked to the patient's fingertip, via which the light wave passes through the blood vessels. The SpO2 measurement is based on the fluctuation of the light wave passing through [34].

3.1.4 Ambulance Fitted with Sensors

Performing diagnosis and treatment processes during ambulance transport is extremely challenging in many emergencies. As a result, the patient's diagnosis and treatment are delayed until they arrive at the hospital. Patients frequently perish in ambulances owing to a lack of required support systems during transit. The quality of care offered to patients has improved because of recent developments in healthcare, lower communication costs, and extensive study in the healthcare arena [35]. Ambulance telemetry is one such breakthrough in which doctors or medical facilities may use the automated measurement and wireless transfer of important data from patients within an ambulance to make essential treatment decisions. The data acquired by the sensors aboard the ambulance is sent to the healthcare centres, allowing the patient to receive the appropriate treatment while remaining in the ambulance. Ambulance telemetry employs a variety of technologies to offer treatment and monitor vital signs while the severely sick patient is transported to the hospital by ambulance [36]. Polycom/Web Camera: A polygamy is a gadget that is highly beneficial for consultation from a remote place. A polycam can be linked to the network lines and the TV at the medical facility/ambulance to monitor patient vitals including heart rate and blood pressure. Polycam is frequently replaced with a web camera. Internet: Once the healthcare organization's portal receives the patient's vital parameters from the ambulance, they may be utilized for online consultations with doctors, ensuring that the critically sick patient receives timely treatment while on the road to the hospital. Wireless communication: In IoT-based systems, where devices interact with one other from different places, wireless technology has become an essential component. Smartphones, GPS (Global Positioning System) units, Zigbee technology, Wi-Fi, Bluetooth,

and other communication devices are utilized [37]. In a remote patient monitoring system, data gathered from sensor nodes is transported to the concentrator or IoT gateway using wireless communication technologies like Zigbee or low-power Bluetooth, where it is aggregated and sent to the cloud for analysis. Zigbee is the most popular device for remote sensing and monitoring applications because of its low power consumption and extended battery life [38].

3.1.5 Benefits of Using Remote Monitoring Devices

Patients who are old, chronically sick, or have mobility problems may benefit from remote monitoring systems. It also allows healthcare providers to analyse patient data from afar and act if necessary. Reduced Hospital Readmission: Remote monitoring devices can be wearable or ambient sensors that gather health-related data from patients and warn healthcare providers if there is a deviation from the threshold specified for each patient. This enables the healthcare professional to intervene quickly, decreasing hospital admissions [39].

It assists patients in managing their health data: Remote monitoring can assist patients in better understanding their health conditions and, in some situations, such as diabetes, self-administering medication as necessary. Because the patient is continually aware of his or her health situation, he or she may lead a better lifestyle. Reduced trip time: Patients in rural locations and those with mobility challenges benefit greatly from remote monitoring systems. The necessity to be physically present at medical facilities is no longer necessary because the patients' health metrics are regularly checked by healthcare specialists from a distant location [40, 41].

3.2 Sensor Enabled drug and equipment tracking

Drug, patient, and device tracking is becoming an increasingly essential component of the healthcare business, as it promises to lower costs while still providing high-quality care to patients. The ability to track medical equipment and patient medication intake will aid care providers in managing their costs. The constant streaming data from the tracking devices may be utilized to successfully manage a variety of chronic conditions, lowering healthcare costs [42].

3.2.1 Sensor Enabled Pills

Sensor Enabled Pills Sensor-enabled tablets provide improved knowledge of how to manage complicated and chronic diseases. It enables the clinician to deliver specialized or tailored treatment to patients’ needs. On intake, the ingestible tablet gathers critical health parameter data and transmits it to a wearable device, which then sends it to the cloud as a report so that

healthcare practitioners may diagnose the condition and determine the effect of a medicine on vital organs [43].

In addition to their normal prescription, the patient is given sensor-enabled tablets containing ingestible sensors. When the patient swallows the sensor-enabled pill, it enters the patient's stomach and sends vital sign signals to the patient's wearable device. The wearable records all the patient's vital signs and transmits them to both the patient and healthcare experts. Healthcare practitioners may use this data to keep an eye on patients, follow their activities, and make informed decisions about their treatment [44].

