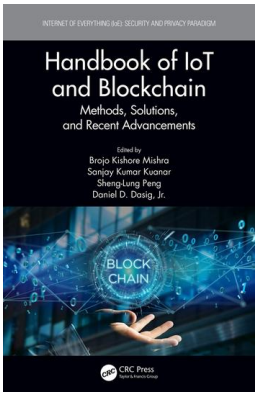


Handbook of IoT and Blockchain
Methods, Solutions, and Recent Advancements

Brojo Kishore Mishra, Sanjay Kumar Kuanar, Sheng-Lung Peng, Daniel D. Dasig

Application and Challenges of IoT in Healthcare

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9780367854744-2
Subhashree Sahoo, Debabrata Dansana, Brojo Kishore Mishra
Published online on: 26 Nov 2020

2 Application and Challenges of IoT in Healthcare

[1]Subhashree Sahoo, [2]Debabrata Dansana, and [2]Brojo Kishore Mishra
[1]Pondicherry University, Kalapet, Pondicherry, India
[2]GIET University, Gunpur, India

CONTENTS

2.1 INTRODUCTION

Healthcare changes dramatically as a result of technological developments, from anesthetics and antibiotics to magnetic resonance imaging scanners and radiation therapy. Future technological innovation is going to keep remodeling healthcare, however, whereas technologies (new drugs and treatments, new devices, new social media support for healthcare, etc) can drive innovation, human factors can remain one of the persistent limitations of breakthrough. No predictions will satisfy everybody. There are no two ways regarding healthcare; technological developments in healthcare have saved innumerable patients and are continuously raising our quality of life. Not solely that, however; technology within the medical field has had a huge impact on nearly all processes and practices of healthcare professionals.

Advancements in medical technology have allowed physicians to better diagnose and treat their patients since the start of the professional practice of medicine. Because of the continual development of technology within the medical field, many lives are saved and also overall quality of life continues to increase over time. Although medical culture is comparable, there are dramatic technological changes, and truly, these changes would be exhausting to explain. Does anybody even know how an infusion pump works? They used to be clockwork and currently nearly everything contains a computer and includes a color screen and plenty of buttons. Implanted defibrillators that use telephone networks and internet sites to keep cardiologists up thus far with their patients are simply magic. New pharmaceuticals that change moods, change

pressure, or kill bacteria: all are trendy magic. Some of what appears to us these days like science fiction becomes routine in the future, even perhaps in our lifetimes. However, much of today's human story regarding relationships, hopes, error, grief, and denial is going to stay entirely recognizable within the future. We will still have authority gradients, we will still have dispute over human error, and patients can still be made helpless so they are easier to treat. The explanation is that technology is driven by the market.

If someone has an idea that they might convert into a physical realization that they can sell, they will additionally patent it or license it, and thereby build a return on their investment. This, in turn, can encourage them to seek out ways of making it smaller and cheaper, and selling it on a bigger scale. Thus it is technology-driven. In contrast, human culture does not build a profit for anybody.

The main reason behind healthcare is patients, and they should be at the center of it. In this article, we will discuss some of the technological trends and their challenges in healthcare. In this era of science, healthcare is nothing but a market for technology and in this case hospitals which act as consumers, and these consumers are ready to pay enough money for technological equipment which includes minimization of cost, division of labor and so on.

2.2 MEDICINE AND TECHNOLOGY

In today's world, technology plays a vital role in each business more than in our personal lives. Out of all of the industries in which technology plays a vital role, healthcare is certainly one of the foremost. This is answerable for saving innumerable lives all around the world.

Medical technology could be a broad field where innovation plays a vital role in sustaining health. Areas such as biotechnology, pharmaceuticals, information technology, the development of medical devices and instrumentation, and others, have all created vital contributions to increasing the health of individuals all around the world. From "small" innovations like adhesive bandages and articulatio-talocruralis braces to larger, additional advanced technologies like magnetic resonance imaging machines, artificial organs, and robotic prosthetic limbs, technology has beyond question created an unimaginable impact on medicine. In the healthcare trade, the dependence on medical technology cannot be exaggerated, and as a result of the development of those brilliant innovations, healthcare practitioners will still find ways to enhance their practice—from better diagnosing, surgical procedures, and improved patient care.

2.2.1 Information Technology and Medicine

Information technology has created vital contributions to our world, particularly within the medical trade. With the increased use of electronic medical records (EMR), telehealth services, and mobile technologies such as tablets and smart phones, physicians and patients are each seeing the advantages that these new medical technologies are bringing.

Medical technology has evolved from introducing doctors to new instrumentation to use within private practices and hospitals to connecting patients and doctors

thousands of miles away through telecommunications. It is not uncommon in today's world for patients to conduct video conferences with physicians to save lots of time and cash that would otherwise be spent on traveling to a different geographic location, or send health information instantly to any specialist or doctor in the world.

With more and more hospitals and practices using medical technology such as mobile devices at work, physicians currently have access to any type of information they have—from drug information, analysis and studies, patient history or records, and so on—in mere seconds. And, with the power to effortlessly carry these mobile devices around with them throughout the day, they are never far away from the information they have. Applications that aid in distinguishing potential health threats and examining digital information such as x-rays and CT scans additionally contribute to the advantages that information technology brings to medicine.

2.2.2 Medical Equipment Technology

Improving the standard of life is one of the greatest advantages of integration new innovations into medicine. Medical technologies such as minimally invasive surgeries, better monitoring systems, and easier scanning instrumentation are permitting patients to pay less time in recovery and enjoy a healthy life for longer.

