International Journal of Electronic Devices and Networking

E-ISSN: 2708-4485
P-ISSN: 2708-4477
IJEDN 2022; 3(2): 43-50

www.electronicnetjournal.com
Received: 07-05-2022
Accepted: 08-06-2022

Arnav Rawat
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Correspondence
Arnav Rawat
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Internet of things in healthcare: Application and challenges

Arnav Rawat

Abstract
The research topic gives an overview of the use of Iot in healthcare, it's working, applications and the challenges it faces regarding those. Iot helps in connecting devices used all around for different purposes which make use of sensors, software etc, and connects them together over the internet or some other network. It's a giant network which helps in sharing data and more between different types of devices. It provides with a platform where data from all devices are collected and is shared with other devices for better understanding of the needs and requirements of people and increasing the user experience overall. In Iot, the data is collected from different patients, their experience and reaction to different medicines, procedures and overall health care system, helps in making healthcare more effective by giving the researchers and doctors a better understanding of how to make procedures more effective and also understanding diseases better due to which the mistakes made in diagnosis would be reduced by a huge number. When devices involved in healthcare are connected to each other through IoT it also becomes easier for health care workers to get a hold on the patient health stats at all times making their care more effective, and also increasing the number of patients a single healthcare worker can handle. The paper thus focuses on the applications of IoT including the quality of data, security of patient information with IoT, Patient behaviour analysis, and the challenges associated with these. The question we focus to answer through the paper is "Is IoT a friend of boon to the healthcare system and how it's future looks".

Keywords: Internet of things, healthcare, smart gadgets, smart era

1. Introduction
With IoT healthcare devices are connected to each other via embedded sensors and softwares and this enables healthcare workers to acquire analytical medical data for better processing and analysis. With the help of existing internet infrastructure, the Iot devices can be connected to computer-based systems which allows the data to be collected in mass in one place and by using pre-existing resources the cost of implementation is also decreased making the mission of making healthcare smart an achievable target. When the devices are made smart, they collect data with the help of sensors and actuators and pre-existing technologies, the data collected can be shared among other devices connected tot the network. In the field of healthcare devices like pacemakers, infusion pumps and personal health devices like Fitbit watches or step counters can be connected through IOT.

1.1 Importance of IoT in healthcare
To implement a smart healthcare system various component, have to be incorporated within the cloud to connect them, the components include multiple hospitals, patients, doctors and research organizations. This is done with the help of technologies like 5g Internet, artificial intelligence, cloud computing, Iot, and biotechnology [11]. Patients use devices which collect data through wearable gadgets which are connected to the cloud through which doctors are connected making a forum making virtual medicine possible.

1.2 Interoperability of data
When data is collected from such wide range of devices the type of data collected is heterogeneous [3] and to analyse it becomes a difficult thus through interoperability of high-quality data the data can be computed into an analysable format. This means the capability of various devices connected to the network to communicate and send and receive data amongst each other effectively so that the data can be used to reach a common goal. For this it's important that all the data collected from the devices connected on the cloud can be transited

effectively and is fathomable by the control system. It's one of the applications of Iot in healthcare to make the data collected from various platforms such that it can be used for detailed and full proof studies and research.

1.3 Patient behaviour Analysis

With the collected data patient behaviours and reaction to different forms of healthcare can be analysed making it possible for healthcare workers to improve techniques and also for organizations to implement methods for better patient satisfaction. Patient behaviour analysis can be either disease centred or patient centred, disease centred analysis focuses on collecting data from different patients for different diseases to account more knowledge of the disease as well as to be able to provide a more effective and wider Range of treatment options to choose from which suit the patient's profile the most, while on the other hand patient centred analysis focuses on patient satisfaction which allows the healthcare organizations to come up with better ways to execute processes to guarantee an easy and patient friendly experience.

1.4 Security and Patient privacy

With IoT and all devices connected to the cloud, security becomes a concern. Medical information of people is private and can be used maliciously, also a system with compromised security can lead to improper transit of data which can be fatal. Thus, it becomes important to make sure that the systems are not easily hackable.

1.5 Opportunities and future

With the rising of IoT in the healthcare sector [1-2] emergency cases can be handles with much more accuracy and speed through real time healthcare monitoring. With this growth new opportunities come and problems like parallel processing flexibility, security problems, data service integration with scalable data storage, and parallel processing need to be addressed to provide for a truly effective and safe smart healthcare system.

