2019 19th International Conference on Computational Science and Its Applications (ICCSA)

IoT Smart Health Security Threats

Shariq Aziz Butt
Department of Computer Science & IT
University of Lahore, Pakistan
shariq2315@gmail.com
Diaz-Martinez Jorge Luis
Department of Computer Science and Electronics,
Universidad de la Costa, Barranquilla, Colombia
jdiaz5@cuc.edu.co
Tauseef Jamal
CS Department PIEAS University,
Pakistan
tauseef.pieas@gmail.com

Arshad Ali
Department of Computer Science & IT
University of Lahore, Pakistan
arshad.ali@cs.uol.edu.pk
De-La-Hoz-Franco Emiro
Department of Computer Science and Electronics,
Universidad de la Costa, Barranquilla, Colombia
edelahoz1@cuc.edu.co
Muhammad Shoaib
Department of Software Engineering
University of Lahore, Pakistan
muhammad.shoaib1@se.uol.edu.pk

Abstract—**The Internet of things (IoT) is an active area in the current research community due to the improvement in mobile computing and wireless networks. Currently, the IoT is involved in many fields like smart cities, smart health monitoring, smart tracking, and smart factory; therefore, it is introducing new research opportunities and industrial revolutions. Smart health, in particular, is very important and trendy domain for researchers and practitioners due to its continuous monitoring of health of patients. The objective of smart health is to provide medical facilities to patients at anytime and anywhere. The smart health monitoring systems are mostly connected with the wireless network medium that is extremely vulnerable for threats. However various attacks are observed that can endanger these health monitoring applications and systems. These attacks include Denial of Service (DoS) Attack, Fingerprint and Timing-based Snooping, Router Attack, Select and Forwarding attack, Sensor attack and Replay Attack. In this paper, we discuss these attacks with their impact on health monitoring systems with some suggestive measures from our research findings.**

Keywords— Internet of Things; Smart Health; Security Threats;

I. Introduction

Due to developments in mobile and wireless networks, a latest domain introduced called internet of Things (IoT). Currently, the IoT is introducing new research areas and industrial revolutions. Its new advancements produce new challenging domains for research community. The IoT can be described as the pervasive and global network that assists and provides a system for monitoring and controlling the physical world with the IoT sensors devices that collect, process, and analyze the generated data. These devices have built-in interfaces to sense and communicate such as sensors, radio frequency identification devices (RFID), Global Positioning Devices (GPS), infrared sensors, laser scanners, actuators, wireless LANs and even Local Area Networks (LANs) interfaces. The smart health system is the domain to continuously monitor the patient's health and in the case of any emergency diagnose the patient. The existing works include many developed systems to monitor patient's health. These systems face vulnerable threats from intruders due to wireless connectivity. There are so many threats by attackers that can endanger these systems. These attacks include Denial of Service Attack, Fingerprint and Timing-based Snooping, Router Attack, Select and Forwarding attack, Sensor attack and Replay Attack. In this paper, we describe these attacks and their impact on health monitoring systems.

II. Literature Work

Internet of Things (IoT) definition is, it allows people and things to be connected with anything, with any network use, from anywhere, any time and anyone to transmit information and data. Everything in the world is becoming connected with others globally due to use of internet. Due to smart things (objects) such as sensor device, mobiles, smart gadgets, wearable devices and Laptop, the environment is becoming smart worldwide such as smart cities, smart industries, smart homes, smart health systems, high mobility devices, and high network flexibility as shown in figure.1. The reason is, over the last 15-20 years the devices are becoming cheap, available and tiny that enabling automation in every aspect of life with internet connectivity [1, 2]. Many researchers worked in IoT and point out that many evolutions have done in networks to make them more reliable, efficient, flexible and large in size for the next generation. They also highlight an alarming stage that the numbers of devices connected to the internet by the people are growing rapidly and can reach or over the 50 billion devices till 2020 [3, 4]. The number of devices will increase gradually with the passing of time. The advancement of the IoT must consider such issues as how to incorporate and interoperate unique networks and a large number of heterogeneous sensor devices. Also, the communication requirements to support IoT are remarkably not

978-1-7281-2847-4/19/$31.00 ©2019 IEEE
DOI 10.1109/ICCSA.2019.000-8

quite the same as present systems as far as different types and sizes of data or information, a variety of transmission capacity requirements from numerous applications and unfathomably unique levels of time and error resistance. The remote connectivity is making the world smart as smart cities mentioned below in Figure.1. From all these remote connection concepts the health is the most important domain to focus because it relates to human life. Due to many sensors attached to the IoT rise serious security threats in the form of attacks that can be internal and external and can affect health monitoring [5, 6].