The integration of medical instrumentation technology and telehealth has also created robotic surgeries, where in some cases physicians do not even have to be compelled to be within the operating theater with a patient as surgery is performed. Instead, surgeons will operate out of their "home base", and patients will have the procedure carried out in a hospital or clinic in their own hometown, eliminating the hassles and stress of health-related travel. With different robotic surgeries, the doctor remains within the room, operating the robotic devices; however, the technology allows for a minimally invasive procedure that leaves patients with less scarring and considerably less recovery time.

2.2.3 Technology and Medical Research

Medical scientists and physicians are perpetually conducting research and testing new procedures to help prevent, diagnose, and cure diseases as well as developing new medicines that may reduce symptoms or treat ailments.

Through the utilization of technology in medical analysis, scientists are able to examine diseases on a cellular level and manufacture antibodies against them. These vaccines against dangerous diseases like protozoa infection, polio, MMR and others prevent the unfolding of disease and save thousands of lives all around the globe. In fact, the World Health Organization estimates that vaccines save about three million lives each year, and prevent lots of others from acquiring deadly viruses and diseases.

2.2.4 3D Printing

Today, it is possible to reproduce bones and a few internal organs using 3D printing technology. These artificial organs and bones will then be introduced into the body of the patient to replace diseased or problematic areas. Surgeons are also using

3D printing technology to gain a far better understanding of what is happening within their patients' bodies. With a 3D model, it is considerably easier for a surgeon to carry out a more in-depth check of the problem and simulate a variety of solutions or possible operations that may be undertaken before performing the actual surgery on the patient.

Similarly, 3D printing has revolutionized medical specialty. With a 3D printer, obtaining a custom-made prosthetic hand or leg is considerably cheaper. It is currently possible to custom print prosthetic hands, for example, for a baby that needs totally different models as it grows, rather than having to travel and get a replacement prosthetic hand fitted every year. Plus, with the huge developments that are being created within the 3D printing industry, prices related to this technology are reducing every day.

One of the various forms of 3D printing that is utilized in the medical device field is bioprinting. Instead of printing using plastic or metal, bio printers use a computer-guided pipet to layer living cells, described as bio-ink, on top of one another to make artificial living tissue in a laboratory.

These tissue constructs or organoids can be used for medical analysis as they mimic organs on a miniature scale. They are also being trialed as cheaper alternatives to human organ transplants.

Another application of 3D printing within the medical field is making patient-specific organ replicas that surgeons can use to practice on before performing sophisticated operations. This method has been tried in order to speed up procedures and minimize trauma for patients.

This type of procedure has been performed with success in surgeries starting from a full-face transplant to spinal procedures and is starting to become routine practice.

Sterile surgical instruments, such as forceps, hemostats, surgical knife handles, and clamps, are often made using 3D printers. Not only will 3D printing manufacture sterile tools; some are provided by the traditional Japanese practice of origami that means they are precise and might be created extremely small in size. These instruments are often used to operate on small areas while not inflicting inessential extra harm to the patient.

One of the main aspects of using 3D printing instead of traditional production methods to provide surgical instruments is that production prices are considerably lower.

3D printing within the medical field may be used to manufacture prosthetic limbs that are custom-made to suit and match the user. It is common for amputees to wait weeks or months to receive prosthetics through the normal route; however, 3D printing considerably accelerates the method, making less expensive products that provide patients continuing functionality just as traditionally factory-made prosthetics.

2.2.5 Digitization of Health Records

Electronic Health Records (EHRs) replacing outdated paper records has been a vast game changer for everybody within the medical world. Medical assistants, medical coding professionals, and registered nurses are just some of the roles that are covered by this industry-wide implementation.

Nurses and technicians are answerable for inputting patient information into a central, digitized system. Medical billers and coders update patient records with diagnostic codes such as test results and submit medical claims to insurance corporations. Not only will patients access their records at the click of a button; it is equally ensured that mistakes are caught a lot more quickly without needing to pore over unreadable physicians' handwriting.

In medicine, the primary information technology wave to hit the art and science of healing was the digitization of medical files, currently referred to as electronic health records (EHRs). The data contained in EHRs together with alternative sources has the potential to remodel medical practice by leveraging information, technologies, and healthcare delivery to improve the overall potency and quality of care at a reasonable price. The widespread adoption of EHRs has generated massive sets of information. The skillful merging of datasets collected from patients and physicians might be a viable avenue to strengthen healthcare delivery. These huge datasets are currently taken as a byproduct of medical practice instead of as useful assets that would play important roles in patient care. Currently, for example, most EHRs collect quantitative, qualitative, and transactional information; all of that could be collated, analyzed, and applied using sophisticated procedures and techniques that are currently available to make use of text-based documents containing disparate and unstructured data. The purposeful use of information is not a mystery to medical practice. From their humble beginnings, evidence-based undertakings are grounded within the principle that questions answered through the methodology were superior to anecdotes, expert opinion, panels, and testimonials. In terms of acknowledging the worth of information in guiding a rational and logical higher cognitive process, medicine has been at the forefront of adapting to modernity. However, physicians, nurses, and healthcare facilities are slow to embrace the most recent methods to completely use the information contained in EHRs.

There are many benefits of EHR which have been brought into healthcare. Some of them are listed below.

- Greater patient care
- Improved public health
- Ease of workflow
- Lower healthcare costs

2.2.5.1 Greater Patient care

EHR will mechanically alert the treating doctor to potential problems (such as allergies or intolerances to certain medicines). EHRs may be accessed from nearly any medical facility, which is very helpful for doctors assessing non-local patients.