2. Acquiring interoperability of data with IoT

The data processed by the devices has a huge amount of heterogeneity [3] which has to be made homogeneous to be able to process it. Thus, interoperability [5] is the only way to transit such huge amount of data to enable effective interaction between multiple systems. With heterogeneity the other problem faced is that the data derived from various sources is of different quality, and for efficient and reliable results it's important that the data we take into consideration is of high reliable quality, to achieve this we need a system to categorize the received heterogeneous data into different levels of quality which should be interoperable. to attain this goal, we have devised a stepwise procedure to quantify data. The steps include: 1) collection of data 2) cleaning the acquired data 3) estimation of the quality of data for segregation into different levels 4) Data interoperability

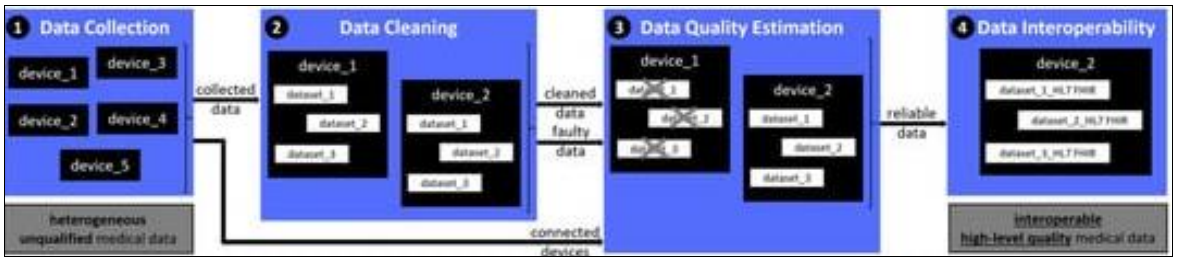

Fig 1: Architecture of the different stages

2.1 Stage 1: Collection of Data

To get data from various devices they first need to be connected with the establishment of proper technology, once this is established the devices are connected and the collection of data takes place. To connect the devices Bluetooth low energy [4] is used which is a specially designed wireless personal area network for healthcare, security etc. All the devices connected via this Bluetooth network must have open API (Application Programming Interface) so that they can give access to the details about their methods, and thus can communicate and transmit data amongst each other. After connection is made all the devices are mapped into different categories depending on the APIs (application programming interface). As the devices connected can be both personal use and professional used ones, it's important to also segregate the data depending on the source among the two, but it's not important to know the exact kind of device that is sending the data. The following process is showed in fig. 2.

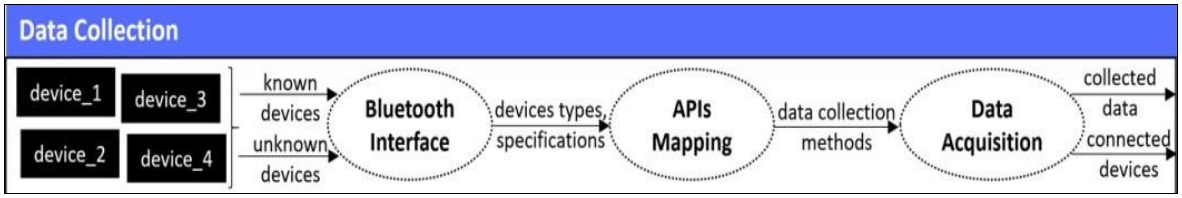

Fig 2: Collection of Data

2.2 Stage 2: Cleaning of acquired data

Once the data is collected and mapped the next stage is to clean the data and this process includes 3 steps 1) Validation of data 2) Elimination of Errors 3) Handling missing Data, this process is showcased in Fig. 3.

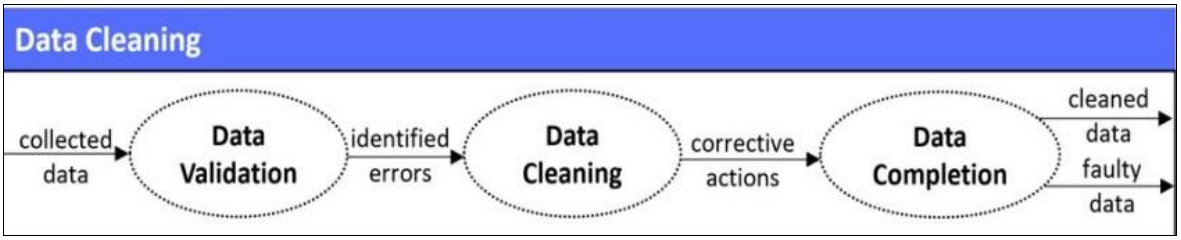

Fig 3: Cleaning of acquired data

In step one from all the segregated data errors are identified which break the constraints like datatype, value range etc set by the producers of the devices connected via Iot, this ensures that all the data is interoperable and abide by the rules of business. The second step methods are defined to take corrective measures to eliminate the errors identified in step 1. The final step makes sure that the data collected after removing errors is complete and in accordance to the constraints. The completion of missing data [12] follows some rules according to the variations in the values missing. When the variations are low and the data is frequent the missing value is set as the previous present non zero value, when the variation is in the medium range, the missing values are replaced by the moving average, which is the average calculated by dividing the data into subsets and computing a series of averages. Similarly, in the case of high variation and low frequent data, algorithms are engineered through the use of machine learning to compute the replacements for the missing values.

