Internet of Things-Based e-Health Care: Key Challenges and Recommended Solutions for Future

Gadiparthy Harika Sai, Khushboo Tripathi, and Amit Kumar Tyagi

Abstract Internet of Things (IoT) has changed the way of living today. Today, Internet connected things (ICT) are increasing at a rapid rate and connecting with devices to reduce load from human being. Irrespective of the sector, the IoT devices are everywhere taking care of everything from the agriculture sector to the sector of manufacturing. But, due to the global COVID 19 pandemic, the sector of health care demands the major use of IoT today. Due to the prevailing pandemic, healthcare professionals also choose to treat the patients virtually rather than treating them physically. IoT plays a major role here. But, most of the application providers or service providers or any other system involving IoT devices for generating and storing data may become a way of leak of information or stolen by a third party for black mailing or financial gain thus leading to privacy and security leak of the user. This work includes all such views with various issues and recommended solutions for the same. Also, other security and privacy requirements and corresponding solutions are also included to provide future researchers a solid base and a clear depth in knowledge regarding the security and privacy issues and solutions required.

Keywords Smart health care · Challenges · Internet of Things (IoT)-cloud-based health care · Wearable devices · Medical Internet of Things (MIoT)

G. H. Sai · A. K. Tyagi (✉)
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India
e-mail: amitkrtyagi025@gmail.com

K. Tripathi
Department of Computer Science and Engineering, Amity University Haryana, Gurgaon, India

A. K. Tyagi
Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India

P. K. Singh et al. (eds.), *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security*, Lecture Notes in Networks and Systems 421,
https://doi.org/10.1007/978-981-19-1142-2_37

1 Internet of Things—Introduction

IoT has become the new environment of computation with all the software services, sensors, and equipment involved. The growth of IoT in near future seems to be very high. IoT can expand its services to almost every existing sector. Though the growth has been very useful to the people, the problems of privacy make it distant to many other people. For example, when a customer visits a store, his/her picture is captured and the face detection services identify the name and the corresponding RFID tags aid in locating. Not only the person is tracked with the help of these but also his location privacy is leaked. In spite of many existing privacy protecting strategies like anonymization, utility trade-offs, and also imposing legal restrictions on data extraction, privacy still stands to be on top of the challenges in IoT.

The two types of privacy protection strategies in IoT include: rule-based approaches and architectural-based approaches [1]. The models involving rule-based approach are mainly for those environments that are closed. These models mainly involve applying the rules over shared information and protecting the privacy. But, since the IoT is considered to be an open environment, these models are not suitable for IoT. Architectural-based approaches include anonymization, utility trade-off techniques, and proxy based approaches. However, the anonymization techniques are actually limited to only like information collection or attempt to steal the information from the collector. The main assumption here is that the information collector is a trusted party. These techniques involve in protecting the information like participation of the devices or the so called "things" in information collection, but they do not matter about the disclosure of the already collected information by the "things."

Discussing about the e-health care, health sector is one of the most prominent sectors. E-health care involves providing health services remotely through servers without actually doctor visiting the patient physically. A quick dive into the fundamental concepts in innovative e-health systems are as follows:

- Wearable Devices: Devices like fitness bands, blood pressure monitoring, heart rate monitoring devices, and pulse monitor are very helpful for patients in this e-health sector. IoT has also helped people like elders with a tracking device which they can wear, and their people can track them in case of any emergency. Also, with the help of these wearable devices, the doctors can keep a track of their patients and their records. They can reach them in case of any emergency or sudden medical attention. Additionally, the data that are produced by these IoT devices aid the doctors in maintaining records of their patients. Not only tracking of patients but also tracking of some sensor-enabled medical equipment like wheel chairs, oxygen pumps, and nebulizers is possible though IoT-based applications.
- Ambient Assisted Living (AAL): The placing of smart devices (or IoTs) for senior citizens in an environment would be more helpful in assisting them and caring for them (in case of any health emergency). These devices or applications can also be helpful in monitoring the patient's activity and some vivid parameters like blood pressure, oxygen level, and temperature, and in case of any emergency, the nearest hospital or a clinic is given the alert.

- Internet of Health Things (IoHT): Smart devices that are integrated with cloud computing, used in the health sector for analyzing the patient's data for providing better healthcare solutions to the patients, and monitor the patient in real time. The patient data that are collected can be analyzed and diagnosed immediately thus making the treatment to happen faster. Apart from these advantages of IoHT, the main disadvantage is that the data are still prone to privacy and security attacks [2].