3.2.2 Smart Pill Bottles

Taking medications at the appropriate times will guarantee that the patient's health is in good hands. Patients in their senior years are prone to forgetting to take their medication and skipping doses, which can lead to serious complications. To significant health problems, particularly in chronically unwell patients. The usage of sensor-enabled smart pill bottles that identify when the patient has forgotten to take their prescription and offer real-time feedback is one solution to this problem. In non-compliance, caregivers and healthcare providers receive alarm messages and energy-saving smart pill bottles with built-in mobile phone technology that permit patients to take the correct dose of medication at the correct time. The pill container not only guarantees that patients take their medications on time, but it also improves income for pharmaceutical businesses, which would otherwise result in missed sales. Adhere Tech's smart pill dispenser solution keeps patients on track by monitoring the dose in real-time. It may notify patients when it's time to take their medicine through a phone call, text message, or flashing light in the bottle. It also aids in pill counting by keeping track of when the container was opened and how many pills were taken [45].

3.2.3 Medication Error Reduction Using RFID

Radio Frequency Identification (RFID) technology is frequently employed as a medical management solution to improve pharmacy operations as well as patient care and safety.

RFID is utilized in drug management, particularly to keep track of medicine supply levels. Several medications, such as ant venom and rabies, are rarely provided to patients but must be ready and available in the hospital. Because these drugs have a short shelf life, are slow-moving, and are also pricey, stock levels must be continuously monitored. When done manually, this process takes longer and has a higher mistake rate. Pharmaceutical companies employ RFID-based medication management systems to automate their restocking processes, and it is an effective method for reducing time, mistake rates, and increasing efficiency in

hospital pharmacies. An RFID tag is affixed to each of the pharmaceutical trays/containers, which carries information such as the drug's name, manufacturer's name, drug identification number, lot number, and expiration date. The system scans the tray regularly and compares the information to the amounts and medications allotted to the tray. It then creates a report in seconds on the drugs that have been ingested, those that have expired or are going to expire, and so on, so that relevant steps may be taken. Because the sort of care or treatment required is not known ahead of time, reliable forecasting of required supplies is challenging in the healthcare industry [46].

Because there is no clear system in place to track inventory goods including consumables, lab supplies, and prescriptions, they are frequently forgotten, lost, or expired, resulting in erroneous inventories and needless last-minute orders. The cost of such unanticipated urgent orders rises. RFID-enabled refrigerators and storage cabinets can continuously monitor inventory levels and alert the user if the inventory level falls below a certain threshold, as well as provide an alert for products that are about to expire, allowing for timely restocking and ensuring that critical supplies are available for patient care [47].

3.2.4 Equipment Tracking

Equipment maintenance, particularly medical equipment maintenance, is critical for healthcare institutions. However, in many hospitals, the bulk of the time is spent identifying equipment, or the equipment is discovered to be in use and so unable to be serviced at the allotted period [48]. Even the tiniest power outage or malfunction of life-saving equipment might have disastrous consequences for the hospital's operations [49]. The asset monitoring system may notify employees when equipment needs to be repaired or replaced regularly. In a hospital, managing hundreds of expensive permanent and mobile equipment is quite difficult. A system to track and monitor all these devices might be an effective option. When dealing with severely sick patients, having the proper equipment accessible at the right moment can be vital in maximizing the availability of assets that can save lives. Hospital beds, IV pumps, blood, stretchers, ECG equipment, ventilators, and other mobile items are frequently misplaced or lost in hospitals. As a large business with numerous departments sharing equipment, it is usual for hospitals to lose a percentage of their equipment each year, making it difficult to manage and find assets [50]