Once this is done, we can compute the accuracy of the cleaned data by the formula mentioned in equation (1)

Total_records = no. of records presend after collection of entries from all the connected devices in the dataset.

Total_actions = no of actions taking in cleaning the data (dropping records, replacing missing values)

$$\text{Accuracy} = \frac{\text{Total\_records} - \text{Total\_actions}}{\text{Total\_records}} \quad (1)$$

From the above equation (1) we can derive the expression for Faulty_data as equation (2)

$$\text{Faulty\_data} = 1 - \text{Accuracy} \quad (2)$$

Similarly, we can compute the completeness of the data, Data_completeness, where dropped = no. of datasets dropped

$$\text{Accuracy} = \frac{\text{Total\_records} - \text{dropped}}{\text{Total\_records}} \quad (3)$$

2.3 Stage 3: Estimation of Data Quality

Once the data is collected and cleaned, it's quality needs to be quantified so as to verify the accurateness and reliability of the data. This happens through a 3-step process, after which only data from fault free reliable sources is taken into consideration, the 3-step process is shown in Fig. 4.

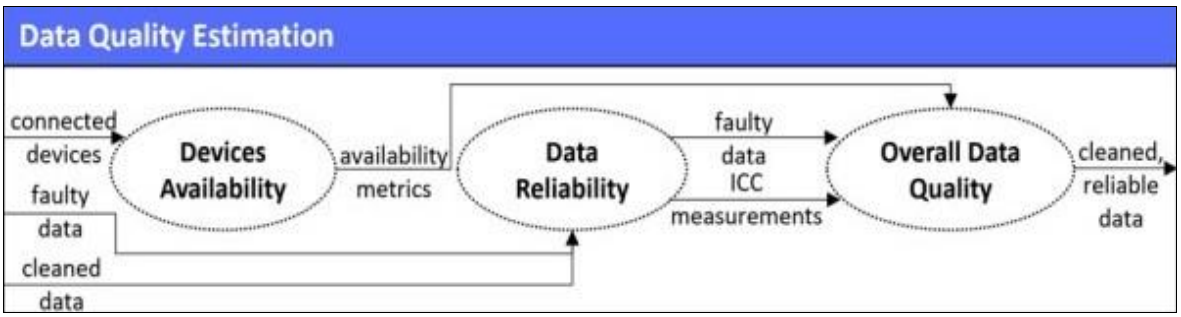

Fig 4: Estimation of Data quality

The quality of data received depends on the devices sending it, thus in the first step of estimating the quality of data we measure the quality of devices into levels. As quality is not a quantifiable aspect, methods are engineered to calculate and evaluate the quality of devices. The most common and widely used of those methods is estimating quality based on the ratio of time the device is operable, called operational availability, operational availability can be calculated through the equation (4) where cycle_time is the total time period of one operational cycle and uptime is the amount of time in one cycle that the device was actually working.

$$\text{Operational\_availability} = \frac{\text{uptime}}{\text{Cycle\_time}} \quad (4)$$

It's not enough to just consider device quality for the qualitative analysis of data, thus we also take in consideration the quality [20] of the data received from different sources in the 2nd step of the process. We take into measure the amount of faulty data in each dataset and methodize a way to relate it with the availability of devices to compute the reliability and quality. To increase the reliability, we also take into account the reliability metric of the datasets. With different time periods with data coming from different patients test-retest reliability is the most effective way to measure the quality of data. In short time periods results are taken on the same patient to attain reliability, for this the devices connected use SPSS library, which is used for calculating ICC (Intraclass Correlation Coefficient). In the final 3rd step of the process, we measure the estimated overall data quality. Here the ICC calculated by SPSS is correlated with the availability and measure of

faultiness to estimate the final quality of data. This computation will be considered reliable only if the set threshold is more than 90%. For calculating the final reliability, the formula in equation (5) is used, where0.7 and 0.3 are set weights that were derived experimentally.

$$Overall\_Quality = ((Availability - Faulty\ \_Data) * 0.7) + (ICC * 0.3)) \quad (5)$$

2.4 Stage 4: Data interoperability

After the data of high quality and reliability is filtered out in the first three steps it has to be interpreted and converted into a format that is widely understood by healthcare centres worldwide. As discussed before that for data to be able to give concrete results it needs to be in the same format. The format that is widely accepted is HL7 Fast Healthcare Interoperability (HL7 FHIR) [6]. In this stage the process methodized to convert the data into the following format has 4 steps as shown in the figure Fig. 5 the steps include 1) Ontology creation 2) Structural Mapping 3) Semantic Mapping and 4) Overall ontology mapping.