Organization of the work: This paper proposes complete information about Medical Internet of Things**.** The rest of the paper is structured as follows. Further, Sect. 2 presents security and privacy requirements toward IoT. Section 3 discusses existing solutions in the field of MIoT. Section 4 discusses Internet of Things healthcare security. Then, Sect. 5 presents the Internet of Things-based healthcare technologies. Section 6 presents the future challenges involved. Finally, the work is concluded in Sect. 7 with explanation of future work in Sect. 8.

2 Security and Privacy Requirement Toward Internet of Things-Based Applications

In the smart era that is prevailing today, IoT has a lot of applications in many sectors like agriculture, medical, manufacturing, and logistics. The IoT devices that are involved here deal with a lot of data belonging to a user. The devices may share the sensitive information related to user to any service provider or a perpetuator leading to privacy and security threats [3]. In this section, several security and privacy requirements are discussed regarding the IoT-based smart healthcare applications.

2.1 Security Requirements for IoT-Based Health Care/Medical Internet of Things (MIoT)

Security and privacy play a major role in MIoT. MIoT devices produce, transmit, and store a lot of data related to user which is highly confidential and sensitive as well. Any security attack on the network of the medical system can lead to very harmful consequences. Also, the patient's private information is present everywhere, i.e., in all the levels of data collection, transmission, and storage. The following four requirements should be considered in developing the required privacy and security models for MIoT:

- Data Integrity: Data integrity refers to the accuracy, reliability, and trustworthiness of a particular data throughout its lifecycle. Data integrity can be referred in terms of both state and a process. In terms of a state, data integrity defines a dataset which is valid and also accurate. In terms of a process, data integrity refers to

measures that are used to secure the validity or correctness of the data that is being worked upon. Data integrity is mainly of four types:

i. Domain Integrity: Domain integrity refers to a specific range of values that are going to be accepted and stored in a specific column within the database being worked on.
ii. Entity Integrity: Entity integrity involves the way that makes sure that every row in the table of the database has a unique and a non-null primary key value.
iii. Referential Integrity: Referential integrity is concerned about the relationship between tables in the database.
iv. User-defined Integrity: It involves the rules that are created by the user to fit her/his needed requirements.

- Data Usability: Data usability ensures that authorized users or systems can make use of the data or the data systems involved. Any access of data by an unauthorized users or system can further lead to the destruction of data usability.
- Data Auditing: Data auditing plays a major role in the security of Medical Internet of Things. Audit of the medical data regularly in an efficient way is a coherent means to check on the use of resources and also track any abnormal or mysterious events that are occurring or about to occur. Adding to this, the cloud service providers turn out to be untrusted after a period of time, and this will definitely require refined auditing methods to take care of.
- Patient Information Privacy: The information related to the patient can actually be categorized into two: general and the sensitive information. General data include the basic details of the patients such as their name, age, and address, whereas the sensitive information may include the details of fertility status, sexual functioning, genetic information, drug addiction, and other personal details of the patient. So, it is very clear that this sensitive information has to be kept private and should never be leaked to unauthorized systems or users which may result in a huge loss to the patient [4].

2.2 Security Requirements for IoT-Cloud-Based e-Health Systems

Internet of Things and cloud computing are two different technologies but are mutually related to each other in several applications [5]. The connection of the IoT devices among themselves leads to generation of a huge amount of big data, and this data are stored on the cloud for further requirements. These cloud-based services are being provided by many companies like Amazon, Google, and IBM. It is problem-free when the company follows all the security and privacy standards. But, on the other side, there are chances of information leaking, security breaches when the security standards are not met. So, defining the security requirements for IoT-cloud-based

e-Health systems is a must. A summary on security requirements for the same is as follows:

- Data gathering, processing, and usage have to be done only in accordance with the law and not by any illegal means.
- Minimum security and privacy protection for the data are a must.
- All the IoT devices that are connected to a particular network should be able to transmit the data and receive the same without destroying the data accuracy and integrity.
- All the protocols involving the collection of data, transmission, and usage must be defined clearly according to the prevailing standards. This will actually improve the trust of the patients/users toward the system.

