Security Issues in E-Healthcare IoT

Aashmeen Jammu[1] Dr.Harjinder Singh[2]
[1,2]Department of Electronics & Communication Engineering
[1,2]Punjabi University, Patiala, India

Abstract— From the last few years, the field of internet of things (IoT) is transforming the concept of e-healthcare. The patients can be easily monitored wirelessly and the record of the patients is available as well as communicated online. But along with every new opportunity, new problems arise. In case of IoT, the major problem is limited security as IoT mostly deals with resource constraint devices. Security is the major concern in the IoT based electronic health (e-health) system. Wireless attacks like eavesdropping, masquerade attacks, replay attack, snooping attack poses a threat to the network security. In this paper, various privacy as well as security issues in e-healthcare IoT are analyzed in tabular form.

Key words: IoT, E-Healthcare, Security, Attacks, Threats, Eavesdropping, Replay Attack

I. INTRODUCTION

With the advancement of technology, almost everything can collect and exchange data. Internet of things (IoT) is a platform that connects any person, any place, anything or even any service to the internet. IoT is a wide application area. The applications of IoT range from industrial and agricultural field to smart cities and healthcare. The following figure 1 illustrates various IoT application areas:

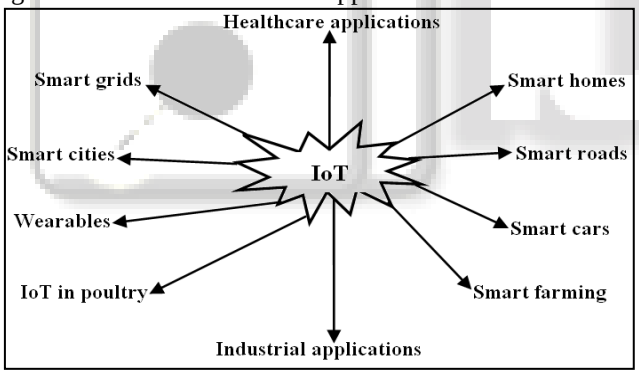

Fig. 1: IoT application areas

In case of e-healthcare, the record of the patient is electronically stored and is made available on internet for future access. So, with this the doctors can remotely access the health conditions of the patient and may alter them. But, these systems are prone to various wireless attacks and therefore, the security of patient is at huge risk. Let us consider an example of a patient, who is connected with a temperature sensor and ECG. The data recorded by these sensors is instantly uploaded to a web-page and the doctor can access the data by logging into the web-page. The doctor can also automatically turn on or off the sensors remotely according to the requirement. In this case, if an attacker is successful to eavesdrop the information of the patient then the privacy of the patient is violated and the attacker may upset the functioning of the sensors. So, due this the privacy of patient is at risk. Moreover, if the patient is suffering from an embarrassing disease then the attacker may upload the data on a social networking site to humiliate the patient [7]. Further, if the attacker is successful in achieving the insurance details for the patient, then he/she may attempt to kill the patient. So, securing the information of sensors in wireless sensor network is desirable.

In e-healthcare, the data of the patients is recorded digitally and is stored in databases. An attacker can make unauthorized access to the database and may modify the data [3]. The following figure 2 illustrates the general block diagram [2, 3] of wireless network in e-healthcare.

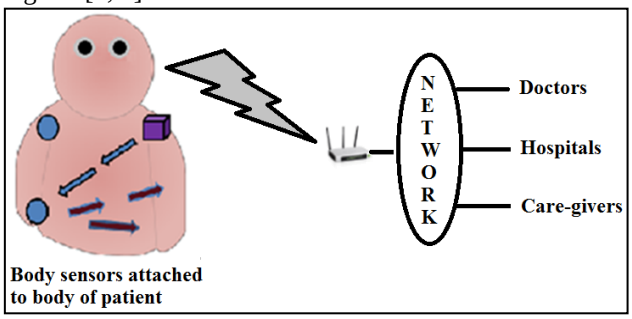

Fig. 2: General Block Diagram of Wireless Network in E-healthcare

The rest of the paper is organized as follows: Section II describes the various security issues in e-healthcare IoT in tabular form and Section III presents literature survey for the review. Conclusion is done in section IV.

II. SECURITY ISSUES

E-healthcare is prone to various attacks and threats that adversely affect the privacy and security of the patients. The following table depicts the various security issues [2, 3] prevailing in a wireless network in e-healthcare IoT:

	Attack	Description
1.	Replay Attack	In this, the attacker secretly acquires access to the secret information between two parties by eavesdropping. The attacker uses this information as a proof to its identity and gain access to the same network
2.	Activity Tracking Threats	In this, the hacker/attacker can track the activity of the patient easily. He/she can easily check and track every move of the patient at any instant of time.
3.	Location Threats	This is similar to the activity tracking threats. The attacker has access to the location of the associated individual or patient. If the attacker holds some sort of grudge against the patient then he/she can easily access the location of the patient and may use this information to kill the patient.