2.2.5.2 Improved Public health

EHRs give valuable information to clinical researchers, serving to advance medical data and also the development of treatments for common health issues (such as viral outbreaks).

A standardized health IT system will give insights into how widespread an endemic is, enabling preventive measures (such as increased respiratory disorder shot production) to be put in place rather more quickly.

2.2.5.3 Ease of Workflow

Medical billers and coders are a number of the most-impacted allied physicians, and—according to the Bureau of Labor Statistics—demand for this sector is predicted to grow by 13% from 2016 to 2026. The introduction of EHRs has just made life easier for medical billers and coders.

Entering information into a processed system is way less time-consuming than paper-based strategies, and it reduces the danger of errors in patient information and money details. Accessing patient records digitally additionally permits medical committal-to-writing experts to work from home, increasing efficiency and productivity.

2.2.5.4 Lower Healthcare costs

According to recent research, the shift from paper-based patient records to electronic records reduces the costs of outpatient care by 3%.

2.2.5.5 Disadvantages of EHR

Theoretically, shifting to EHRs ought to change everything for the better. Sadly, there are some kinks that also need to be smoothed out. Instead of a records system that works fluidly, several networks lack interconnectivity, which suggests that several do not have the ability to speak to each other. Sometimes, this lack of communication will place patients' health at risk.

2.2.6 Big Data

Big data is the buzzword nowadays. It is seen everywhere, particularly within the healthcare business. Historically, the massive quantity of data generated by the healthcare business was held as a hard copy. This information has the potential to support a wide range of healthcare and medical functions. The conversion of such information is termed big data. All of the data that is associated with patient healthcare and wellbeing makes up big data.

The wide diversity of big data and also the pace at which it is managed makes it overwhelming. It includes clinical information from CPOE and clinical decision support systems, physicians' written notes and prescriptions, medical imaging, laboratory, pharmacy, insurance, and other administrative data; patient data in electronic patient records (EPRs); machine-generated or sensor data, such as from monitoring vital signs; social media posts, together with Twitter feeds, blogs, status updates on Facebook and different platforms, and web pages; and less patient-specific data, together with emergency care information, news feeds, and articles in medical journals.

Big data is extremely helpful within the healthcare business. Over the past decade, electronic health records (EHR) have been widely adopted in hospitals and clinics

worldwide. Important clinical data and a deeper understanding of patient sickness patterns may be studied from such information. It will help to boost patient care and improve efficiency. Sometimes, this lack of communication will place patients' health at risk.

With its diversity of format, type, and context, it is tough to merge big healthcare data into standard databases, making it tremendously difficult to process, and hard for business leaders to harness its important promise to remodel the industry.

Despite these challenges, many new technological enhancements are permitting healthcare big data to be born again into helpful, weighted data. By leveraging applicable software package tools, big data is informing the movement toward value-based healthcare and is open to outstanding advancements, even while reducing prices. With the wealth of knowledge that healthcare data analytics provides, caregivers and administrators will currently make better medical and monetary decisions while still delivering an ever-increasing quality of patient care. But adoption of big data analysis in healthcare has lagged behind alternative industries thanks to challenges like privacy of health data, security, sliced knowledge, and budget constraints. Meanwhile, 80% of executives from financial services, insurance, media, entertainment, manufacturing, and supply firms surveyed report their investments in big data processing as "successful," and almost one in five declare their big data initiatives are "transformational" for his or her corporations.

There are at least two trends nowadays that encourage the healthcare business to embrace big data. The primary is the move from a pay-for-service model that

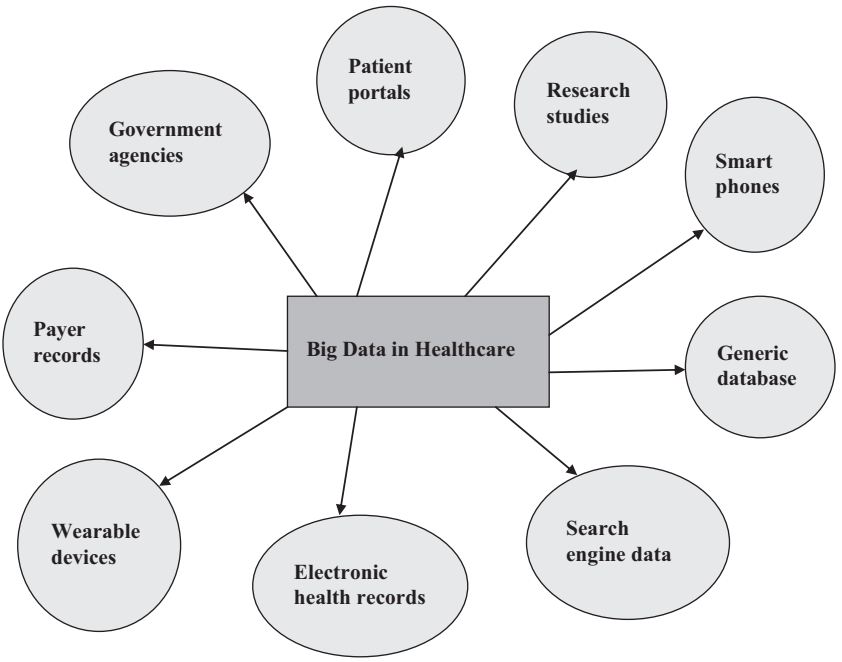


FIGURE 2.1 Sources of Big data.

financially rewards caregivers for performing procedures, to a value-based care model that rewards them for supporting the health of their patient populations. Healthcare data analytics can change the measuring and tracking of population health, thereby sanctioning this switch. The second trend involves exploiting big data analysis to deliver data that is evidence-based and can, over time, increase efficiencies and facilitate sharpening of our understanding of the most effective practices related to any disease, injury or ill health.