4. Security concerns for IoT in healthcare

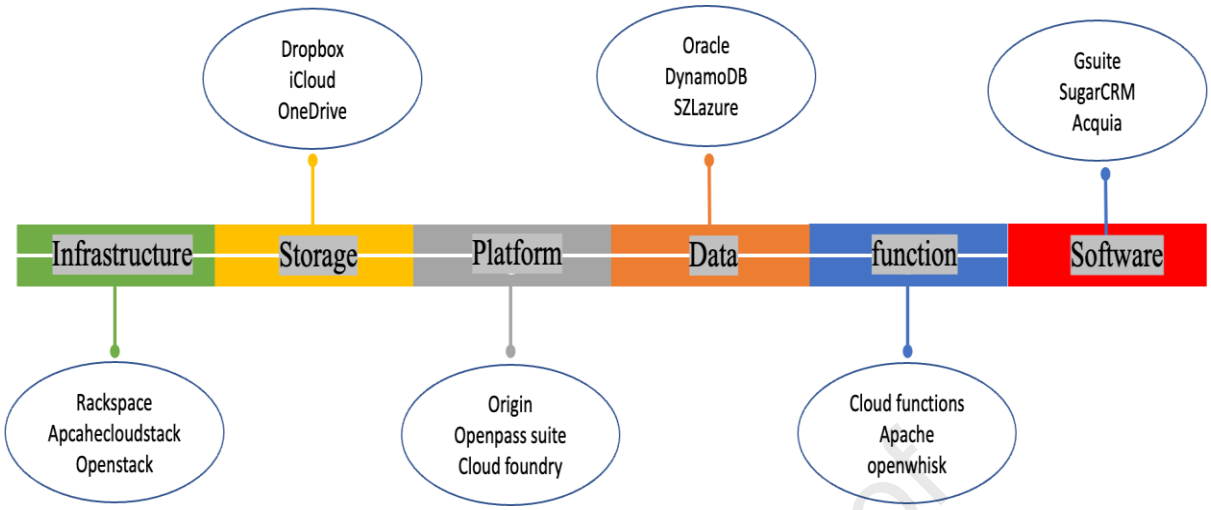


Figure 2: Architecture of IoT

The Internet of Medical Things (IoMT) is an infrastructure covering the globe which includes a collection of applications being used for medical devices so that information can be shared or communicated with the user and analyzer [51]. The data collected by these devices are mostly used for diagnosis and clinical care. The patient's health can be monitored and any upcoming threat can be avoided with the help of these connected devices [52, 53]. There are many expensive and challenging services that are responsible for the maintenance of a patient's economy and quality of life. In the coming decade, body-worn monitoring devices will see a surge in their application in the daily life of patients [54]. Despite having multiple advantages it can facilitate a breach of privacy and the personal information of the patient in the wrong hands. To operate any system efficiently it is required to assure its security. The system's security is related to its safety of operability. Most of the networking applications involved in the healthcare system work on a wireless platform which can result in a threat to the security of its user [55]. These security issues in this device can affect the personal and social life of the patient. The private data of the user can be used by any person with malicious intent to cause harm to the patient. Safe exchange of patient information can prevent the improper use of these devices. There are certain points over which the security of the devices should be addressed upon. They are represented in figure 2.

