International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Interconnected Medical Devices and their Security Aspects

Anurag Panwar[1], Syed Imtiyaz Hassan[2], Jawed Ahmed[3]
[1, 2, 3]*Department of Computer Science and Engineering, Jamia Hamdard (Deemed to be University), New Delhi, India*

Abstract: With the rapid growth of interconnected technologies in the recent time, the world is going under a huge change. Medical and healthcare sectors are also influenced by the advancement in connected technologies. Internet of Things (IoT) in medical device has played a key role in increasing the facilities which can be provided by the healthcare sector. As the healthcare sector is getting digitalized and millions of interconnected devices would communicate important information, it increases the risk factor and new privacy and security issues would arise. This paper focuses on how secure communication between the devices can be achieved and how a weak link in the chain can turn into disaster. It would also look on the research directions which can be done to strengthen the system.
Keywords: Internet of Things, Internet of Medical Things, Security, Privacy Issues, Lightweight cryptography.

I.INTRODUCTION

"The most erudite technology are those that dissipate. They blend themselves into the fabric of everyday life up to a level until they are indistinguishable from it" was Mark Weiser's central statement in his seminal paper (Weis 91) in Scientific American in 1991[1]. The word IoT is not new itself but two decades old but as the time passes the technology is also growing and reaching newer sectors such as schools, automobile industry, healthcare and medical industry. Internet of Medical Things (IoMT) is becoming a well known concept in numerous number of medical devices. Just to give an example how IoT in medical devices affect our life: you enter a market and while going through shopping , as you move towards the pharmacy your fitness monitor vibrates and takes all your vital statistics and send it to your doctor who in return updates your prescriptions [2].

In the early years of IoT, it was basically known for machine to machine communication. This type of communication indicates two machine communication with each other without human involvement [2][3]. The term IoT was first used by Kevin Ashton, co-founder and executive director of Auto-ID Center at Massachusetts Institute of Technology in the year 1999 and refers to peculiarly identifiable objects and their virtual portrayal in an "internet-like "structure [4][2]. Nevertheless, in the past ten year, this concept has been used in healthcare, transport utilities and various other domains [4][2]. A range of various devices are used in healthcare. One such example is fitness band (FitBit) [19] to monitor activity of the user. Fitbit broadcast a unique ID through which a user can be uniquely identified and by using a network of cheap receiver a user can be tracked to a small geographical area [3].

There are three major constraint in security on IoMD: power requirement, bandwidth requirement, and processing requirement [3]. These three constraints will always be present in the IoMT and we have to work our way around them to make the technology more secure and reliable. As the medical devices would be transmitting very important data of the user so it should be securely transmitted and received. Manipulating the data from IoMT can prove fatal for its user. Some of the uses of IoMT are discussed here along with the security threats they may face.

II.SECURITY ISSUES

IoMT device may be widely used in the healthcare sector but still there are concerns left regarding how secure are they. As they are low power computing device with limited computational capabilities it is easy to target them as they have very less protection against an attack.

A. Cancer Treatment

In year 2018 in the month of June, data was presented at the ASCO annual meeting from a randomized clinical trial of around 350 patients who were being treated for cancer in various parts of human body. The process used a low frequency communication device attached to the patients' body to measure blood pressure and weight, based on the input from the sensors the symptom-tracking app send updates to patients' physicians on which he can give his consent for proper treatment [5]. Suppose if the data transmitted here is changed, it can fatally harm the patient as he would be receiving wrong treatment.

B. Smart and continuous glucose monitoring (CGM) and insulin pens

A CGM is a device which monitors the blood glucose levels at regular intervals and recommends the correct type and amount of insulin injection at the appropriate and necessary time [5]. The data from the CGM device if changed can harm the user as the user would be taking incorrect dose of his medicine.

C. Closed Loop (Automated) Insulin Delivery

The automatic system of delivery of insulin may change the life of diabetic patients completely by itself releasing the insulin as and when required in the correct amount [5]. As this system would receive data form a sensor which monitors blood glucose levels and then the pump would release correct amount of insulin so if someone could get access to it he may change the blood reports and due to it incorrect insulin may be released which may prove fatal.