Undoubtedly, adopting the utilization of healthcare big data will remodel business, driving it from a fee-for-service model toward value-based care. In short, it will deliver on the promise of lowering healthcare prices while revealing ways in which to deliver superior patient experiences, treatments, and outcomes.

Using big data has multiple benefits such as

- Reducing healthcare costs
- Predicting epidemics
- Avoiding preventable deaths
- Improving quality of life
- Reducing healthcare waste
- Improving efficiency and quality of care
- Developing new drugs and treatments

2.2.6.1 Applications of Big Data in Healthcare

- Integrating big data with medical imaging.
- Telemedicine
- Reduce fraud and enhanced security
- Predictive analytics in healthcare
- Using health data for strategic planning
- Real-time alerting
- Electronic health records
- Enhancing patient engagement
- Smoother hospital administration
- Big data to fight cancer.

2.3 REMOTE HEALTH MONITORING

Remote health monitoring, also described as remote patient monitoring, is the technique of exploiting technology to observe patients in non-clinical environments, such as within the home. Once incorporated within the management of chronic diseases, remote health monitoring has the potential to considerably improve quality of life for patients and so it ought to come as no surprise that this technology is growing progressively standard. Remote health monitoring could be a specific field; however, associated technologies frequently share similar elements. Firstly, a monitoring device needs a sensor which might generate specific physiological information and wirelessly communicate this data to both the patient and aid professionals.

Shared information storage for this data is additionally crucial, both as software that may analyze health information and supply treatment recommendations and

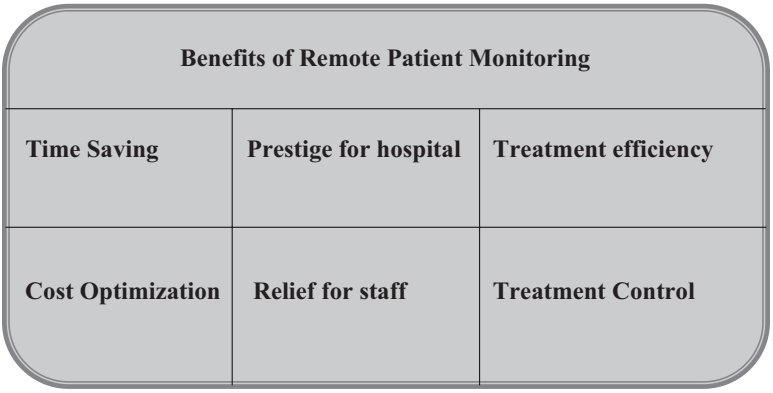


FIGURE 2.2 Benefits of Remote Health monitoring in Healthcare.

alerts. Health-monitoring technologies that accept smartphone apps have become progressively standard. These will aid patients with varied conditions; however, the technology is most generally used for monitoring heart conditions and diabetes. Diabetics need to regulate their weight, blood pressure and blood glucose levels to remain healthy.

2.3.1 Benefits of Remote Health Monitoring

- Improved education, support and feedback
- Improved quality of care
- Better access to care
- Daily assurance
- Cost-effective
- Makes healthcare services accessible
- Makes healthcare services efficient
- Makes healthcare consumer centric
- Improves patient's lifestyle
- Allows sending data from patients to doctors in real time.

Below is a figure which describes the key benefits of using remote health monitoring in healthcare units.

2.3.2 Challenges of Remote Health Monitoring

Some of the most general difficulties encountered with remote health monitoring in healthcare units are listed below.

- Confidentiality and privacy
- Users' attitudes
- Organizational and technological barriers
- Maintainance cost

- Implementation cost
- Costly modern systems
- Poor design and implementation
- Insufficient investment
- System incompatibility with personal tasks
- Data manipulation, rewriting, data misrepresentations
- Documentation mistakes
- Violation of patients' legal rights
- Decrease in face-to-face communication between doctors and patients
- Weight of wearable devices

Although the technology has several proven successes, its main flaws mask the fact that remote health monitoring will heavily count on patients taking a vigorous role in their own health and a few patients are more passive or forgetful than others. Wireless technologies also are not appropriate for some rural areas, and a few older patients might not know how to use modern technologies such as apps. Any collected health data additionally has to be encrypted and protected from hackers, and a few remote health-monitoring technologies are very expensive.

However, remote health monitoring will provide patients with additional power to keep an eye fixed on their health and may offer peace of mind for those managing chronic conditions. As technology will alert patients and healthcare professionals to slight physiological changes, any definitely dangerous conditions are also likely to be caught and treated earlier. The prices are high and therefore the technology still has to be refined; however, as those barriers bit by bit are countermined, remote monitoring is probably going to become a core part of preventive care in the longer term.

2.3.3 Obstacles of Remote Health Monitoring Usage

There are several obstacles in the path of Remote Health Monitoring (RHM) usage. Below are some of the points which describe these.

2.3.3.1 Is Not Accessible for Everyone

RHM needs good broadband connectivity that is difficult to attain for small healthcare establishments and rural hospitals. On the other hand, it is necessary to keep under consideration that not everybody owns a smartphone, and older people typically face difficulties in using modern gadgets, such as mobile phones.

2.3.3.2 Patients' and Doctors' Skepticism

RHM seems to be the least effective patient engagement initiative according to the NEJM Catalyst Insights Council survey. The researchers justify these statistics by the very fact that the employment of wearable remains unobtainable for everyone. By the way, doctors who took part in the survey did not notice any improvements in chronic disease management. Additionally, healthcare professionals added their expertise to express doubt that technology alone is probably going to alter the behavior of higher-risk patients. Doctors are involved in the difficulties they will face

handling received information. Some patients are afraid that their personal health information will be obtained by third parties and used for dubious purposes.