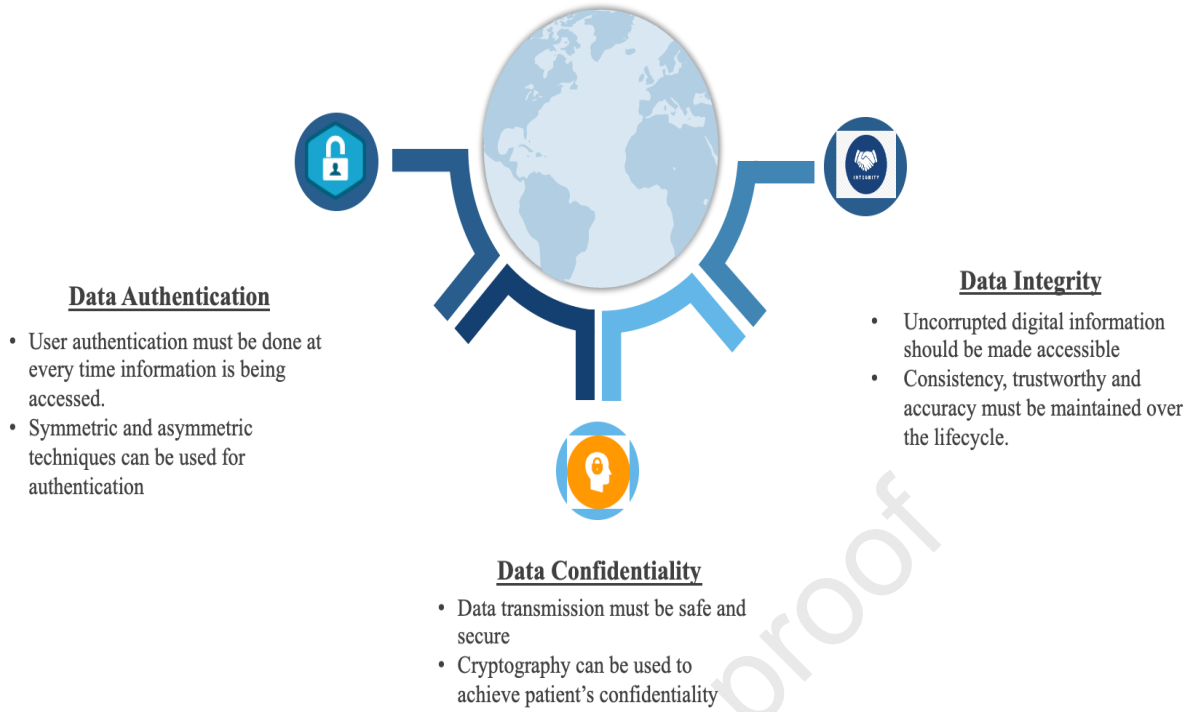


Figure 3: Security requirements for IoT in healthcare

An IoT system is represented by the three-layer model which can be classified as perception, transportation, and Application. A specific set of technologies is being used at each level. This also brings about certain issues and weaknesses in the security of the system. The perception layer relates itself to the physical sensors being used in various devices [56]. Wireless sensor network, Radio-frequency identification sensors network along with global positioning system. Various measurement-taking hardware such as actuators and sensors are included in this layer. The perception layer is vulnerable to security threats via Physical mode, impersonation and Service denials, routing, and data transit. In physical attacks, the hardware of the IoT is being targeted. This also requires the attacker to be in the close vicinity of the target. It can be done by tampering with the node of sensors or injecting malicious code to gain access to significant information which can be used to alter sensitive information [57]. Sometimes a fake identity can also be used for collusion attacks in a disturbed environment. This is regarded as impersonation. The device nodes have finite functionalities which can be exploited by the attacker to make them unavailable to the accessing authority also known as denial of services. The routing path of the device can be modified at an intermediate nodal level during the process of forwarding and collecting the data. With the help of sniffing the integrity and confidentiality of the data can be hacked during its transit [58]. The perception layer is being managed with the help of the transportation layer which provides it with a global milieu. This layer is

responsible for the transformation of data and information collected to the processing device with the help of existing network communication. This layer is also vulnerable to routing attacks, denial of service, and data transit attacks. The third layer for the operation of IoT is the application layer. It is closely related to the user. This layer can provide smart information of high quality to curate the needs of the customer. Computation of the data and its resource allocation is also done at this level of the system. It is exposed to leakage of data, denial of service, and injection of malicious code [59]. The ethics of the service providers can also be put under the lens to evaluate the safety of these connected devices. The solutions for the implementation of these devices require a reach within. If a wearable device is being given for monitoring the patient's in a high-risk areas such as mental health facilities then the ethical values of the person analyzing the data can be put under question, as if such devices and facilities will be able to provide protection [60].

Most of the time IoT tracking devices work on the public network and the data that is being transferred can be easily intercepted by implementing various attacks such as Man in the Middle and Botnet over the channel of communication. In case of a data breach, remote access can be controlled from the stored data in the cloud which can be compromising if any malicious software is being used [61]. The reputation of the user can be conceded if someone hacks the storage or device. If we talk about sleep tracking devices, they help in monitoring the sleep of the patient and help in reducing the cost and promoting quality of sleep by increasing the treatment efficiency [62]. These device does not only track the sleep of a patient but also various other physiological functions too. In case any kind of breach happens in the security of the data. The hacker can try to disturb the sleep of the user thereby affecting the treatment. The profiles of the user stored in the cloud can also be used to create fake profiles which can be used for fake advertisements [63]. Using any IoT device requires profile creation. Most user gives their consent without reading the terms of data usage and privacy policy of the company. This willingly offered data can be easily used by various organizations for making their decision regarding credit analysis [64]. Such kinds of issues scratch the aspirations of the customer to use the services of IoT and it will reduce the actual potential that can be harnessed from IoT. To target mass appropriation the security issues of the customer should be addressed with every specific end [65].

5. Ways to overcome the security concern

IoT is connected via a heterogenous network which comes with its challenges for protection and security. There is a certain number of inborn vulnerabilities associated with the IoT and

the objects which are fitted along with it to the physical world with the help of smart objects [66]. The information gathered by the devices is sent to analyzing monitoring authorities. This transferring and sharing of data can be considered a potential boundary that can diminish the prospects. These devices should be able to self-diagnose any security threat and inform the user about unauthorized access of information by any third party. IoT devices should have automation for the recognition of danger and response to threats [67]. Data provenance is a tool that helps in the recovery of data from the point of origin to its complete history chain. Any kind of action and modification during the life of data is documented. This helps in getting information about any changes that have been made in data that can lead to its misuse. A variety of data models can be used to get the data provenance related to any particular patient [68]. Authentication, access control, confidentiality, enforcement, and mobile can be used as tools for a strong network protocol to personalize and secure the service model [23]. The operation of IoT relies on data transmission which can be easily compromised. The restricted processing power of IoT devices hinders convoluting them through HTTP protocol. Therefore it is required to have a strong intercommunication standard or unifying the IoT communication can help in this regard. The data transfer from the device to the central processing unit is generally in a raw format which makes it vulnerable. The integrity of this data can be resolved by transmitting an enormous amount of data over discontinuous wireless connections [67].