Key elements that have to be kept in mind while securing the IoT-cloud-based e-health systems are as follows:

i. Confidentiality: Confidentiality is a way of ensuring that any kind of data or other exchanges between the sender and receiver are protected against any kind of malicious or suspicious usage. Confidentiality should be guaranteed at different levels of the communication network, i.e., the data have to confidential when it is being exchanged between any two IoT devices in the network, IoT device, and cloud computing to e-health systems or even between the system and the end user.
ii. Data Integrity: Data integrity refers to the trustworthiness, accuracy of the data throughout its lifecycle. In this particular IoT-cloud-based e-health system, data integrity check can be done at each node involving transmission of data between a sender and a receiver.
iii. Availability: It ensures that the data are available to the authorized users but not to any other suspicious or unauthorized users at any stage of the data lifecycle, i.e., generation, processing, transmission.
iv. Access Control: This refers to the controlling of access and authorization to protected data by actually evaluating or enforcing the access required.
v. Anonymization: The use of anonymous access helps in protecting the user's security and privacy without letting the details passed on to the perpetrators.
vi. Authentication: The very important security element in any system. Verification and validation of users details before letting them access the data or the system help in majorly reducing the identity thefts or data breaches.
vii. Resistance Attraction: Resistance attraction ensures that any attacks from unauthorized users or systems are prevented or avoided.

2.3 Privacy Requirements for IoT-Cloud-Based e-Health Systems

Privacy of the patient's information has to be maintained throughout its life cycle. The internal privacy policies judge who can access, use, or view the sensitive and

confidential data belonging to the patient. The most important is the protection of patient's sensitive data from leakage or unauthorized access or use. There are several methods that can safeguard the data like cloud computing, anonymization of data, and tracking the data exchange. These methods can be useful to some extent to identify or track the suspicious or malicious actions happening. There are a plethora of privacy protection measures coming up these days, but these have to be tailored separately to every need of privacy protection for better results [6]. For example, the e-health system offers several applications like patient tracking, remote monitoring, and artificial intelligence-based diagnosis. All of these services should be provided with respective potential privacy protection measures. The users have become more cautious about their data on any kind of system, especially when it comes to their medical data since this carries a lot of sensitive information about the users. If there is privacy leak from the system, this makes the system less trustworthy to the users. Strengthening of the privacy of IoT-cloud-based e-health system can be done by including privacy by design (PbD) [7] along with the following measures:

- Location Privacy: Applications involving big data networks make it mandatory to seek location information for the data being used. To prevent the loss or leakage of the location information, related effective privacy measures and strategies are used [8–11].
- Data Lifecycle Protection: This ensures that the necessary security measures needed for privacy are taken in all the different stages of the data life cycle right from retaining the data security till it is destroyed safely after the processing and usage.
- Default Privacy: Privacy as a default setting means that the privacy of a user is preserved in all situations even without his/her intervention [12]. This means that no action or work is needed from the user's end to protect his/her privacy since the privacy comes built in with the system, whereas the traditional systems require the user to take the basic steps toward privacy protection.
- Embedded Privacy: Embedding privacy into the design of the system or the architecture of the IoT systems makes it a core function of the system.
- Robustness: This ensures that all the security requirements are met at all stages of the data lifecycle in order to protect the privacy for the IT systems.
- Visibility and Transparency: Privacy just does not mean protecting the data but also maintain the trust of the users. This is where the factors visibility and transparency come into play. The operations that are being performed on the data should remain visible to the users. These factors make sure that the actions including collection, analyzing, processing, and transmission of personal data are maintained a record of and available to the users for their purposes of accountability.

Both the security and privacy measures should accord with the international standards of risk management techniques and methods in order to provide a hassle-free environment and get adopted. Data privacy is also a fundamental strategy that is concerned about protecting user data. One of the major requirements in this context is the data protection through design known as privacy by design (PbD) which is playing

a key role in securing and safeguarding privacy in many of the major technological systems.

2.4 System Requirements of IoT-Cloud-Based e-Health Systems

Other system requirements concerning with the IoT-cloud-based e-health systems are as follows:

- Secure Protocols: These protocols aid in establishing secure and safe computer network connections and improve the security of the entire network. The application of such secure protocols not only ensures the security of the network but also enhance the security of information.
- Secure communication: This is guaranteed by specific cryptosystems and also aids in making sure of the confidentiality of the data. A secure communication is meant to protect the data transmissions from any kind of malicious exploitation by the perpetrators.
- Secure Transmission: This ensures that the data transmission is happening without any malicious or suspicious users causing harm to the system both internally and externally. The security of the data transmitted can be achieved through necessary cryptographic mechanisms.
- Data Encryption: This ensures that the data are protected throughout its lifecycle by encoding the entire data that are being worked with. This also aids in avoiding security breaches of the raw data available through encoding.