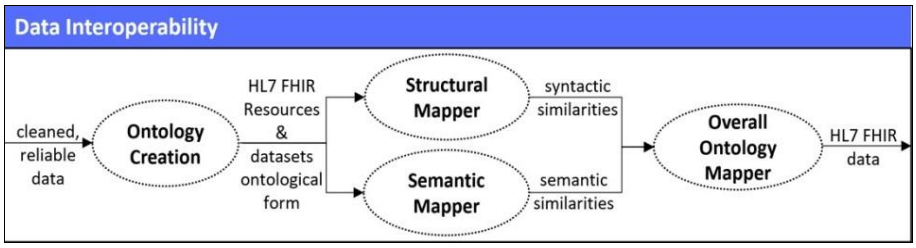

Fig 5: Data interoperability

3. Patient behaviour analysis

One of the most important applications of Iot in healthcare is to use the collected data for the purpose of studying patient behaviour [10] on the grounds of either medicine or administerial in order to improve in those sectors accordingly and provide with a more effective, reliable and patient friendly healthcare system. Fig. 6 shows the diagram depicting how the doctors use Iot to monitor multiple patients remotely, expanding their reachability and thus maximizing the utilization of time and resources and decreasing risks on patients.

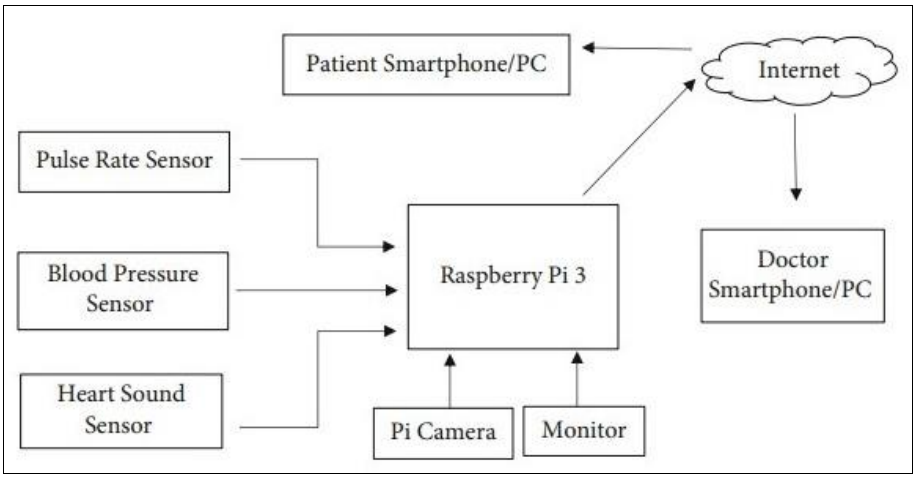

Fig 6: shows the diagram depicting how the doctors use Iot to monitor multiple patients remotely

3.1 Technology, Methods, and their Application

Healthcare running on Iot has IoT healthcare network (IoThNet) which has IoThNet platform, IoThNet architecture, and IoThNet topology. In massive research done on the following with the involvement of more than 300 leading healthcare workers, out of these participants 70% reported that more less than half of the patients were highly involved, while 42% documented that less than 25% showed extreme involvement. Smart healthcare devices can be used to keep records of patients stats like oxygen saturation percentage, heart rate, and body temperature [8]. For this SPO2, heartbeat and temperature sensors are used respectively, SPO2 sensors uses red and infrared sensors which use high quality led, and for the elimination of secondary frequencies calibrated receptors are used, while these sensors help recording the information it needs to be processed for which Arduino UNO is used. The data is firstly collected by the sensors and then with the help of raspberry pi it's processed to be sent to healthcare dives in a format which in interpretable by the people and healthcare workers. This system works well for recording real time information but the issue it faces is that the data collected could not be visualized, to be of better use it needed interfaces to be created for the same. Data visualization is an important aspect to make it comparable and beneficial while extracting out findings for research and development thus a system was engineered with plethysmography method to do the same. With this data could not only be processed but visualized in real time for monitoring, the accuracy and time taken by the devices to do this is safe to be used on patients and gives efficient results. Fig. 7 and Fig 8 show the accuracy of the devices.

Subjects	Actual data (bpm)	Observed data (bpm)	Error (%)
S1	65	67	1.47
S2	69	72	4.25
S3	75	76	4.03
S4	74	74	2.63
S5	72	71	1.32
S6	79	80	3.70

Fig 7: Monitoring of BP

Subjects	Actual data (F degree)	Observed data (F)	Error (%)
S1	96.3	98.7	0.50
S2	97.4	98.7	0.70
S3	98.2	97.6	0.50
S4	96.7	97.1	0.61
S5	97.4	97.0	0.40
S6	98.1	97.5	0.79

Fig 8: Monitoring body temperature

These devices can be used to monitor cardiac activity my monitoring the flow of blood in the finger with the help of a light and camera thus reducing the cost of importing devise to remote places and in homes for patients in need of regular check-ups by making them portable, also this helps doctors to monitor patients without being in their close premises by accessing the details gathered by the devices unto their phones for which they need a smartphone which can detect the devices and connect to them [9]. While being an amazing idea the first ever implementation of the idea wasn't as successful, while it successfully caught coronary tears, it failed to give records of heart rate and also besides tears it was not able to diagnose vascular diseases. Thus, showing we have the right ideas but needed more work on real life implementations of the same. While we still have a long way to go before Iot devices can be used to diagnose diseases without the interference of humans, they do help a lot in assisting doctors in making diagnosis, it also has made life of patients with diseases like diabetes and BP to monitor their health stats daily and be able to plan a more effective day without having to go to the hospital every day.