III.SECURITY LAYERS OF IoMT

There are four layers in IoMT which have various working and has some drawbacks which are looked upon below

1) *Perceptual Layer:* Most of the time the perceptual nodes in medical devices are a bit short of computing power and also has very limited storage capacity. Therefore they are unable to apply random and fast frequency switching for a secure communication and encryption algorithm using public key for security protection. Also attack from external network such as denial of service is also a major problem [6].
2) *Network Layer:* It is where the network/internet lives and communicates [7]. Although the main network itself can be called a secure network but still Man in the Middle (MITM)[18] and counterfeit attack are a threat. Junk mail and virus can also not be ignored [6]. In IoMT if someone perform a MITM[18] attack then he may change the data leading to problems and improper diagnosis.
3) *Support Layer:* It does the intelligent decision making and mass processing the data in bulk, but it has limited ability to recognize malicious data [6]. Due to this limited capability to identify malicious data an wireless medical device may receive malicious data and process it and misbehave.
4) *Application Layer:* In the application layer the security requirements for various application are different, and here data is shared which creates a problem of data privacy, access control and discloser of information [6]. As the IoMT device may carry the user's personal information like his complete health record so if captured by someone when in transit it may be misused.

IV.SECURITY REQUIREMENTS OF IoMT

By the analysis we have done above of the security features in IoMT, we can summarize the security requirement in each layer as:

1) *Perceptual Layer:* Authentication of medical device node which is to be communicated is necessary to prevent illicit node access; encryption should be used to prevent classified information during transference; the encryption methods should be lightweight as the power and processing constraints are also present, so lightweight cryptographic protocol and encryption should be used.
2) *Network Layer:* Existing security measures of communications of data in between different medical device are difficult to be used here. Identity authentication can be a measure that can identify rogue nodes and prevent DDoS[17] type of attack and MITM[18] attack. Confidentiality and integrality mechanism are of equal importance to maintain trust as the data the device is transmitting is the personal health data.
3) *Support Layer:* It requires a variety of security based application architecture such as secure computation between multiparty and cloud computing, almost all of the robust encryption algorithms' and protocol are in dire requirement for the support layer, strong system security and antivirus technology [6].
4) *Application Layer:* To solve the security issues of application layer in IoMT key authentication and agreement should be there across various systems, and end user privacy protection should be taken care.

To maintain the required security in the devices of the medical application there is the requirement of using strong encryption algorithms and technique. Encryption is required at both the time, first when the data is stored on the device and second when it is transmitted. While it is stored on the sensor it store all the health information of the user which is confidential and can be misused. Anyone with proper reader can access the information stored on the chip as it has the basic functionality of just monitor medical stats of the user and transmit it when requested. It does not check that the receiver asking for information is genuine of not. For this purpose various security mechanisms such as device authentication and identification should be implemented which can be done by using cryptographic algorithms.

Cryptographic algorithms can be used to to identify the sender and receiver and also help in maintaining data confidentiality.

V.CRYPTOGRAPHIC ALGORITHM IN IoMT

The use of symmetric encryption algorithm such as advance encryption standard (AES) is used to maintain confidentiality in the process of communication on the other hand the asymmetric such as RSA is used for key transport and digital signature. Also asymmetric algorithm such as diffie-hellman(DH) is used for key agreement and for integralitySHA-1 and SHA-256 algorithms can be applied. Another important asymmetric-algorithm which provide safety by using shorter key length is elliptic curve cryptography (ECC), can also be used [6][8].

The processing and transfer of data in a secured form is the main function of using various form of cryptography. The operations performed in cryptography which are key generation, hash generation and their verification [11]. Table 1 names a few cryptographic algorithm and their uses. Hu et al. [12] and Wood et al.[13] gave solutions for smart objects to use cryptography in their study[11][12][13].Liu et al.[13] and Chung et al.[15] works show key distribution mechanism for lightweight communication channels and network in which resources are limited[11].

A. Cryptographic Primitives Goals to secure IoMT

The primal goal of cryptography in general is to comply with the main security goals for exchanged messages and the system itself [2][9].

1) Main Security Requirement Are: Confidentiality, Integrity, Authenticity, Availability

B. Securing IoMT

Here in IoMT the use of the CIA triad can also be implemented to improve the security aspectof the devices communication as it is important to protect the information of the individual to get exposed as in IoMT the device has the capacity to autonomously form a network of sensors and relay information so even collection of tiny bits of data from a huge sensor array could lead to yield important information [10].

VI. OFFLINE SIMULATION AND RESULTS AND SECURITY

In a Client and server model various cryptographic technique are used to impart security and manage confidentiality, integrity, non-repudiation and authentication[16].Here we have simulated a communication between nodes in a simulator. We have set up in total of six nodes of which node 3 and 6 are receiver nodes and node 2, 4 and 5 are used to transmit data.

A. Experiments and Simulations

All the experiments were performed using contiki[20] with Cooja[21] simulator running in Ubuntu-64 bit on 7th generation, i5 CPU processor and 8 G.B RAM.