3 Existing Solutions for Internet of Things-Based Health Care/Medical Internet of Things (MIoT)

We have discussed several security and privacy requirements of IoT-cloud-based e-health systems and IoT-based health care as well. In both the healthcare systems, there is a chance of privacy leakage or security breaches possible. Also, there are chances for stealing of information from the system by perpetrators. Let's take a quick dive into some of the existing solutions for the above mentioned issues:

i. Data Anonymization: Data anonymization [13] refers to the process of protecting sensitive information by either erasing or encrypting the identifiers that play a role of connectors between the individual and the data. A few data anonymization techniques that are used are [14]:

   - Data masking: Masking the data with altered values.
   - Pseudonymization: Replacing the identifiers that are private with fake identifiers.

- Generalization: Removing some of the data intentionally in order to make it less identifiable.
- Data Swapping: Rearranging the attribute values of the dataset or the database so that they do not exactly correlate with the original records.

ii. Data Encryption: Cryptography is the main and basic technology that is being used in the data encryption process where the data are encoded and then used in its life cycle of processing, analysis, transmission, etc.

iii. Access Control: Access control is a technique that is used to regulate who can access the data in a particular computing environment or the system. This is a fundamental yet efficient security concept that aids in minimizing the risk to the related business or the organization. The two major types of access control are as follows:

- Physical access control: This ensures the access control to campuses, rooms, buildings, or any physical assets or devices.
- Logical access control: This ensures the access control over the computer network, files, systems, and data.

iv. Trusted Third-party Auditing: The cloud servers that are being used cannot be fully trusted. There may be a possibility of loss of data integrity and consistency in case of any data corruption or any deletion without the notice of users. Here, the trusted third party comes into play. This trusted third party [15] with a good reputation provides proper and accurate auditing results which results in accountability of the cloud service providers.

v. Data Search: In terms of protection of data privacy over the system or cloud, data should be initially encrypted. This overcomes the existing traditional plaintext keyword searches. So, enabling an accurate encrypted cloud data search will be of a great importance toward the protection of privacy.

vii. Blockchain: Blockchain is a system in which a record of actions is actually maintained across several linked computers in a network. Use of blockchain technology in the IoT-based healthcare systems aids in increasing the transparency between the doctors and patients, also ensures efficient collaboration between different health organizations and also smart contracts. Also, this helps in resisting failure and data fragmentation. But, at the same time, blockchain technologies are prone to attacks because of their transparency.

Few interesting enhancement and solutions toward IoT-based health care have been discussed in [16, 17].

Security of Electronic Healthcare Records (HERs) Systems

Electronic healthcare records (EHRs) consist of mainly the medical history of the patient, his/her statistical laboratory test results, etc. Security and privacy of these data have to be ensured properly and is crucial to save these from any kind of malicious security or privacy attacks. Adding to these, there are a number of challenges in building and deploying the healthcare systems. Because such models are vulnerable to several kinds of cyber- attacks and the users are much concerned about these cyber-

attacks and required efficient and effective solutions for such cyber-attacks. Similarly, the EHRs are prone to several kinds of security attacks [18]. Therefore, the following requirements are to be met based on the relevant standards when implementing the secure electronic healthcare records in the future:

- Accuracy and data integrity
- Privacy and security of the data dealing with
- An efficient data sharing mechanism
- Accurate and proper auditing and accountability of data
- Ability that the patients can control their own EHRs, i.e., monitoring them, checking records frequently, etc.

Hence, security of EHR records can be found in detail in [16].

4 Internet of Things Healthcare Security

With the rapid development of the IoT and its applications over the recent years, the healthcare sector is also expected to witness the applications of IoT majorly in the coming future. All the devices involved in the healthcare or the medical sector are also expected to deal with the integration of IoT. Though this leads to many kind of applications and makes it easier for both doctors and patients in the sector, it has its drawbacks of security and privacy challenges as discussed earlier in the paper. To completely facilitate the adoption of IoT into health sector, it is also important to know about the threat models, attack taxonomy, and possible countermeasures related which are discussed further below:

Threat Model
Both the IoT health devices and the network being used by them is prone to different kinds of security attacks. One case can be the expansion of the current network, cloud networks, and services. Second case could be the increase in the communication between the IoT devices over the network, cloud services, and applications. Another scenario would be in the in-device hardware and software limitations. Threats can be raised from both within the network or outside the network. If an attack or a threat arises from a health device in a proximal network, then the risk related would be more severe. Also, determining the malicious or suspicious device causing this would be very difficult within a proximal network.