2.3.3.3 The Necessity of Extra Custom Healthcare Software

Once the information is collected IT departments need to direct it from RHM devices to electronic medical history systems (EMRs) by means of multiple third-party applications.

2.3.3.4 Uncertain Reliability

Fashionable fitness wearables supporting physical activity are perceived to have giant variations of accuracy with error margins up to 25 percent. The reliability of RHM information is called into question also. For example, a review in JAMA dermatology showed that smartphone apps for skin cancer detection have a 30 percent failure rate. The lack of reliability is the most significant issue that has to be fixed before devices and applications might be utilized by healthcare suppliers.

RHM is extremely keen on the individual's motivation to manage their health. If it is not the patient's temperament to be a lively participant in their care, RHM implementation can probably fail. Price is additionally a barrier to its widespread use. There's an absence of compensation pointers for Remote Patient Monitoring (RPM) services, which can deter its incorporation into clinical observation. The shifting of untrustworthiness identified with RHM raises liability problems. There are no clear pointers of relevance as to whether or not clinicians need to intervene when they receive an alert in spite of the urgency. The continual flow of patient information needs a frenzied team of healthcare suppliers to handle the data, which may, in fact, increase the work. Though technology is introduced with the aim of extending potency, it will become a barrier to some healthcare suppliers that do not seem to be technological. There are common obstacles that health information processing technologies encounter that apply to RHM. Looking at the comorbidities monitored, RHM involves a wide choice of devices in its implementation. Standardization is needed for information exchange and ability among multiple elements. Moreover, RHM development is extremely keen on an intensive wireless telecommunications infrastructure, which cannot be on the market or possible in rural areas. Since RHM involves the transmission of sensitive patient information across telecommunication networks, data security could be a concern.

2.4 DISADVANTAGES OF USING IOT IN HEALTHCARE

2.4.1 Expensive

A progressively refined health technology does not return low cost. We have got to grasp that each first-world national healthcare system faces a variety of challenges; one among those is the aging population. People live longer. This suggests an increased health need; however, the working population generating financial gain to procure the healthcare system is reduced. Therefore one thought would be: Is the high price that comes with technology economically viable for the government?

2.4.2 Time-consuming Adaption

As we know, technology is continually evolving. Many times there will be new software systems, new upgrades, and a brand new way of doing things. In order to keep a competitive edge, hospital employees have got to sustain such changes. This will be a struggle for a few, particularly for the older workers.

2.4.3 Technology Dependent

Once the workers have adapted to the new manner of labor, there comes a further drawback. It is not uncommon for a computer system to face technical errors. The healthcare informatics system is no exception. This drawback is particularly crucial within the Accident & Emergency (A&E) Department. Varied departments within the hospital are interconnected by a standard data system. Once one department is down, others are affected. For instance, a patient is rushed into the A&E Department. Once there is a mistake retrieving blood analysis data, the remainder of the procedures following it will be delayed. This can cause great inconvenience or worse; it is even going to have adverse effects on the patient's health condition.

2.4.4 Susceptibility to Network Hackers

Patients' medical history and data should be kept confidential for legal reasons. But even if the healthcare system network is equipped with security measures it is possible for network hackers to extract this information, which is now a matter of concern for Health Informatics.

2.4.5 Technical Requirements

For an IoT network to give value to a business, it should work as one, cohesive system. From a technical perspective, the truth is that IoT is commonly fragmented and lacks ability. To combat this, platforms should be ready to operate across devices no matter the build, manufacturer or business. Overcoming compatibility problems may be a

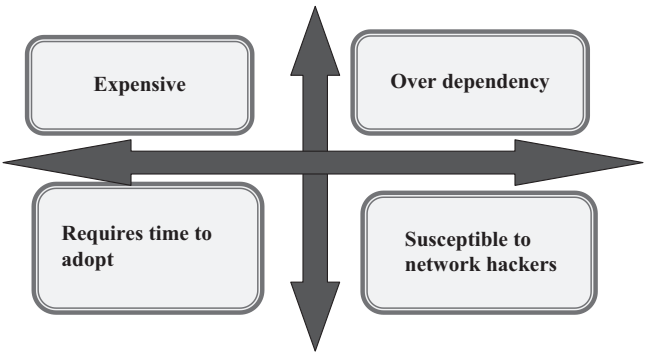


FIGURE 2.3 Disadvantages of IoT in Healthcare.

vital IoT hurdle; however, more businesses are beginning to modify increased ability through open-source development.

2.4.6 Regulatory Concerns

IoT implementations are collecting massive amounts of information that would probably be sensitive or harmful if exposed. This includes personal knowledge concerning workers or customers, as well as proprietary business knowledge concerning operations and internal processes. From a restrictive perspective, privacy considerations, such as clarifying who will access IoT knowledge and the way that data is employed, should be addressed. Governments and business bodies have to be compelled to set standards and rules for the varied industries to make sure that knowledge is not misused.

2.4.7 Scalability

Businesses typically successfully develop an IoT application with several devices in a single location. However, they later discover that measurability is a problem. It is crucial that the planning of a system caters for extra resources.

2.4.8 Time Constraints

The rolling out of IoT is an extended and expensive endeavor for businesses. Speedy changes in technology mean that businesses run the danger of any new technology system becoming obsolete as soon as it is installed. To profit from the advantages of a brand new IoT system, businesses should attempt to eliminate as many of the obstacles as possible from the company's development method to achieve a quick and economical rollout. Equally they have to make sure that they partner with competent service suppliers that may meet their technology wants and modify agile solutions.