Here in figure 1 we can see the set up of an array of some of the nodes which can be any form of medical device

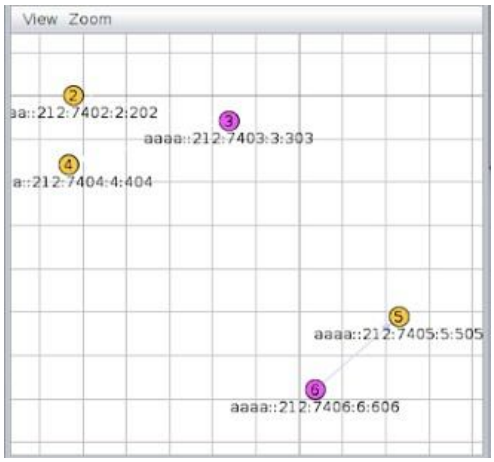

Figure 1: Showing Setup of Nodes with the Address

In the figure 2 we can see the nodes have started passing the data in between them where node 3 and node 6 is receiver and node 2, 4 and 5 are sender of the data.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

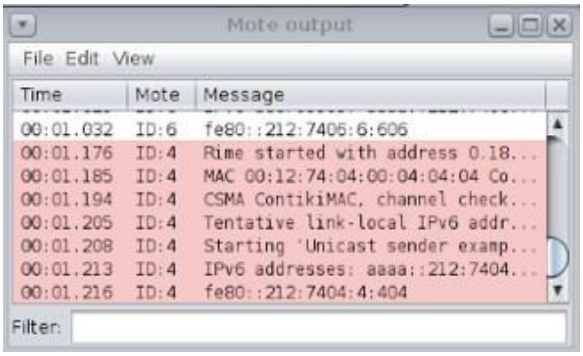

Figure 2: Shows the communication has started

Figure 4 shows the data transfer between nodes 2, 4 and 3 and figure 6 shows the log of communication

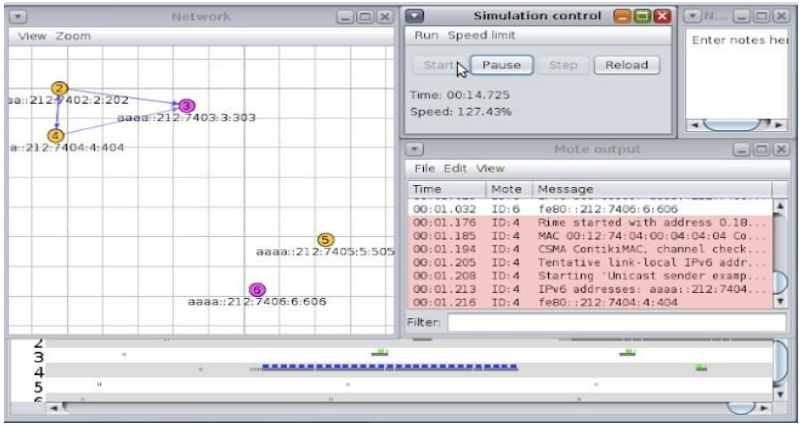

Figure 3: Shows Flow of Communication between nodes

In Figure 3 the flow of message is seen from node 2 and 4 to receiver 3.

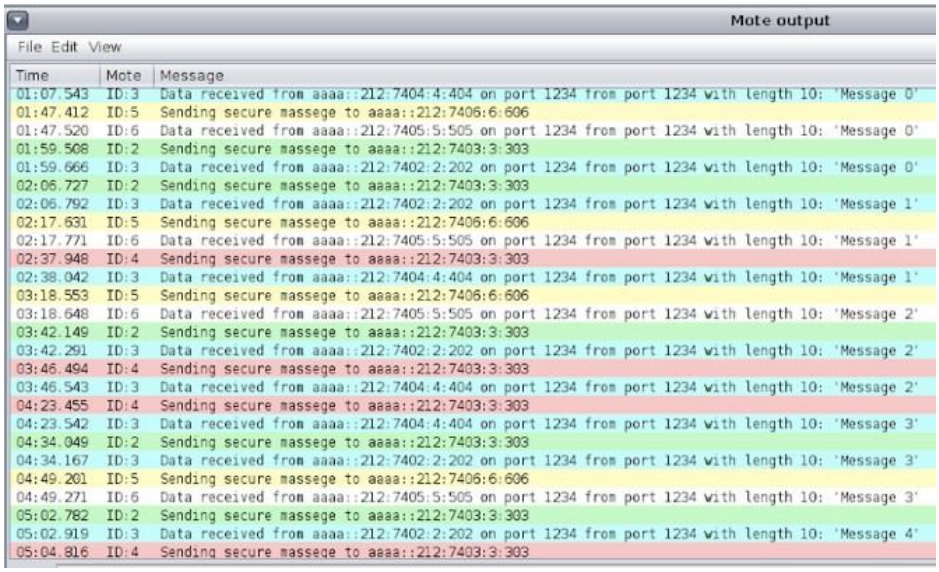

Figure 4: Message communication between nodes

In figure 4 we can see the secure communication in between the simulated node devices.
We can see the flow of message from one node to another.