An Attack Taxonomy
With the increasing advancements in the technology field, not only they are becoming advantageous to people but also to the perpetrators increasing their ability to introduce several types of security attacks and threats into the networks [19] or the system devices. Some of the threats are predictable and tangible, whereas it is even harder to predict many of the other threats. The major types include: attacks based on network properties, attacks based on host properties, and attacks based on information

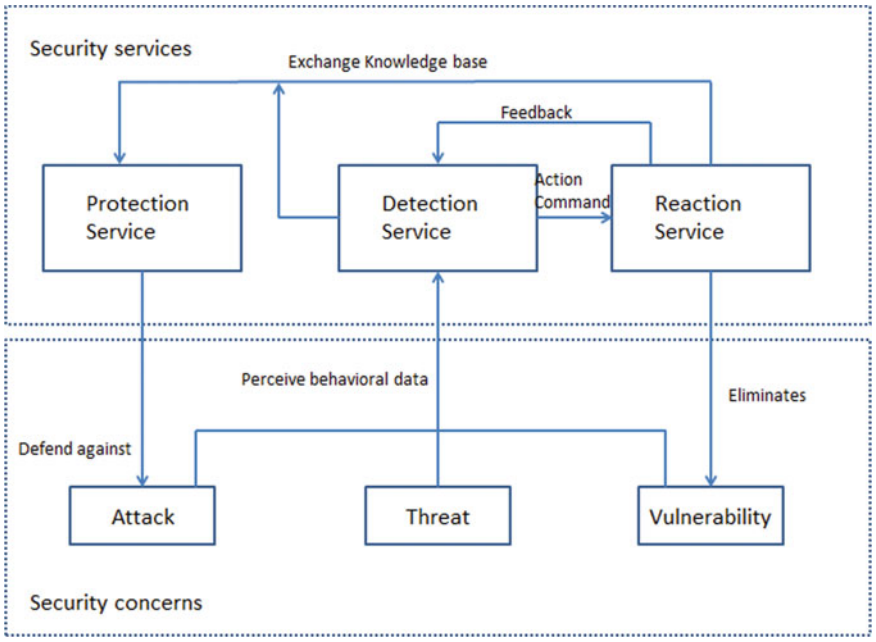

Fig. 1 Collaborative scheme for providing security services

disruptions. A security model for IoT-based health care is discussed in Fig. 1, or Fig. 1 represents a security collaboration scheme for the following security services [20]:

- Protection services: designed to reduce attacks.
- Detection services: These services will be receiving data from the applications involving health care periodically and analyze the captured data, detecting if there is any anomaly being involved.
- Reaction services: This specific type of services help the health entities in surviving all the attacks with the help of defense mechanisms.

5 Internet of Things-Based Healthcare Technologies

There are actually many prevailing technologies strengthening the Internet of Things-based health care. So, preparing an explicit list on this is definitely a tougher job. So, a brief idea on the core technologies available is given below:

i. Cloud Computing: Integration of IoT-based health care with cloud computing has enormous advantages. Some of them include access to shared resources, ability to increase the storage capacity for the data being worked with, and another important added advantage would be providing services upon

request over the network. All these advantages together make it easier for the operations to get executed and thus also resulting in good efficiency.

ii. Big Data: Big data aid in accommodating huge amounts of data be it generated by the medical sensors or the IoT devices involved in the IoT-based health care or also the data that are being transmitted over the network among the IoT devices. In addition to these advantages, big data also provide a number of tools to actually improve the necessary health diagnosis in terms of efficiency.

iii. Grid Computing: In general terms, grid computing involves working of a network of computers under a single working protocol acting almost like a super virtual computer to perform a specified task which may be difficult for a single machine or computer to execute or achieve [21]. With this particular application of grid computing, it can be used in the field of IoT-based health care addressing the insufficient computational capability of the medical sensors or the devices that are aiding in the system. Grid computing can also be viewed as a backbone for the cloud computing.