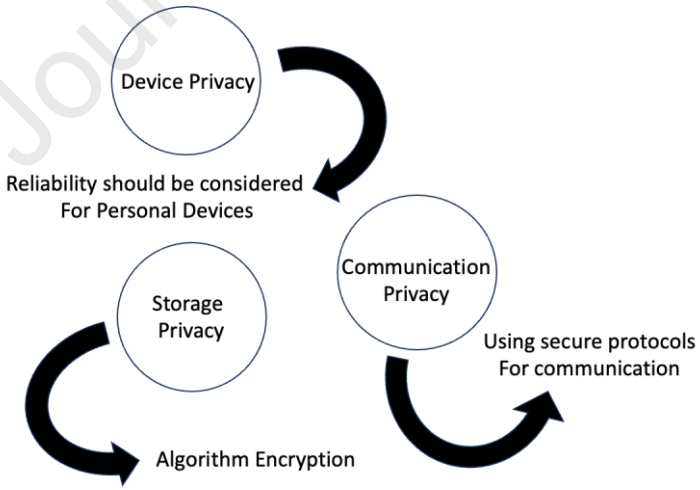


Figure 4: Privacy issues in IoT and their solutions

The privacy requirement of any device can be ascertained by identifying the externals, which can be doctors, devices, and patients before we allow the system resources to interact with

them. Privacy authentication is very important in monitoring remote patients so that their identity can be verified and it can be determined that the device is interacting with the correct person. The nodes which are authorized to interact should be activated in monitoring the patient remotely to check whether resource and service nodes are accessible. The nodes used at the patient's end should be efficient enough to identify authorized access to the device [68].

6. Conclusion

The amalgamation of a variety of technology is required to build an IoT. Due to this complexity, the system becomes more vulnerable to security and privacy threats. The generic engineering framework involved in patient monitoring remotely should meet the security requirements with the help of cryptographic algorithms. These algorithms should be device-specific to nurture the design & environment of patient-specific needs. The security and safety issues of a patient which arise from the application of IoT cannot be solved with the help of a single solution. To practice, the best security controls an informed user is also necessary. The management ability of the network and device automation can be of great help to deliver patient well-being and care. Delivering healthcare to patients efficiently and effectively, independent of time and location requires a new paradigm that is opened by IoT. The existing foundations of telemedicine have now been extended and better assessment of normal public health in a cohort sense has shifted the passive involvement of patient data gathering. Improving the outcomes for the patient and reducing the care cost are being balanced against the privacy and confidentiality of data and threats of cyber security. There is a vast source of data collection and potential to transfer clinical data, but there is a challenge to triage this data for clinical use. The cyber security and safety of patient data need to move faster than regulation and implementation of policy. The way forward for IoT needs superior standards every day to use the connected devices.

References

1. Shah AR, Goyal RK. Current status of the regulation for medical devices. Indian J Pharm Sci. 2008 Nov;70(6):695-700. doi: 10.4103/0250-474x.49085. PubMed PMID: 21369427; PubMed Central PMCID: PMCPMC3040860. eng.
2. Health, Center for Devices and Radiological. "Classify Your Medical Device." FDA, October 22, 2020. Accessed June 21, 2022. https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device.

3. U.S. Medical Device Manufacturers Market Report, 2021-2028." Accessed June 21, 2022. https://www.grandviewresearch.com/industry-analysis/us-medical-device-manufacturers-market.
4. Case Study - Artificial Intelligence in Health Care - How Apple Watch Becomes a Portable ECG. Interview with a Sparkbit Expert." Accessed June 21, 2022. https://www.sparkbit.pl/blogs/artificial-intelligence-health-care-apple-watch-becomes-portable-ecg-interview-sparkbit-expert.
5. Gia TN, Rahmani AM, Westerlund T, et al., editors. Fault tolerant and scalable IoT-based architecture for health monitoring. 2015 IEEE Sensors Applications Symposium (SAS); 2015 13-15 April 2015.
6. Islam SMR, Kwak D, Kabir MH, et al. The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access. 2015;3:678-708. doi: 10.1109/ACCESS.2015.2437951.
7. Haythornthwaite C, Wellman H. The Internet in Everyday Life: An Introduction. The Internet in Everyday Life2002. p. 1-41.
8. Atzori L, Iera A, Morabito G. The internet of things: A survey. Computer networks. 2010;54(15):2787-2805.
9. Hassan HK, Waheb MA, editors. The IoT for Healthcare Applications2021: IOP Publishing; 1).
10. Foote KD. DATAVERSITY [Internet]2022 2022/01/14/T08:35:00+00:00. Available from: https://www.dataversity.net/brief-history-internet-things/.
11. IoT Analytics [Internet]2014 2014/12/19/T10:08:11+01:00. Available from: https://iot-analytics.com/internet-of-things-definition/.
12. Kumar PM, Lokesh S, Varatharajan R, et al. Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. Future Generation Computer Systems. 2018 2018/09/01/;86:527-534. doi: https://doi.org/10.1016/j.future.2018.04.036.
13. Khattak HA, Ruta M, Di Sciascio EE, editors. CoAP-based healthcare sensor networks: A survey2014: IEEE.
14. WhatIs.com. "IoT Basics and Fundamentals: A Guide for Beginners." Accessed June 21, 2022. https://www.techtarget.com/whatis/feature/IoT-basics-A-guide-for-beginners.