2.4.9 Security

IoT devices are typically susceptible to security breaches due to poor design. This may have a significant impact on company knowledge security, and also put pricey IoT-related equipment in danger. For this reason, IoT requires robust authentication methods, encrypted information and a platform that may track irregularities on a network. If businesses are clear on how IoT information is collected and used, shopper confidence in IoT will grow.

2.4.10 Managing IoT Obstacles

The inflow of information as a result of adopting IoT can modify businesses to considerably improve management and operations. However, despite the prospect of IoT remodeling businesses, implementing associated IoT resolutions will be fraught with complexities. Whereas deploying IoT technologies has huge potential, in order to exploit these advantages IoT challenges ought to be addressed effectively, and

potential challenges and security problems ought to be overcome to ensure IoT success. Problems such as technology, regulation, measurability, roll out and security all need to be addressed.

2.5 CHALLENGES WITH MANAGING IOT TECHNOLOGIES

While the IoT can bring important advantages, they will be difficult to implement. Forbes Insights recently surveyed almost five hundred executives and, when asked about their greatest challenge in building their IoT capabilities, twenty-nine said it had been the standard of IoT technology. This is not stunning. In some cases, IoT platforms must support thousands of vendors, dozens of standards, and be able to scale to countless devices, along with creating and receiving billions of messages.

IoT-based solutions are generally created from a number of technologies, some already existing and a few entirely new. Everything has its own path of development, and once they are combined, they will produce an atmosphere that is complicated and speedily dynamical. Here are four challenges with managing IoT technologies these days.

2.5.1 Integrating New Technologies into Existing Environments

In the era of the smartphone, it will appear as if each machine is connected and sharing data; however, that is not the case. Within the client world, a combination of technologies competes for dominance, and standardization remains elusive. As a result, comparatively few homes, appliances, or other commodities are literally IoT-enabled and connected. In the industrial world, it gets even more sophisticated owing to the character of the investments. Capital instrumentality that has been within the field for twenty years or so is not invariably a viable target for replacement, as a stove or refrigerator could also be within the shopper world. Retrofitting is usually the sole realistic resolution to bring IoT capabilities to existing instrumentation. However, retrofitting is neither easy nor assured. Whereas connecting legacy equipment and systems offers huge advantages and is a very important step within the IoT initiatives at several industrial corporations, the hurdles to implementation may be formidable.

That said, corporations are creating vital strides within this space. They are adding complete sensors and cameras to existing environments and devices to monitor and collect information regarding machine performance and health. These sensors attached to existing devices and connect with gateways to firmly collect and transmit information, which might then be analyzed.

2.5.2 Managing Protocol Complexity

Another huge challenge within the development of the IoT is the immense variety of protocols. Some of the common standards include:

- BLE (Bluetooth low energy)
- ZigBee
- Z-Wave

- Thread
- We-Mo

In some ways, BLE, ZigBee, Z-Wave, and Thread are similar. They are all wireless technologies that use mesh networks to wirelessly connect and network IoT devices while not involving a cellular or Wi-Fi signal. However, they differ in the frequency they use, and they vary in operation and therefore the variety of devices they will support at a given time. We-Mo, however, needs Wi-Fi, which eliminates the requirement for a hub or controller, and permits devices to attach directly via the net. Two of the massive disadvantages of this technique are that it needs a lot more power and processing capability than alternative, lower-energy choices.

Again, this can only be a brief list; the quantity of protocols is in depth. Each has its advantages and downsides; however, since there is no single common standard, businesses should confirm the correct protocol for every use case and make sure the technologies they select are compatible with their overall platform. As standards are still evolving, it is going to be advantageous to exchange or upgrade the method.

2.5.3 Networking Challenges

Beyond the various completely different protocols and disparate hardware, there are basic networking challenges that have got to be addressed to make IoT-enabled devices a reality. The primary step is to make sure that information is flowing quickly and reliably. Security is additionally crucial, as IoT devices are often evolving into targets for hackers and cyber terrorists. Once devices connect, they have to certify, information should be encrypted, and they ought to communicate their presence and activity.

Power consumption and bandwidth present alternative distinctive challenges. During a scenario where thousands of devices are communicating with each other, frequent communication and transmission may be a drain on battery-operated devices. In those cases, minimal, economical power usage is vital. During a scenario where thousands of devices are communicating over wireless networks, bandwidth will become a priority, and costs will increase quickly. The goal should be to keep IoT information streams as compact and economical as possible.

2.5.4 Best Practices in the Era of IoT

Within the IT world, best practices are generally described as procedures that are well known and considered to be the most effective. Nowadays there's an absence of best practice to help businesses write code, manage the life cycle of certain IoT-related hardware and software systems, and address the distinctive kinds of breaches that may occur, together with intrusions that are initiated at the device level. Without best practices as a road map, programmers and IT professionals are traveling in unmapped waters. Consider the Mirai botnet attack in October 2016. Throughout this incident, IT professionals saw firsthand how prolific a breach can be. Although the incident was damaging, many things were learned, together with the importance of getting an IoT security strategy and the concept of fast response.

As the IoT continues to proliferate, there are guaranteed to be growing pains. Hardware can still advance and improve. The software system can become a lot more refined. New standards, protocols and connectivity choices can become much more prevalent. However, businesses should ensure that their new capabilities stay compatible with legacy systems. With this sort of approach, businesses will simply handle the speed of change that comes with the IoT and very much notice its advantages.