iv. Augmented Reality: Augmented reality (AR) which is a part of IoT can play a major role in the IoT-based health care. Since the IoT-based healthcare systems mostly involve remote monitoring and diagnosing, AR comes into play here thus aiding the doctors and the system in performing remote monitoring and the needful.

v. Wearables: Wearables also play a major role in the IoT-based healthcare systems. The main advantages of these would actually be patient engagement, ability to track the patients in case of any emergency. This is also a way helpful to the senior citizens who can be tracked in case of any medical emergency, and the needful treatment can be provided, or a nearby hospital or clinic can be informed of this situation.

vi. Networks: Networks are the basic necessity of any IoT-based healthcare system. All sorts of networks ranging from short-range communications to long-range communication networks aid in the system being a part of the infrastructure of the IoT-based healthcare network. All the data transmissions or any tracking information could be shared only through these connected networks. In addition to these, the introduction of ultra-wide bands or RFID tags into the network can actually help in designing the low-power-based medical sensors and also aid in communication protocols.

vii. Ambient Intelligence: Ambient intelligence basically involves the electronic environments that are able to respond to the presence of people and are sensitive as well [22]. Since the end users of the IoT-based healthcare systems are actually humans, ambient intelligence can play an effective role over here.

6 Future Challenges Involved Internet of Things-Based Health Care

Anyone involving in the development of the security and privacy of the Medical Internet of Things (MIoT) should take the following into account:

i. Network Insecurity: Keeping in mind of various parameters like the low cost or convenience, many devices and services depend on the wireless networks like Wi-Fi which are actually prone to any unauthorized access or several intrusions taking place. They may also be vulnerable to security attacks like man-in-the-middle attack and denial of Service arracks easily. Adding to these, the free wireless networks available publicly mostly do not adhere to the standards of security and thus resulting in more chances of any kind of security attacks
ii. Lightweight protocols: Any low-cost devices or any kind of software applications should follow specific set of policies and rules in order to provide their services. Failing to do so would result in a huge loss causing security attacks over the network. In present days, the security and the cost are directly proportional, i.e., if we want to provide a high-level security for a network or a device, then the cost requirements would also be extremely high. This is not always possible in MIoT. So, developing lightweight protocols [23] for security at different levels is one good option in the future.
iii. Data Sharing: Though there is a day-to-day development in the fields of medical information technology, the problems of security and privacy are still being revolved around. The issue of information leakage seems to be in an active state even now. The information would have to be shared between different systems of MIoT in the future. Since the data are collected from different sources, it is not really possible to completely unify the data management. Any kind of disclosure or unauthorized sharing of the patient data would cause a serious loss to the patient and remains as a security issue in MIoT system.

7 Conclusion

With the recent advancements in technology and introduction of several medical devices and related software applications, large amounts of data are being generated and stored. In present days, the importance of data is on the high. With huge amounts of data over the networks, the problems of security and privacy attacks are also on rise. The ways of protecting data security and privacy at all the different stages of the data lifecycle would be of a great importance in the future research. Starting off with the IoT security and privacy requirements of the IoT-based health care and IoT-cloud-based e-health systems, this paper discusses many requirements including the security requirements, privacy requirements, system requirements, and the problems being faced and the possible solutions for the same. Medical Internet

of Things (MIoT) is given a good importance in the paper. The recent advancements and innovations being made in the field of IoT have changed the lives and networks a lot connecting a plethora of devices. The IoT-based healthcare systems, IoT-cloud-based e-health systems, Medical Internet of things (MIoT) all come under the applications of the same providing remote medical facilities from anywhere in the world thus reducing the cost and getting better patient outcomes when compared to the traditional modes. However, security and privacy of these systems are still vulnerable. So, the researchers should focus on these aspects and provide possible other different solutions to these issues in the future.

8 Future Work

Due to the prevailing pandemic everywhere in the world, many sectors are not able to provide services to the people properly. Healthcare sector also comes into this list. Afraid of the conditions outside and the increase in number of Covid-19 cases everywhere, people are not willing to go to the hospitals or clinics especially. So, this is resulting in a lot of unaddressed medical cases everywhere, especially in rural areas where the lack of basic transportation facilities is adding up to this. In such situations, IoT-based healthcare systems can play a major role. Bringing the IoT-based healthcare systems to rural areas can majorly aid in addressing the medical cases of the people over there remotely without actually needing them to visit the hospital or clinic physically unless it is a serious medical issue that cannot be addressed remotely. Also, the applications of this IoT-based healthcare system like the wearables can make it easier for the doctors to track their patients' status and records easily in a remote manner.