A regular check on symptoms and health stats also makes it easier to keep track of small changes and make a more effective diagnosis faster than the traditional ways, even when diagnosis is made it's important to see whether the prescribed medications are working, which can also be monitored with great precision with the help of smart healthcare devices. These ideas when implemented to check the accuracy if this method showed high levels of accuracy with some errors, for temperature sensors and BP sensors the error percentage can be observed in Fig 7 and Fig 8. When studies were done to increase accuracy, the main reason found for the deviation in temperature sensors is moment of patients, and it was also taken into consideration that a small portion of deviation must also be caused by motion artefacts, these two motion affects combined lead to deviations and minor inaccuracies in data. Also, when people use these devices at home without any professional supervision, mistakes can be made in the placement of devices which further leads to the sensors not working at their maximum capacity leading to inaccuracies. Another important aspect of implementing these systems is to make sure that only the patient and assigned doctor can access the data, thus the information should be password protected. While implementing smart healthcare devices to make sure that the devices are safe and don't cause extra damage due to errors, after experiments 5% was bet as the threshold of acceptable error percentage. With time the number of studies in smart healthcare sector are increasing, as shown in Fig 9, thus, making it more effective and reliable.

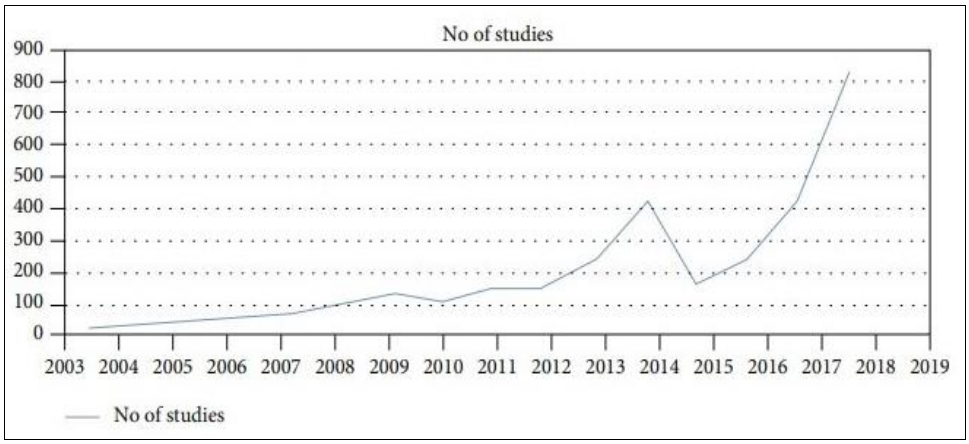

Fig 9: No of studies in healthcare over the years

4. Security and Patient privacy

To create a system where a large number of devices are connected to the cloud and share data amongst one another, with increasing number of IPS the probability of a malpractice [13] increases as well. The control of healthcare devices in wrong hands can lead to misuse as well as a hinderance in the normal functioning of the system, also these devices store medical information of patients which is personal to the people and can be used for wrongful purposes, thus, making safety a concern while digitizing healthcare.

4.1 DDoS

One such type of attack to which the system might be susceptible to is DDoS which stands for Distributed Denial of Services. The attack works by making multiple devices of a system by getting control over them and denying the services commanded by the central control system of the person using the device, thus making the whole system ineffective. These attacks are usually done with the use of malicious bonnets [15]. When the code for Miral virus leaked it opened opportunities for hackers and thus lead to an increase in the number of systems affected from the virus

from 493,000 from 213,000. This not only causes hinderance in the systems till control is restored but also collateral damage, also some devices can both receive and send commands thus an attack on them puts the health of people in risk, and with millions of devices worldwide susceptible to such viruses this becomes a bit issue making the whole working of smart healthcare unreliable, thus, actions are needed to be taken to maximize security. Making IoT devices malware proof not only makes them safer and more effective but also assure that the maintenance cost is reduced thus reducing the cost of working of smart healthcare by a good margin. Even the studies done by Analysts at Goldman Sachs it was proved that while the perfect smart healthcare system has a long way to go, but it's a cause worth working on as it'll increase efficiency and reduce the cost of healthcare dramatically.

