IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Security issues in IoT enabled Health Monitoring

Renu Sharma

PG Dept. Of Computer Sc. & IT, DAV College, Amritsar, India

Available online at: www.ijcseonline.org

18/May/2018, Published: 31/May/2018

Abstract- IoT (Internet of things) means to connect heterogeneous devices with internet. When devices are medical then it involves human is at stake. It isimportant to provide security as well as privacy to a human. It should not be like a person using such devices, can be controlled from anybody and from anywhere. In this paper various security threats are discussed which can be raised while using smart health monitoring.

Key words: IoT, BAN, RFID

I. Introduction

IoT (Internet of things) means we are having devices connected to internet. And that information can be shared to produce outcomesvaluable for mankind. Forthcoming of computing will not rest on desktops but will be of IoT devices.[1]. IoT is most significant electronic revolution after internet[2]. Even gartnerreport(2014) states that this going to have major expansion. If we check at area of applications of IoT, list is quite long but some of them are:[3]

- Smart Health
- Smart Home
- Smart cities
- Smart Education
- Smart Transport
- Disaster detection etc…..

In today's world, there is no area untouched by IoT.

II. Main components of IoT

IOT is largely based on:[4]

- Sensors
- Middleware
- Cloud computing
- Internet

Sensors: They are used to get get relevant data. Restraints of sensors are low availability of energy, low computation and low memory. Due to these restraints making such a system is difficult.

Middleware: in such an environment all devices have diverse architecture to make communication possible, we need softwares.

They are in control to fit in various devices.

Cloud computing : To design an IoT based application we need a cloud because sensors has low computation power and to make the computation possible we need processing power which is of a cloud.

Internet: to attachmany sensors and cloud we prerequisite Internet. Sensors are also power constrained so it is not feasible to have sensors all time on internet. SoPAN(personal area network) can be used. In medical applications even BAN(Body Area Network) can also be used And linking with the internet can be given for smaller time duration.

III. Challenges in development of IoT

In development of IoT many key problems are there. Some of them are:[5]

- Security
- Privacy
- Interoperability and integration
- Data storage
- Constrained resources

Security: smart health monitoring is primarily based on sensor network which can be controlled from anywhere using internet. So in such an environment security is the major concern. Nodes can be compromised that's why a very strong security system is required to monitor any kind of external as well as internal threat.

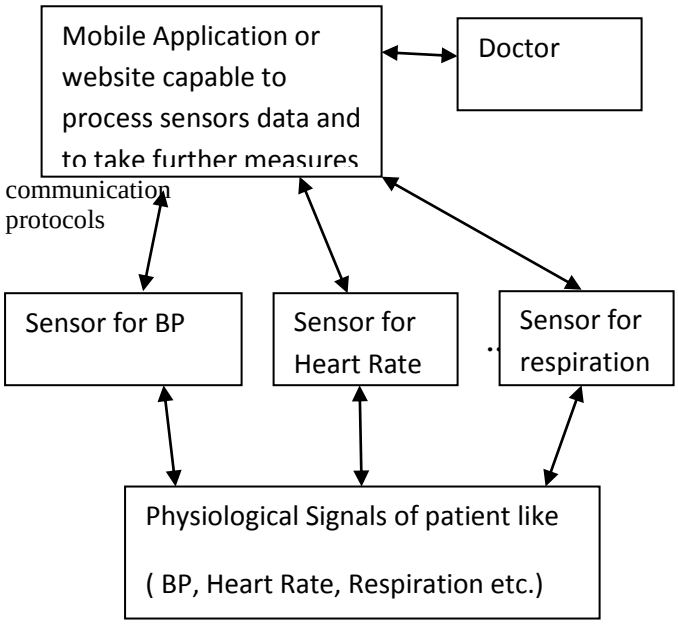
Privacy: privacy is also main worry. Somebody can learn all patterns of anyone just by analyzing data of sensors. And that information can be used for criminal activities.

Interoperability and integration: IoT is mostly based upon sensors. Sensors do have diverse architectures. To join them and to integrate them is main challenge.