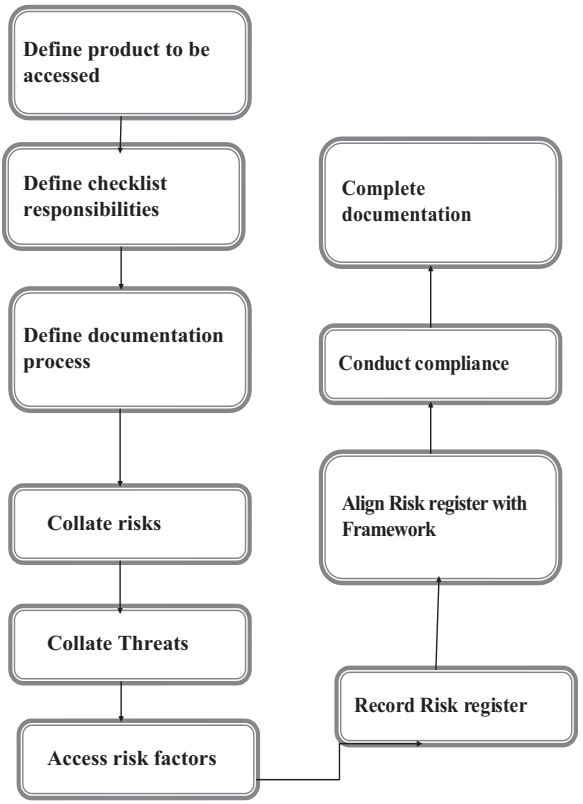
2.6 SECURITY THREATS OF IOT

The Internet of Things (IoT) delivers substantial advantages to end-users. However, it also brings new security challenges. Part of the central security issue is that connected devices share implicit trust. This shared trust between connected devices means the devices automatically transmit their information to every alternative straight away upon recognition while not initially running any malware detection tests. The worst-case eventualities of those IoT security dangers lead to physical harm or maybe the loss of life.

Connected devices are creating pleasant experiences for consumers; however, they also represent current targets for hackers. The Internet of Things (IoT) and cyber-criminal activity share two vital traits: they are mostly invisible to the eye, and they surround us at any given moment.

As additional organizations use a combination of sensors and complicated software system applications to create smart homes, smart workplace environments, and even smart cities, the results typically feel magic. Lights turn on after you enter a room. A piece of machinery proactively requests an upgrade to stop breaking down. A retail store automatically restocks a shelf before customers become annoyed over missing things. These are all ways in which the IoT makes technology omnipresent and seamless. Unfortunately, the foremost prospering cybercriminals behave in an almost identical way. Hacking databases, attacking websites, and stealing passwords seldom involves a face-to-face encounter. Once technology becomes essential, the security problems associated with the technology tend to mount. Over time, these problems have transitioned from email to text messages, from desktop PCs to smartphone and currently to the IoT.

The Internet of Things (IoT) may be a quickly growing phase of the internet. Whereas different parts of the internet are dependent on individuals exchanging data, IoT allows devices to gather data, transmit data and receive data. It is easier to think about IoT as similar to online, email or social networks; however, rather than connecting individuals, it connects smart machines.



2.6.1 Vulnerability

The most basic and easy-to-pick threat to IoT devices is their vulnerability. Corporations providing IoT solutions begin with addressing this issue initially before looking at the underlying software system. We are also compelled to perceive that vulnerability is often of two types: hardware and software. Hardware vulnerability is commonly hard to discover or penetrate. However, it is even harder to repair or overhaul the injury. Software vulnerability points toward a poorly written algorithmic program or a line of code with a backdoor. This backdoor will simply give access to intruders prying for such opportunities.

2.6.2 Easy Exposure

This can be one of the most basic problems faced by the IoT business. Any device, if unattended or exposed to troublemakers, is an open invitation to discomfort. In most cases, IoT devices are not flexible to third-party exposure; they either expose or are simply accessible to anyone.

This means that an attacker will either simply steal the device, connect the device to a different device containing harmful information, or attempt to extract cryptological secrets, modifying the programming or perhaps substituting those devices with malicious ones over which the intruder has complete management.

2.6.3 Threats

Threats are often of two types: an individual's threat or a natural threat. Any threat arising from natural occurrences like earthquakes, hurricanes, floods, or fires will cause severe injury to IoT devices. We regularly take a backup or produce contingency plans to safeguard information. However, any injury caused to the devices physically cannot be repaired.

Nowadays, IoT solutions have matured over time. Devices, today, have evolved to be waterproof. It will be a long journey before IoT solution suppliers come up with something that is fireproof or earthquake-proof. On the contrary, we tend to do everything in our power to curb any human threats to IoT devices. These threats are typically malicious attacks.

2.6.4 Insecure Web Interface

The security issues relating to the Internet of Things are that the built-in IoT allows the end-user to interface with devices while at the same an attacker or intruder may also gain an unauthorized access to these devices.

Some of the security issues are listed below.

- Account enumeration
- Weak default credentials
- Credentials exposed in network traffic
- Cross-site scripting (XSS)
- SQL-injection
- Session management
- Weak account lockout settings.

The solution to the above problems is

- Default passwords and default usernames must be changed during initial setup.
- Ensuring password-recovery mechanisms are robust and do not supply an attacker with information indicating a valid account.
- Ensure that web interface is not susceptible to XSS, SQLi or CSRF.
- Ensure that credentials are not exposed in internal or external network traffic.
- Weak passwords should not be allowed.
- Account lockout after 3–5 failed login attempts.