4.2 Security Concerns

The extent at which security is an issue in healthcare can be seen by the findings of a study done in 2015 by researchers which showcased that more than 70,000 systems are online which are susceptible to one or another kind of malpractice virus attack, and a finding was made that one of the main reasons for this vulnerability is that the systems were on the internet connected to devices which ran on older, less protected versions of windows XP. To conduct the search a specific kind of search engine Shodan was used which had the capability to look for IoT devices over the internet. The systems detected not only used devices which shows stats of health but also operational devices such as anaesthesia equipment, cardiology devices, nuclear medical systems, infusion systems, pacemakers, MRI scanners. All these devices were also easily found with the help of Shodan, which brings in more weight to the finding that the systems were susceptible to attack which could be hazardous [19]. As much as it's possible to cause harm to patients by getting control over the devices, it is a situation that hasn't occurred yet, most of the hacking attacks are done with the intention of getting access to private medical and personal details in the system database.

4.3 Medjacking

Considering the risk on medical records that digitizing healthcare imposes the term Medjacking [18] was coiled to refer to the same by TarpX a security company. The company also released data [16] that showed that almost all healthcare systems are susceptible to some sort of virus attack [14], also it gave case studies of three attacks that took place at three hospitals. In one of those attacks the attackers tried to get control over the systems to get access to private medical data and personal information of the staff and patients, the information collected from the attack was being send to eastern Europe. In this attack the attack begins by taking control over blood gas analysers with the help of two malwares. While in the other case control was gained by initially attacking the hospital's radiology department and the information harvested was being sent to some place in China. The last case drug pump was used toget control over the systems. From these case studies we can also note that the primary function of these hacks has been to gain access to medical identities and not cause harm to patients, this is because monetarily these identities carry a lot of value, even more than getting access to credit card details from the systems.

4.4 How to implement secure smart healthcare

Smart healthcare is the future, and with time the connectivity and transferability of data and growth in the ability of devices to perform procedures, taking over the doctors the degree of risk imposed on the systems gets hight and thus the need to make the network more secure and reliable also increases. For the current time encryptions and secure boots are some of the ways that can increase the safety of systems by making them more difficult to break into. One of the most important things is to prioritize safety and incorporate measures in the initial designs itself so the final product can have multiple layers of security levels to breach making it safer. The connection between different devices should also be end to end encrypted so that no third party can access the information. This way when we implement some security measures at each step of implementation, we can make sure that the security system has depth and multiple layers. As we have noticed before that when plans are executed the results can show deviations, thus all systems should be tested thoroughly against various kinds of attacks to maximize the efficiency of the implemented safety system [17-43].

5. Conclusion

Smart healthcare is a fast growing and ever-expanding field and it's the future of medicine which is also very important as it'll make healthcare more efficient and easier to access while also making diagnosis and taking account of new findings easier. Plus, with smart healthcare the overall cost would also be reduced which is not only good for governments and organizations but also for the people as it'll make access to good healthcare not a luxury but something with an easy access to all. IoT solves problems such as making It possible for the huge amount of data in different formats to be compared through interoperability of data, makes diagnosis and analysis of patient behaviour easier and assuring maximum utilization of resources. But these applications are not without challenges, while multiple steps have to be incorporated in order to make data interoperable, the diagnostic side of application suffers from the problem of achieving enough accuracy to replace human work, and the system all together suffers from the security and privacy risks. As seen in Fig 9 the number of researches and studies in the sector are increasing thus making Iot in healthcare more widespread and reliable with time. Being on the same path our goal is to achieve a system which can make maximum use of the data received from multiple devices while processing the data received with high accuracy and through it all maintaining the security of systems.

6. References

1. Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS. The internet of things for health care: A comprehensive survey. IEEE Access. 2015;3:678-708.
2. Kim HH, Lee SY, Baik SY, Kim JH. MELLO: Medical lifelog ontology for data terms from self-tracking and lifelog devices. Int. J Med. Inform. 2015;84:1099-1110.
3. Mezghani E, Exposito E, Drira K, Da Silveira M Pruski C. A semantic big data platform for integrating heterogeneous wearable data in healthcare. J Med. Syst. 2015;39:185.
4. Gomez C, Oller J, Paradells J. Overview and evaluation of Bluetooth low energy: An emerging low-power