15. Mahfoud H, Barkany AE, Biyaali AE. A Hybrid Decision-Making Model for Maintenance Prioritization in Health Care Systems. American Journal of Applied Sciences. 2016;13(4). doi: 10.3844/ajassp.2016.439.450.
16. Bhuvaneswari D, Gnana Jayanthi J, editors. A Research Insights of Big Data Analytics: Tools and Techniques, Issues and Challenges. Computer Networks and Inventive Communication Technologies; 2021 2021//; Singapore: Springer Singapore.
17. Rejeb A, Rejeb K, Treiblmaier H, Appolloni A, Alghamdi S, Alhasawi Y, Iranmanesh M. The Internet of Things (IoT) in healthcare: Taking stock and moving forwards. Internet of Thinigs. 2023 Feb 14:100721.
18. Amira A, Agoulmine N, Bensaali F, et al. Special Issue: Empowering eHealth with Smart Internet of Things (IoT) Medical Devices. 2019;8(2):33. PubMed PMID: doi:10.3390/jsan8020033.
19. Lee BM. Personalized service model for sharing medical devices in IoT health-platform. Advanced Science and Technology Letters. 2015;99:180-182.
20. Chandy A. A review on iot based medical imaging technology for healthcare applications. Journal of Innovative Image Processing (JIIP). 2019;1(01):51-60.
21. Davoodnia V, Slinowsky M, Etemad A. Deep multitask learning for pervasive BMI estimation and identity recognition in smart beds. Journal of Ambient Intelligence and Humanized Computing. 2020 2020/06/26. doi: 10.1007/s12652-020-02210-9.
22. Kumar P, Kumar R, Gupta GP, Tripathi R, Jolfaei A, Islam AN. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. Journal of Parallel and Distributed Computing. 2023 Feb 1;172:69-83.
23. Almadani B, Bin-Yahya M, Shakshuki EM. E-AMBULANCE: Real-Time Integration Platform for Heterogeneous Medical Telemetry System. Procedia Computer Science. 2015 2015/01/01/;63:400-407. doi: https://doi.org/10.1016/j.procs.2015.08.359.
24. Abo-Zahhad M, Ahmed SM, Elnahas O. A Wireless Emergency Telemedicine System for Patients Monitoring and Diagnosis. International Journal of Telemedicine and Applications. 2014 2014/05/06;2014:380787. doi: 10.1155/2014/380787.
25. Sharma N, Mangla M, Mohanty SN, et al. A smart ontology-based IoT framework for remote patient monitoring. Biomedical Signal Processing and Control. 2021 2021/07/01/;68:102717. doi: https://doi.org/10.1016/j.bspc.2021.102717.