References

1. Samani, A., Ghenniwa, H. H., & Wahaishi, A. (2015). Privacy in internet of things: A model and protection framework. *Procedia Computer Science, 52*, 606–613. https://doi.org/10.1016/j.procs.2015.05.046
2. Fernandez, F., & Pallis, G. C. (2014). Opportunities and challenges of the internet of things for healthcare: Systems engineering perspective. In *2014 4th International Conference on Wireless Mobile Communication and Healthcare—Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)* (pp. 263–266). https://doi.org/10.1109/MOBIHEALTH.2014.7015961
3. Oh, S., & Kim, Y. (2017). Security requirements analysis for the IoT. In *2017 International Conference on Platform Technology and Service (PlatCon)* (pp. 1–6). https://doi.org/10.1109/PlatCon.2017.7883727
4. Hodge, Jr., J. G., Gostin, L. O., & Jacobson, P. D. (1999). Legal issues concerning electronic health information: Privacy, quality, and liability. *JAMA, 282,* (15), 1466–1471.
5. Malik, A., & Om, H. (2018). Cloud computing and internet of things integration: Architecture, applications, issues, and challenges. In *Sustainable cloud and energy services* (pp. 1–24). Springer.

6. Sahmim, S., & Gharsellaoui, H. (2017). Privacy and security in internet-based computing: Cloud computing, internet of things, cloud of things: A review. *Procedia Computer Science, 112*, 1516–1522.
7. Cavoukian, A. (2009). *Privacy by design.*
8. Wang, L., & Meng, X.-F. (2014). Location privacy preservation in big data era: A survey. *Journal of Software, 25*(4), 693–712.
9. Nair, M. M., & Tyagi, A. K. (2021). Privacy: History, statistics, policy, laws, preservation and threat analysis. *Journal of Information Assurance and Security, 16* (1), 24–34, 11p.
10. Tyagi, A. K., & Shamila, M. (2019). Spy in the crowd: How user's privacy is getting affected with the integration of internet of thing's devices (March 20, 2019). In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM).* Amity University Rajasthan, February 26–28, 2019.
11. Tyagi, A. K., Rekha, G., & Sreenath, N. (2020) Beyond the hype: Internet of things concepts, security and privacy concerns. In Satapathy, S., Raju, K., Shyamala, K., Krishna, D., & M. Favorskaya (Eds.), *Advances in decision sciences, image processing, security and computer vision. ICETE 2019. Learning and analytics in intelligent systems* (Vol. 3). Springer. https://doi.org/10.1007/978-3-030-24322-7_50
12. Willis, L. E. (2014). Why not privacy by default. *Berkeley Technology Law Journal, 29*, 61.
13. Bayardo, R. J., & Agrawal, R. (2005). Data privacy through optimal *k*-anonymization. In *21st International Conference on Data Engineering (ICDE'05).* IEEE.
14. https://www.imperva.com/learn/data-security/anonymization/
15. Nigel, J., Mitchell, C., & Walker, M. (1995). A proposed architecture for trusted third party services. In *International conference on cryptography: Policy and algorithms.* Springer.
16. Tyagi, A. K., Gupta, M., Aswathy, S. U., & Ved, C. (2021). Healthcare solutions for smart era: An useful explanation from user's perspective. In *Recent trends in blockchain for information systems security and privacy.* CRC Press.
17. Nair, M. M., Tyagi, A. K., & Sreenath, N. (2021). The future with industry 4.0 at the core of society 5.0: Open issues, future opportunities and challenges. In *2021 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–7). https://doi.org/10.1109/ICCCI50826.2021.9402498
18. Fernández-Alemán, J. L., et al. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46* (3), 541–562.
19. Mayzaud, A., Badonnel, R., & Chrisment, I. (2016). A Taxonomy of attacks in RPL-based internet of things. *International Journal of Network Security, 18*(3), 459–473.
20. Singh, S., Ra, I.-H., Meng, W., Kaur, M., & Cho, G. H. (2019). SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *International Journal of Distributed Sensor Networks.*
21. Joseph, J. (2004). *Grid computing.* Pearson Education India.
22. Aarts, E., & Wichert, R. (2009). Ambient intelligence. In *Technology guide* (pp. 244–249). Springer.
23. Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. *IEEE Internet of Things Journal, 8* (6), 4132–4156.