wireless technology. Sensors. 2012;12:11734-11753.
5. Argyro Mavrogiorgou, Athanasios Kiourtis, Konstantinos Perakis, Stamatios Pitsios. Dimosthenis Kyriazis IoT in Healthcare: Achieving Interoperability of High-Quality Data Acquired by IoT Medical.
6. HL7 FHIR. Available online: https://www.hl7.org/fhir/ (accessed on 25 March 2019).
7. Ahmed S, Ilyas M, Raja MYA. Internet of Things: application in smart healthcare, in Proceedings of the 9th International Conference on Society and Information Technology (IICSIT 2018), Orlando, Florida; c2018. p. 19-24.
8. Banka S, Madan I, Saranya SS. Smart healthcare monitoring using IoT. International Journal of Applied Engineering Research. 2018;13(15):11984-11989.
9. Anurag Tiwari, Viney Dhiman, Mohamed AM, Iesa Haider Alsarhan, Abolfazl Mehbodniya, Mohammad Shabaz. Patient Behavioral Analysis with Smart Healthcare and IoT [http://www.hindawi.com/journals/bn/2021/4028761/]
10. Uddin MZ. A wearable sensor-based activity prediction system to facilitate edge computing in smart healthcare system, Journal of Parallel and Distributed Computing. 2019;123:46-53.
11. Chen L, Jagota V, Kumar A. Research on optimization of scientific research performance management based on BP neural network, International Journal of System Assurance Engineering and Management; c2021. p. 12.
12. Walton MK. Addressing and advancing the problem of missing data. J Biopharm. Stat. 2009;19:945-956.
13. Chacko A, Hayajneh T. Security and privacy issues with IoT in healthcare. EAI Endorsed Transactions on Pervasive Health and Technology. 2018 Jul 23;4(14):e2.
14. Brook C. Health and fitness applications poor at protecting privacy, FTC says, Threatpost; c2014 May 8.
15. Michael K. Hackers create more IoT botnets with Mirai source code, PC World, 2016 October 18.
16. Catalin C. Thousands of IoT Medical Devices Found Vulnerable to Online Attacks; c2015 September 29. http://news.softpedia.com/news/thousands-of-iotmedical-devices-found-vulnerable-to-online-attacks493144.shtml
17. William T. Healthcare's Internet of Things should be the security of Things; c2015 May 19. http://www.healthcareitnews.com/blog/healthcaresinternet-things-should-be-security-things
18. Mahmood S. Medjacking: The newest health care risk; c2015 September 24; http://www.healthcareitnews.com/news/medjackingnewest-healthcare-risk
19. Harriet T. How the Internet of Things could be fatal, 2016 March4; http://www.cnbc.com/2016/03/04/howthe-internet-of-things-could-be-fatal.html
20. Jayaprakash V, Tyagi AK. Security Optimization of Resource-Constrained Internet of Healthcare Things (IoHT) Devices Using Asymmetric Cryptography for Blockchain Network. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2021. Lecture Notes in Networks and Systems, Springer, Singapore; c2022. p. 481. https://doi.org/10.1007/978-981-19-3182-6_18
21. Saravanabavan V, Aneesh P, Babu HM, Harieswari M, Balaji D, Vinothini C. Patient's perception and level of primary health care utilization in east block of Madurai North taluk: A geo-health study. Int. J Geogr. Geol. Environ. 2021;3(1):34-41.
22. Shruti Kute, Amit Kumar Tyagi, Rohit Sahoo, Shaveta Malik, Building a Smart Healthcare System Using Internet of Things and Machine Learning, in Big Data Management in Sensing: Applications in AI and IoT, River Publishers; c2021. p. 159-178.
23. Meghna Manoj Nair, Amit Kumar Tyagi, Richa Goyal, Medical Cyber Physical Systems and Its Issues, Procedia Computer Science. 2019;165:647-655. ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.01.059.
24. Shruti Kute, Amit Kumar Tyagi, Meghna Manoj Nair. Research Issues and Future Research Directions Toward Smart Healthcare Using Internet of Things and Machine Learning, in Big Data Management in Sensing: Applications in AI and IoT, River Publishers; c2021. p. 179-200.
25. Kumari S, Muthulakshmi P, Agarwal D. Deployment of Machine Learning Based Internet of Things Networks for Tele-Medical and Remote Healthcare; In: Suma V, Fernando X, Du KL, Wang H. (eds) Evolutionary Computing and Mobile Sustainable Networks. Lecture Notes on Data Engineering and Communications Technologies; c2022. p. 116. Springer, Singapore. https://doi.org/10.1007/978-981-16-9605-3_21
26. Rekha G, Tyagi AK, Anuradha N. Integration of Fog Computing and Internet of Things: An Useful Overview; 2020. In: Singh P, Kar A, Singh Y, Kolekar M, Tanwar S. (eds) Proceedings of ICRIC. Lecture Notes in Electrical Engineering; c2019. p. 597. Springer, Cham. https://doi.org/10.1007/978-3-030-29407-6_8
27. Sheth HSK, Tyagi AK. Mobile Cloud Computing: Issues, Applications and Scope in COVID-19. In: Abraham, A., Gandhi, N., Hanne, T., Hong, TP., Nogueira Rios, T., Ding, W. (eds) Intelligent Systems Design and Applications. ISDA 2021. Lecture Notes in Networks and Systems; c2022. p. 418. Springer, Cham. https://doi.org/10.1007/978-3-030-96308-8_55
28. Amit Kumar Tyagi, Aswathy SU, Aghila G, Sreenath N. AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology IJIN. 2021 October;2:175-183.
29. Shamila M, Vinuthna K, Tyagi Amit. A Review on Several Critical Issues and Challenges in IoT based e-Healthcare System; c2019. p. 1036-1043. 10.1109/ICCS45141.2019.9065831.
30. Mishra S, Tyagi AK. The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. In: Pal S., De D., Buyya R. (eds) Artificial Intelligence-based Internet of Things Systems. Internet of Things (Technology, Communications and Computing). Springer, Cham; c2022. https://doi.org/10.1007/978-3-030-87059-1_4
31. Amit Kumar Tyagi, Meghna Mannoj Nair, Deep Learning for Clinical and Health Informatics, in the book Computational Analysis and Deep Learning for Medical Care: Principles, Methods, and Applications; c2021 July 28. Doi: https://doi.org/10.1002/9781119785750.ch5