26. Khan IH, Javaid M. Role of Internet of Things (IoT) in Adoption of Industry 4.0.0(0):2150006. doi: 10.1142/s2424862221500068.
27. Ullah F, Haq HU, Khan J, et al. Wearable IoTs and Geo-Fencing Based Framework for COVID-19 Remote Patient Health Monitoring and Quarantine Management to Control the Pandemic. Electronics. 2021;10(16). doi: 10.3390/electronics10162035.
28. Bhatt V, Chakraborty S. Improving service engagement in healthcare through internet of things based healthcare systems. Journal of Science and Technology Policy Management. 2023 Feb 9;14(1):53-73.
29. Acampora G, Cook DJ, Rashidi P, et al. A Survey on Ambient Intelligence in Healthcare. Proceedings of the IEEE. 2013;101(12):2470-2494. doi: 10.1109/JPROC.2013.2262913.
30. Tiwari A, Dhiman V, Iesa MAM, et al. Patient Behavioral Analysis with Smart Healthcare and IoT. Behavioural Neurology. 2021 2021/11/03;2021:4028761. doi: 10.1155/2021/4028761.
31. Mamdiwar SD, R A, Shakruwala Z, et al. Recent Advances on IoT-Assisted Wearable Sensor Systems for Healthcare Monitoring. Biosensors. 2021;11(10). doi: 10.3390/bios11100372.
32. Subhan F, Mirza A, Su'ud MB, Alam MM, Nisar S, Habib U, Iqbal MZ. AI-enabled wearable medical internet of things in healthcare system: A survey. Applied Sciences. 2023 Jan 20;13(3):1394.
33. Masud M, Gaba GS, Choudhary K, et al. Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare. IEEE Internet of Things Journal. 2022;9(4):2649-2656. doi: 10.1109/JIOT.2021.3080461.
34. Pal S. Introduction. In: Pal S, editor. Internet of Things and Access Control: Sensing, Monitoring and Controlling Access in IoT-Enabled Healthcare Systems. Cham: Springer International Publishing; 2021. p. 1-12.
35. Godwin JJ, Krishna BVS, Rajeshwari R, et al. IoT Based Intelligent Ambulance Monitoring and Traffic Control System. In: Balas VE, Solanki VK, Kumar R, editors. Further Advances in Internet of Things in Biomedical and Cyber Physical Systems. Cham: Springer International Publishing; 2021. p. 269-278.
36. Kalaivani K, Valarmathi G, Akshayaa U, et al., editors. Smart Ambulance with IOT and Periodic Data Analysis. 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT); 2022 10-11 March 2022.

37. Zeadally S, Das AK, Sklavos N. Cryptographic technologies and protocol standards for Internet of Things. Internet of Things. 2021;14:100075.

38. Imberti JF, Tosetti A, Mei DA, et al. Remote monitoring and telemedicine in heart failure: implementation and benefits. Current Cardiology Reports. 2021 2021/05/07;23(6):55. doi: 10.1007/s11886-021-01487-2.

39. Houlding E, Mate KKV, Engler K, et al. Barriers to Use of Remote Monitoring Technologies Used to Support Patients With COVID-19: Rapid Review. JMIR Mhealth Uhealth. 2021 2021/4/20;9(4):e24743. doi: 10.2196/24743.

40. Mohammed MN, Syamsudin H, Al-Zubaidi S, AKS RR, Yusuf E. Novel COVID-19 detection and diagnosis system using IOT based smart helmet. International Journal of Psychosocial Rehabilitation. 2020 Mar;24(7):229

41. Lee Y, Kim H, Kim Y, et al. A multifunctional electronic suture for continuous strain monitoring and on-demand drug release [10.1039/D1NR04508C]. Nanoscale. 2021;13(43):18112-18124. doi: 10.1039/D1NR04508C.

42. Aditya Manikanta A, Sahu H, Arora K, et al., editors. An IoT Approach Toward Storage of Medicines to Develop a Smart Pill Box. International Conference on Artificial Intelligence and Sustainable Engineering; 2022 2022//; Singapore: Springer Nature Singapore.

43. Kumar SK, Manimegalai R, Rajeswari A, et al., editors. A Literature Review: Performance Evaluation of Wearable system with Pill Dispenser Box for Post Covid Elderly Patients. 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N); 2021 17-18 Dec. 2021.

44. Hassanalieragh M, Page A, Soyata T, et al., editors. Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. 2015 IEEE International Conference on Services Computing; 2015 27 June-2 July 2015.

45. Lu Y, Xu LD. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. IEEE Internet of Things Journal. 2019;6(2):2103-2115. doi: 10.1109/JIOT.2018.2869847.

45. Corciovă C, Andritoi D, Ciorap R, editors. Elements of risk assessment in medical equipment. 2013 8TH INTERNATIONAL SYMPOSIUM ON ADVANCED TOPICS IN ELECTRICAL ENGINEERING (ATEE); 2013 23-25 May 2013.

46. Hospital Asset Tracking: Use Cases in Healthcare. en.

47. Sangwan RS, Qiu RG, Jessen D, editors. Using RFID tags for tracking patients, charts and medical equipment within an integrated health delivery network. Proceedings. 2005 IEEE Networking, Sensing and Control, 2005.; 2005 19-22 March 2005.

48. Manogaran G, Lopez D. Spatial cumulative sum algorithm with big data analytics for climate change detection. Computers & Electrical Engineering. 2018 2018/01/01/;65:207-221. doi: https://doi.org/10.1016/j.compeleceng.2017.04.006.

49. Manogaran G, Vijayakumar V, Varatharajan R, et al. Machine Learning Based Big Data Processing Framework for Cancer Diagnosis Using Hidden Markov Model and GM Clustering. Wireless Personal Communications. 2018 2018/10/01;102(3):2099-2116. doi: 10.1007/s11277-017-5044-z.