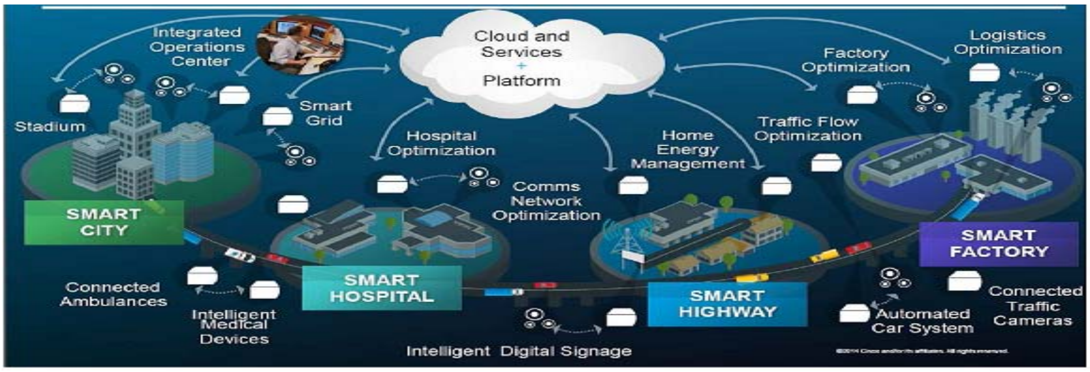

Fig.1 IoT Smart Cities Concept [1]

III. Health Monitoring Scenario

For the smart health monitoring system development, following four steps are required to be followed: (i) complete knowledge to abstract information from intelligent things connected with network, (ii) maintenance and transmission of data, (iii) intelligent processing and decision making by the system, and (iv) securing from vulnerabilities. An example scenario of smart health monitoring is shown in Fig.3. The given scenario is smart watch application to monitor patient heart beat. Objects are interconnected with each other such as laptop connected to smartphone, smartphone connected to heart rate monitor etc. The intruder can easily threat the laptop and can get access to heart rate monitor [24].

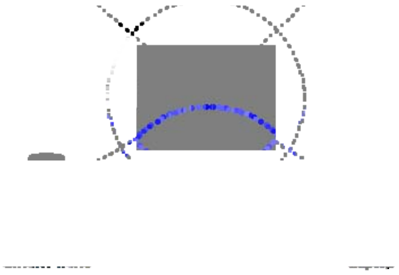

Fig.3 Smart Health Monitoring Scenario

IV. Security Attacks to Smart Health Systemss

Health care sensors are foreseen that would manage vital private information and individual medical services data. Likewise, such smart sensors may be associated with overall information applications for their access to anytime and anywhere. To empower the full use of IoT in the medical health care domain, it is necessary to recognize and examine specific qualities of IoT including security necessities, vulnerabilities, and countermeasures, from the human health care perspective. In different security threats to health care, the attackers try to (i) steal information of the patient (ii) deny the services of the system, and update data. There are two types of attackers in IoT Health systems (i) Internal Attackers, and (ii) External Attackers. **Internal Attackers** exist inside the system and perform malicious activities silently. The detection of the attacker is quite easy due to its existence within the system. **External Attackers** exist outside the system and perform malicious activities. The detection of the attacker is quite difficult due to its existence out from the system. It silently examines the system operations and then performs malicious activities as shown below in Figure.3 [6, 7].

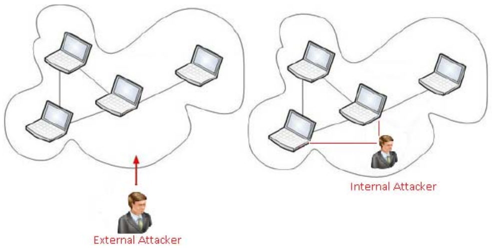

Fig.3 Internal and External Attackers.

V. Taxonomy of Attacks

There are mainly two kinds of attack in eHealth enviroment such as routng attack and locaiton baesd attack. Routing attacks include router attack, select and forwarding attack and replay attack. Location based attack include denial of service attack, finger and timing-based snooping attack and sensor attack. In the routing attacks mostly the intruders targets the route of data to send or drop data packets. In the locaiton based attack mostly the intruders attacks on the destination node to deny the services of the system. Experts systems are also very benificial for identifying and overcomming dengue fever[26], managing private information and individual medical services data is also a challenging task here. As shown below in Figure.4 the hierarrchical structure of the categorizes [23, 25].