VII. RESULT AND CONCLUSION

In this paper we have studied various drawbacks which are there in the IoMT which is internet of medical things and how they can be improved. Various security measures like using lightweight cryptography and device authentication are discussed in here for the interconnected medical device and their security. This can be improved by implementing the strong authentication of device when communicating sensitive information of the user.

REFRENCES

[1] Madakam, S., Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3, 164-173. http://dx.doi.org/10.4236/jcc.2015.35021
[2] Muhammad A. Iqbal, Oladiran G.Olaleye & Magdy A. Bayoumi "A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches"
[3] Christian Dancke Tuen "Security in Internet of Things Systems" Master Thesis Norwegian University of Science and Technology.
[4] Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. Vision and Challenges for Realising the Internet of Things; European Commission—Information Society and Media: Brussels, Belgium, 2010. [5] internet of things healthcare ; Available [online] https://econsultancy.com/internet-of-things- healthcare//
[5] Suo, Hui & Wan, Jiafu & Zou, Caifeng & Liu, Jianqi. (2012). Security in the Internet of Things: A Review. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012. 3. 10.1109/ICCSEE.2012.373.
[6] Designing the internet of things,part 3:Internet Protocol Stack option Available [online]"https://www.micrium.com/iot/internet-protocols/"
[7] T. Polk, and S. Turner. "Security challenges for the internet of things," Available [online]: http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf
[8] Hossein Shafagh (2013) "Leveraging Public-key- based Authentication for the Internet of Things" Master Thesis, RWTH Aachen University, Germany.
[9] https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
[10] "A Review of Security Concerns in Internet of Things" EnginLeloglu
[11] Hu, W., Corke, P., Shih, W.C. and Overs, L. (2009) SecFleck: A Public Key Technology Platform for Wireless Sensor Networks. Springer European Conference on Wireless Sensor Networks, Cork, 11-13 February 2009,296-311. https://doi.org/10.1007/978-3-642-00224-3_19.
[12] Wood, A. and Stankovic, J. (2006) AMSecure: Secure Link-Layer Communication in TinyOS for IEEE 802.15.4-Based Wireless Sensor Networks. ACM Conference on Networked Embedded Sensor Systems, Boulder, 31 October-3 November 2006, 395-396. https://doi.org/ 10.1145/1182807.1182873.
[13] Liu, D., Ning, P.and Li, R. (2003) Establishing Pairwise Keys in Distributed Sensor Networks. ACM Conference on Computer and Communications Security, Washington DC, 27 October 2003, 52-61. https://doi.org/10.1145/948109.948119.
[14] Chung, A. and Roedig, U. (2008) DHB-KEY: An Efficient Key Distribution Scheme for Wireless Sensor Networks. IEEE International Workshop on Wireless and Sensor Networks Security, Atlanta, 29 September-2 October 2008, 840-846. https://doi.org/10.1109/MAHSS. 2008.4660127
[15] William Stallings, Cryptography and Network Security: Principles and Practices, Pearson, 2014
[16] C. Wang, J. Zheng and X. Li, "Research on DDoS Attacks Detection Based on RDF-SVM," *2017 10th International Conference on Intelligent Computation Technology and Automation (ICICTA)*, Changsha,2017,pp.161-165.doi: 10.1109/ICICTA.2017.43
[17] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027-2051, third quarter 2016.doi: 10.1109/COMST.2016.2548426
[18] Fitbit®: An accurate and reliable device for wireless physical activity tracking Diaz, Keith M. et al.International Journal of Cardiology , Volume 185 , 138 – 140
[19] A. Dunkels, B. Gronvall and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," *29th Annual IEEE International Conference on Local Computer Networks*, Tampa, FL, USA, 2004, pp. 455-462. doi: 10.1109/LCN.2004.38
[20] M. Tutunović and P. Wuttidittachotti, "Discovery of Suitable Node Number for Wireless Sensor Networks Based on Energy Consumption using Cooja," *2019 21st International Conference on Advanced Communication Technology (ICACT)*, PyeongChang Kwangwoon_Do, Korea(South),2019,pp.168-172. doi: 10.23919/ICACT.2019.8702021