50. Manogaran G, Lopez D. A Gaussian process based big data processing framework in cluster computing environment. Cluster Computing. 2018 2018/03/01;21(1):189-204. doi: 10.1007/s10586-017-0982-5.

51. Arias O, Wurm J, Hoang K, et al. Privacy and Security in Internet of Things and Wearable Devices. IEEE Transactions on Multi-Scale Computing Systems. 2015;1(2):99-109. doi: 10.1109/TMSCS.2015.2498605.

52. Jing Q, Vasilakos AV, Wan J, et al. Security of the Internet of Things: perspectives and challenges. Wireless Networks. 2014 2014/11/01;20(8):2481-2501. doi: 10.1007/s11276-014-0761-7.

53. Manogaran G, Chilamkurti N, Hsu C-H. Emerging trends, issues, and challenges in Internet of Medical Things and wireless networks. Personal and Ubiquitous Computing. 2018 2018/10/01;22(5):879-882. doi: 10.1007/s00779-018-1178-6.

54. Mokliakova K, Srivastava G. Privacy Issues in Smart IoT for Healthcare and Industry. In: Ghosh U, Chakraborty C, Garg L, et al., editors. Intelligent Internet of Things for Healthcare and Industry. Cham: Springer International Publishing; 2022. p. 307-326.

55. Lin K, Chen M, Deng J, et al. Enhanced Fingerprinting and Trajectory Prediction for IoT Localization in Smart Buildings. IEEE Transactions on Automation Science and Engineering. 2016;13(3):1294-1307. doi: 10.1109/TASE.2016.2543242.

56. Frustaci M, Pace P, Aloi G, et al. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. IEEE Internet of Things Journal. 2018;5(4):2483-2495. doi: 10.1109/JIOT.2017.2767291.

57. Laplante PA, Kassab M, Laplante NL, et al. Building Caring Healthcare Systems in the Internet of Things. IEEE Systems Journal. 2018;12(3):3030-3037. doi: 10.1109/JSYST.2017.2662602.

58. Dimitrov DV. Medical Internet of Things and Big Data in Healthcare. Healthc Inform Res. 2016 7;22(3):156-163. doi: 10.4258/hir.2016.22.3.156.

59. Kolla BP, Mansukhani S, Mansukhani MP. Consumer sleep tracking devices: a review of mechanisms, validity and utility. Expert review of medical devices. 2016;13(5):497-506.

60. Sadek I, Seet E, Biswas J, et al. Nonintrusive Vital Signs Monitoring for Sleep Apnea Patients: A Preliminary Study. IEEE Access. 2018;6:2506-2514. doi: 10.1109/ACCESS.2017.2783939.

61. Peppet SR. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. Tex L Rev. 2014;93:85.

62. Maksimović M, Vujović V, Perišić B, editors. A custom Internet of Things healthcare system. 2015 10th Iberian Conference on Information Systems and Technologies (CISTI); 2015 17-20 June 2015.

63. Bui N, Zorzi M, editors. Health care applications: a solution based on the internet of things2011.

64. Elkhodr M, Alsinglawi B, Alshehri M, editors. Data Provenance in the Internet of Things. 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA); 2018 16-18 May 2018.

65. Jaigirdar FT, Rudolph C, Bain C, editors. Can I trust the data I see? A Physician's concern on medical data in IoT health architectures2019.

66. Suhardi, Ramadhan A, editors. A Survey of Security Aspects for Internet of Things in Healthcare. Information Science and Applications (ICISA) 2016; 2016 2016//; Singapore: Springer Singapore.

67. Arora A, Kaur A, Bhushan B, et al., editors. Security Concerns and Future Trends of Internet of Things. 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT); 2019 5-6 July 2019.

68. Jaiswal S, Gupta D, editors. Security Requirements for Internet of Things (IoT). Proceedings of International Conference on Communication and Networks; 2017 2017//; Singapore: Springer Singapore.

The authors would like to express their gratitude to Ganpat University for its support and encouragement in the development of this review article.

Author Contributions:

Conceptualization: BGP, JBP

Formal analysis: BGP and JBP

Resources: BGP, PE and JBP

Data curation: BGP, AP and PE

Writing—original draft preparation : AP, AT and BT

Review and editing: BGP, PE, JBB

Project administration: BGP and JBP

All authors have read and agreed to the published version of the manuscript.

All literature is collected form various scientific journals. No specific data source used here.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Sincerely,

Yours sincerely,

Dr.Bhupendra Prajapati,

Professor, Ganpat Univeristy

Emails: bhupen27@gmail.com/bhupendra.prajapati@ganpatuniversity.ac.in
Contact: +91-9429225027/7990533373