4.	Eavesdropping	Eavesdropping is the unauthorized way to spy on a private communication. The word eavesdrop means to actually stand and listen to a private conversation. So in this, the attacker secretly gains access to the private messages.
5.	Message Tampering	In this, the attacker makes unauthorized attempts to access the network and extract the data.
6.	Threats of Cyber Attacks on Privacy	In IoT, cyberattacks can cause censorious damage to the system. Along with this, it may add erroneous data/information to the system. Due to resource constraint nature of IoT, desired and efficient security solutions cannot be implemented in it. The risks of cyber-attacks are increasing spontaneously.
7.	Masquerade Attack	Masquerade means to pretend to be someone else. So in this, the attacker uses fake identity to access the network. The attacker may also use illegal nodes to access the network. The network will assume the illegal nodes to be real ones and the attacker may alter the information. If attacker changes value of the biological information of the patient then this may lead to false treatment and may prove to be fatal.
8.	Privilege Abuse	The privilege abuse occurs when the users accessing the database are provided with more privileges than desired. In such cases, the user may easily exploit the privileges for unfair purposes and may exploit the network by accessing secret data. So, it is termed as privilege abuse.
9.	Legitimate Privilege Abuse	Legitimate stands for authorized. In this, the attacker is provided with legitimate privilege that is, authorized access to the database. Due to this, the user/attacker can use the information attained from the database for malevolent purposes.
10.	Privilege Promotion	In privilege promotion, the software is more prone to attack due to some errors and fragility. Attacker can easily access the critical information by elevating his/her clearance level. In this, clearance determines that whether a person should be authorized to access secret information or not.
11.	Operating System Vulnerabilities	In operating system vulnerabilities, the attacker takes advantage of the vulnerabilities in operating system to attain unauthorized access to the information.
12.	Snooping Attack	In snooping attack, the attacker uses fake identity i.e. the attacker pretends to be someone else to access the data. It is quite similar to eavesdropping. But, the difference is that it is not limited to accessing of data at the time transmission.
13.	Black hole Attack	In this, the data is dropped without the source node being aware about the communication.
14.	Denial of Service Attack	In this, the network loses its ability to execute further requests and the services provided by the network are denied due to the attack. This attack may also increase the network traffic.
15.	Grey hole Attack	The grey hole attack resembles with the black hole attack in terms of behavior [13]. The dissimilarity is that in this, the entire packet of data is not dropped. The false node that is, the attacker node drops some part of data packets. This can be really dangerous for a patient as if some part of the vital information of the patient is lost then this may result in his/her false treatment.
16.	Worm hole attack	In this attack, traffic is recorded from a particular region of network and then replayed in some different region. This means that packets are captured by a compromised node from one location and then are released at some other far away location. This attack can easily commence without any information of the network. This attack is very acute as it is very difficult to perceive.
17.	Routing Threats in WSN	A malicious user may attack the network [7] and may purloin or alter the data. The routing attacks in a multi-hop network are selective forwarding, sink hole threat and sybil attack.
18.	Selective Forwarding threat	In selective forwarding threat, the information (like temperature, ECG) or some part of information/message is not forwarded by malevolent nodes. The nodes may simply drop the message to block its broadcasting. This threat can

		acutely affect the system if the attacker is also included in the routing path.
19.	Sink hole Threat	In sink hole threat, in order to initiate routes through a malevolent node, the attacker attempts to attract the existing nodes. The major drawback of this attack is that after its commencement, the network becomes vulnerable to attacks like eavesdropping, message tempering etc.
20.	Sybil Attack	In sybil attack, a malicious node uses a number of fake identities to communicate with the existing nodes. In multipath routing protocols, the compromised node may exist in various locations. This results in severe damage to the network. The code blue system is prone to this attack.

Table 1: Various security issues

III. LITERATURE SURVEY

Kalsoom Shabana, et al. [1], discussed wireless sensor network and security issues associated to it. Further, security attacks like performance oriented attacks, goal oriented attacks and layer oriented attacks were discussed.

Pathan, et al. [4], discussed various security threats and proposed security mechanisms for WSN. It also included feasibility of some common security schemes like cryptography, steganography in WSN.

Anwar, et al. [5], reviewed various security issues and attacks in WSN. The paper concentrated on physical attacks in WSN. So, security issues and physical attacks are analyzed.