32. Kumari S, Vani V, Malik S, Tyagi AK, Reddy S. Analysis of Text Mining Tools in Disease Prediction. In: Abraham A., Hanne T., Castillo O., Gandhi N., Nogueira Rios T., Hong TP. (eds) Hybrid Intelligent Systems. HIS 2020. Advances in Intelligent Systems and Computing. Springer, Cham; c2021. p. 1375. https://doi.org/10.1007/978-3-030-73050-5_55
33. Gudeti B, Mishra S, Malik S, Fernandez TF, Tyagi AK, Kumari S. A Novel Approach to Predict Chronic Kidney Disease using Machine Learning Algorithms, 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore; c2020. p. 1630-1635. Doi: 10.1109/ICECA49313.2020.9297392.
34. Amit Kumar Tyagi, Dr. Meenu Gupta, Aswathy SU, Chetanya Ved. Healthcare Solutions for Smart Era: An Useful Explanation from User's Perspective, in the Book Recent Trends in Blockchain for Information Systems Security and Privacy, CRC Press; c2021.
35. Tyagi, Amit Kumar, Nair, Meghna Manoj, Niladhuri Sreenath, Abraham, Ajith. Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead, Journal of Information Assurance & Security. 2020;15(1):1-16.
36. Nair MM, Tyagi AK, Sreenath N. The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges, 2021 International Conference on Computer Communication and Informatics (ICCCI); c2021. p. 1-7. Doi: 10.1109/ICCCI50826.2021.9402498.
37. Kute SS, Tyagi AK, Aswathy SU. Industry 4.0 Challenges in e-Healthcare Applications and Emerging Technologies. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore; c2022. https://doi.org/10.1007/978-981-16-6542-4_1
38. Kute SS, Tyagi AK, Aswathy SU. Security, Privacy and Trust Issues in Internet of Things and Machine Learning Based e-Healthcare. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore; c2022. https://doi.org/10.1007/978-981-16-6542-4_15
39. Madhav AVS, Tyagi AK. The World with Future Technologies (Post-COVID-19): Open Issues, Challenges, and the Road Ahead. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications; c2022. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_2
40. Nair MM, Kumari S, Tyagi AK, Sravanthi K. Deep Learning for Medical Image Recognition: Open Issues and a Way to Forward. In: Goyal D., Gupta A.K., Piuri V., Ganzha M., Paprzycki M. (eds) Proceedings of the Second International Conference on Information Management and Machine Intelligence. Lecture Notes in Networks and Systems; c2021.p. 166. Springer, Singapore. https://doi.org/10.1007/978-981-15-9689-6_38
41. Sai GH, Tripathi K, Tyagi AK. Internet of Things-Based e-Health Care: Key Challenges and Recommended Solutions for Future. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P.C., Ganzha, M. (eds) Proceedings of Third International Conference on Computing, Communications, and Cyber-Security. Lecture Notes in Networks and Systems; c2023. p. 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_37
42. Tyagi AK. (Ed.). Data Science and Data Analytics: Opportunities and Challenges (1st ed.). Chapman and Hall/CRC; c2021. https://doi.org/10.1201/9781003111290
43. Tyagi AK, Abraham A. (Eds.). Recurrent Neural Networks (1st ed.). CRC Press; c2022. https://doi.org/10.1201/9781003307822.
44. Kute S, Shreyas Madhav AV, Tyagi AK, Deshmukh A. Authentication Framework for Healthcare Devices Through Internet of Things and Machine Learning. In: Suma V, Fernando X, Du KL, Wang H. (eds) Evolutionary Computing and Mobile Sustainable Networks. Lecture Notes on Data Engineering and Communications Technologies. Springer, Singapore; c2022. p. 116. https://doi.org/10.1007/978-981-16-9605-3_27