2.6.5 Insufficient Authentications

This area deals with mechanisms insufficient to authenticate IoT devices. These give rise to such issues as

- Lack of password complexity.
- Poorly protected credentials.
- Lack of two-factor authentication.
- Insecure password recovery.
- Privilege escalation.
- Lack of role-based access control.

The solution to the above problems is

- Ensure that strong passwords are required.
- Ensuring granular access control is in place when necessary.
- Ensuring credentials are properly protected.
- Implement two-factor authentications where possible.
- Ensuring those password-recovery mechanisms are secure.
- Ensuring re-authentication is required for sensitive features.
- Ensuring options are available for configuring password controls.

2.6.6 Insecure Network Devices

Here are some of the problems related to the insecure network devices with IoT:

- Vulnerable services
- Buffer overflow
- Open ports via UPnP
- Exploitable UDP services
- Denial-of-service
- DoS via network device fuzzing.

The solution to the above problems is

- Ensuring only necessary ports are exposed and available. Ensuring services are not vulnerable to buffer overflow and fuzzing attacks.
- Ensuring services are not vulnerable to DoS attacks which can affect the device itself or other devices and/or users on the local network or other networks.
- Ensuring network ports or services are not exposed to the internet via UPnP for example.

2.6.7 Lack of Transport Encryption

This area deals with the data or information being exchanged in an unencrypted format.

- Unencrypted services via the internet.
- Unencrypted services via the local network.
- Poorly implemented SSL/TLS.
- Misconfigured SSL/TLS.

The solution to the above problems is

- Ensuring data is encrypted using protocols such as SSL and TLS while transiting networks.
- Ensuring other industry-standard encryption techniques are utilized to protect data during transport if SSL or TLS are not available.
- Ensuring only accepted encryption standards are used and avoid using proprietary encryption protocols.

2.6.8 Privacy Concerns

Collection of unnecessary personal information is the main concern of patients. The information of patients should be legal and it should not be accessed by any third party.

Some points should be kept in mind while dealing with privacy threats. They are listed below:

- Ensuring only data critical to the functionality of the device is collected.
- Ensuring that any data collected is of a less sensitive nature.
- Ensuring that any data collected is de-identified or anonymized.
- Ensuring any data collected is properly protected with encryption.
- Ensuring the device and all of its components properly protect personal information.
- Ensuring only authorized individuals have access to collected personal information.
- Ensuring that retention limits are set for collected data.
- Ensuring that end-users are provided with "Notice and Choice" if data collected is more than what would be expected from the product.

2.6.9 Insecure Cloud Interface

This point concerns security issues related to the cloud interface used to interact with the IoT devices.

- Account enumeration.
- No account lockout.
- Credentials exposed in network traffic.

The solution to the above problem is

- Default passwords, default usernames to be changed during initial setup.
- Ensuring user accounts cannot be enumerated using functionality such as password reset mechanisms.
- Ensuring account lockout after 3–5 failed login attempts.
- Ensuring the cloud-based web interface is not susceptible to XSS, SQLi or CSRF.

FIGURE 2.4 Demonstration of Web security.

- Ensuring credentials are not exposed over the internet.
- Implement two-factor authentications if possible.

2.7 CONCLUSIONS

This chapter discussed the various types of application of the Internet of Things (IoT) in the healthcare industry. We have focused on the various types of application of IoT in the healthcare industry; the major security issues and the challenges present in the way of successful implementation of IoT in the industry. IoT is often blamed for delusions of grandeur and therefore the conviction that it is a big deal. The fact is that it is a giant deal and destined to grow larger. IoT is certainly a giant deal and it is only planning to get larger with the passage of time. Sadly, the larger it gets the greater a target is on its back. Likewise, all the related threats and IoT trends can get larger. Manufacturers and others linked with the IoT trade may have to be compelled to get serious regarding protection problems and threats.

REFERENCES

1. Alok Kulkarni, Sampada Sathe. "Healthcare applications of the Internet of Things: A Review". *(IJCSIT) International Journal of Computer Science and Information Technologies*, 5 (5), 2014, 6229–6232.
2. B. Sobhan Babu, K. Srikanth, T. Ramanjaneyulu, I. Lakshmi Narayana. "IoT for Healthcare" *International Journal of Science and Research (IJSR)* 2014.
3. Shubham Banka, Isha Madan, S.S. Saranya. "Smart Healthcare Monitoring using IoT. *International Journal of Applied Engineering Research ISSN 0973-4562*, 13 (15), 2018, 11984–11989.

4. Ananda Mohon Ghosh, Debashish Halder, SK Alamgir Hossain "Remote Health Monitoring System through IoT" 5th International Conference on Informatics, Electronics and Vision (ICIEV)
5. Damian Dziak,*, Bartosz Jachimczyk, Wlodek J. Kulesza "IoT-Based Information System for Healthcare Application` Design Methodology Approach" *Appl. Sci*. 2017, 7, 596; doi:10.3390/app7060596 www.mdpi.com/journal/applsci
6. Harold Thimbleby. "Technology and the future of healthcare." [*Journal of Public Health Research*, 2013; 2:e28]
7. Burgos S. Medical information technologies can increase quality and reduce costs. *Clinics*, 2013, 68(3):425, http://dx.doi.org/10.6061/clinics/ 2013(03)LE04.**Jo**
8. https://dzone.com/articles/the-biggest-security-threats-and-challenges-for-io Health Research 2013; vo
9. www.iotforall.com/7-most-common-iot-security-threats-2019/28
10. www.ubuntupit.com/25-most-common-iot-security-threats-in-an-increasingly-connected-world/
11. www.sdxcentral.com/5g/iot/definitions/iot-security/