Kahina Celli [6], discussed major aspects of WSN security. The common security attacks and their classification mechanisms were discussed. Further, the paper included the proposed schemes in WSN.

Pardeep Kumar and Hoon-Jae Lee [7], discussed various security issues and some security techniques in e-healthcare. The paper also analyzed various e-healthcare projects on the basis of security.

Harshavardhan Kayarkar and Sugata Sanyal [8], reviewed various security vulnerabilities and attacks in WSN. The paper also included comparative analysis of various security techniques in tabular form.

IV. CONCLUSION

Security in e-healthcare is a vital requirement. A single attack by a malevolent user may pose a threat to the life of a patient. Moreover, the provision of security is desirable for secure as well as reliable communication. This paper provides an overview of various security threats and attacks in e-healthcare IoT. The main focus of the paper is on the analysis of existing attacks on the wireless sensor network based e-healthcare systems. Based on survey, it can be concluded that the security in e-healthcare IoT is of utmost concern.

REFERENCES

[1] Kalsoom Shabana, Nigar Fida, Fazlullah Khan, Syed Roohullah Jan, and Mujeeb Ur Rehman, "Security issues and attacks in wireless sensor networks," International Journal of Advanced Research in Computer Science and Electronics Engineering, Vol. 5(7), pp. 81-87, Jul. 2016.

[2] Aashmeen Jammu and Dr. Harjinder Singh, "A Review on data security in e-healthcare IoT," International Journal for Scientific Research & Development, vol. 5(4), pp. 863-865, Jun. 2017.

[3] Aashmeen Jammu and Dr. Harjinder Singh, "Improved AES for data security in e-health," International Journal of Advanced Research in Computer Science**,** vol. 8(5), pp. 2016-2020, Jun. 2017.

[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges," ICACT, pp. 1043-1048, Feb. 2006.

[5] Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah, and Kashif Naseer Qureshi, "Security issues and attacks in wireless sensor network," World Applied Sciences Journal, vol. 30(10), pp. 1224-1227, 2014.

[6] Kahina Chelli, "Security issues in wireless sensor networks: Attacks and counter measures," WCE, vol.1, pp. 2078-0966, 2015.

[7] Pardeep Kumar and Hoon-Jae Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Network: A Survey," Sensors, vol. 12, pp. 55-91, Dec 2011.

[8] Harshavardhan Kayarkar and Sugata Sanyal, "Classification of various security techniques in databases and their comparative analysis," Acta technical corviniensis bulletin of engineering, pp. 135-138, 2012.

[9] V.Harsha Shastri, V.Sreeprada, P.Sree Rathna Malathi, and K.Siva Rama Krishna, "A study of security techniques for Internet of Things Applications," IRJMST journal, vol. 6(10), pp. 167-172, 2015.

[10] Puneet Kumar and Shashi B.Rana, "Development of Modified AES Algorithm for Data Security," Optik Journal, vol. 127, pp. 2341-2345, Nov 2015.

[11] Gagandeep Kaur, Harjinder Singh, and Amandeep Singh Sappal, "Band gap computation of 1-dimentional silicon photonic crystal for high contrast grating application," International Journal of Computer Applications, vol. 94(7), pp. 41-44, May 2014.

[12] Harjinder Singh and Amandeep Singh Sappal, "Comparative study of power amplifier linearization techniques," International Journal of Engineering Research and Development, vol. 12(3), pp. 45-48, Mar. 2016.

[13] Harjinder Singh and Amandeep Singh Sappal, "Memetic algorithm for digital pre-distortion of WiMAX power amplifier based on a memory polynomial model," Second International Conference On Innovative Trends In Electronics Engineering, vol. 20, pp. 135-140, 2016.

[14] Omar Cheikhrouhou, "Secure Group Communication on Wireless Sensor Networks: A Survey," Journal of Network and Computer Applications, vol. 61, pp. 115-132, Nov 2015.

[15] Harjinder Singh and Amandeep Singh Sappal, "Power amplifier linearization using digital pre-distortion techniques based On memory polynomial model and estimated by self-organizing migrating algorithm," Journal of Electronics and Communication Engineering Research, vol. 3(7), pp. 10-15, 2016.
[16] Mrs.A.S Bhave and Mr.S.R Jajoo, "Secure communication in wireless sensor network using symmetric and asymmetric hybrid encryption scheme," International journal of innovative science, vol. 1(4), pp. 382-385, Jun. 2014.
[17] Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Ethiopia Nigussie, Amir M.Rahmani, Seppo Virtanen, Hannu Tenhunen, and Jouni Isoaho, "End-to-end security for mobility enabled healthcare internet of things," Journal of future generation computer systems, vol. 64, pp. 108-124, Mar. 2016.