Data Storage: in any smart environment a large amount of data is produced. To process that large data traditional data processing techniques cannot be used.

Constrained resources : in IoT devices major parts are sensors. Sensors are constrained in processing power , battery life and memory. To conquer these constraints are also a big challenge.

IV. General Architecture for Smart Health Monitoring System



in smart health care architecture generally three layers are there.[6] First is patient having all the sensors for determining his or her physiological condition. All the sensors communicate using protocols like zigbee, Zwave, Bluetooth etc. with their software (which can be a mobile application or web based application)[7]. That software is going to act as a bridge between patient and doctor.

V. Security Threats in Smart Health Monitoring

Smart health care can have many Security threats.[8] Some of them could be:

- Unauthorized Access
- Modification of message
- Denial of Service
- Controlled Node
- Routing attack.
- Alteration in dosages. ……

Unauthorized Access : Generally third layer of such system is an app or software which can be accessed by user names and passwords. That can have a security breach.
In many papers solution to this problem has been given like cryptography or RFID, EPC [9] [10]

Modification of message: sensors are going to communicate with central software and that is internet enabled. So if a hacker wants to change message give by sensors, that could be a very serious threat.

Denial Of Service: all the system is Internet enabled, so a hacker can create a denial of service situation. In that case all the system will be collapsed. So some measures are to be taken to deal with it.

Controlled Node : if any of the node is being controlled by any hacker. It can mislead the system. In this case misleading is very important because it involves human life.

Routing attack: routing attack could be possible which can create delay in message receiving and if some one is in critical situation delay means at the cost of somebody's life.

Alteration in Dosage : some devices like insulin based dosage can be controlled remotely. But unauthorized person can do havoc in such situations.

VI. Conclusion

Smart health care is for sure going to be in our life. Advantages of this type of monitoring are a lot. But some problem areas are also there and one of the main problem is security. In this area many solutions are being proposed but still there are many gaps. A lot of research is required to cover each and every aspect of security.

References

[1] Gubbi Jayavardhana et al.,"Internet of Things(IoT): a vision, architectural elements and future directions ", Journal of Future Generation Computer Systems, Volume 29, Issue 2, 2013, Pages 1645-1660
[2] NguH. Anne et al., " IoT Middleware: A Survey on Issues and Enabling Technologies", IEEE Internet of Things journal, volume 4, issue 1, February 2017
[3] D Sehrawat et al., "Data Mining in IoT and its Challenges", International Journal of Computer Science and Engineering, Vol-6, Issue-4, 2018
[4] Lee In, Lee Kyoochun," The Internet of Things (IoT): Applications, investments, and challenges for enterprises", Business Horizons, volume 58, issue 4, july-august 2015, pages 431-440

[5] D. Raggett, " The Web of Things: Challenges and Opportunities," IEEE Computer, volume 48, May 2015
[6] A. Lymberis,"Smart Wearables for remote health monitoring, from preventation to rehabilitation : current R & D, future challenges", Information Technology Applications in Biomedicine, 2003.
[7] Alexandros Pantelopoulous and Nikolaos G. Bourbakis, "A Survey on Wearable Sensor Based Systems for Health Monitoring and Prognosis", IEEE transactions and Systems, Man and Cybernetics, Vol 40, No. 1, January 2010.
[8] Ng H.S. et. al. ,"Security issues of wireless sensor networks in healthcare applications", Springer, April 2006.
[9] Alexandre Santos et. al.,"Internet of Things and Smart Objects for M-health Monitoring and Control", ProcediaTechnology,2014.
[10] A. Pandey et. al, "IOT Based Home Automation Using Arduino and ESP8266", International Journal of Computer Science and Engineering, Vol-6, Issue-4, 2018

Authors Profile

Ms. Renu Sharma pursed Masters in Computer Applications from Guru Nanak Dev University, Amritsar in 2001. She is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Sc. & IT, DAV College, Amritsar . She has published 10 research papers in reputed international journals and conferences. Her main research work focuses on Internet Of Things, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. She has 14 years of teaching experience.