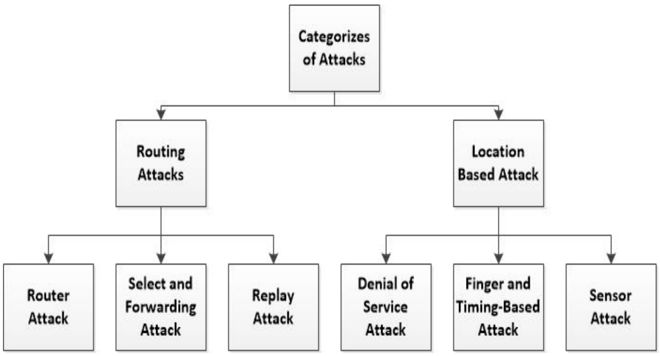

Fig. 4 Categories of Attack in Smart Health Systems.

A. Denial of Service Attack (DoS)

In Denial of service attack, the attacker over-burdens the system's data transmission with unknown traffic, which makes resources inaccessible for others, because other nodes won't be capable to send their information after sensing the busy channel. In the Denial of service attack, the attacker ordinarily exploit the NAV behavior by tempera portion of the flags in control frames. In the IEEE 802.11 standard, the nodes don't counter check every one of the flags in control frames; therefore, it is difficult to detect such kind of attack [8, 9]. In the Denial of service attack, the patient data can be accessed without the authentication and permission of access to data. The Denial of service attack also makes the system channel of data busy so that no other information can pass to any other sensor in the network. The Denial of service attacks to cause transmission of data between nodes connects to be lost or inaccessible. This type of attack undermines system or health care services accessibility, network functionality, and sensors obligation. In the Denial of service attack, the attacker can temper the data of the patient, mislead the receivers about the patient's information, can send false information of a patient, and can add false information of a patient and an adversary replays existing messages to threaten message freshness. These all threats of DoS attack can lead to false treatment, a false status of a patient and a false emergency call to any specific people. The modification of data can cause patient death. The DoS attack mostly occurs on each layer of the network and performed different threats [10, 21, 27].

B. Fingerprint and Timing-based Snooping (FATS)

The wireless network is unable to detect the new security threats that get information from examining the data transmission sensor to sensor, sensor to private location when the transmission is encrypted. This physical layer threat just requires broadcast time and finger print of every message, where a fingerprint is a set of features of an RF waveform that are exceptional to a specific transmitter. This kind of attack is called a fingerprint and timing based snooping (FATS) attack. To mitigate this attack, an intruder listens silently all sensors' data transmission with timestamps and finger prints. After observing this, the intruder uses the fingerprint to attach with every message to a specific transmitter and utilizes different times of deduction for every sensor location. When the intruder can get this information and can disrupt the health conditions [4, 12].

C. Router Attack

The routing of data is important for health care based systems in the light of the fact that it permits remote information delivery and it encourages network versatility in huge hospitals. Nonetheless, routing involves a few issues, primarily because of the open nature of wireless systems. In this attack the attacker attacks on the information that is routing between the sensors in a wireless sensor network. This is due to in a health care systems based on wireless the most essential requirement is the protected delivery of patient information at the receiving end that can be doctor and hospital. In this assault steering of fundamental and vital information showing human services status of the patients is considered, there are incredibly scarcely any applications that usage multi-trust directing. Multi-trust directing is basic in extending the incorporation district of the system subsequently giving flexibility at the expense of complexity. In addition, the level of being unremarkable and varies in applications as shown below in Figure.5 [13, 14].

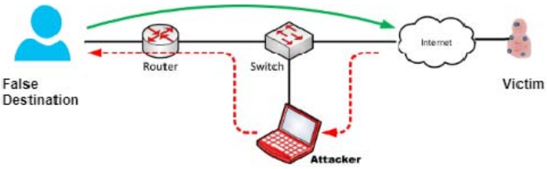

Fig.5 Routing Attack to Smart Health System.

D. Select Forwarding (SF) Attack

The selective forwarding threat is other type of black hole attack. In this threat the intruder gets access to single or multiple sensors to mitigate this attack. Therefore this is known as community-oriented specific forwarding. In this attack when the intruder gets access to any sensor then it drops the data packets and also send these packets to neighbor sensors to make it suspicion. This attack affects the system very badly, if the sensor is close to base station. In this way, because of packet drop from the SF attack, it tends to be hard to recognize the cause for packet drop. This attack can be harmful for any patient or smart medical health system by incomplete data reaching at the receiver end. This attack can be more harmful than no data. This is in light of the fact that in medical health terms one may not see the entire picture without complete information. The changed patient data might sent to the receiver end. This could result in the wrong treatment of the patient as shown in Figure.6 [11, 15].

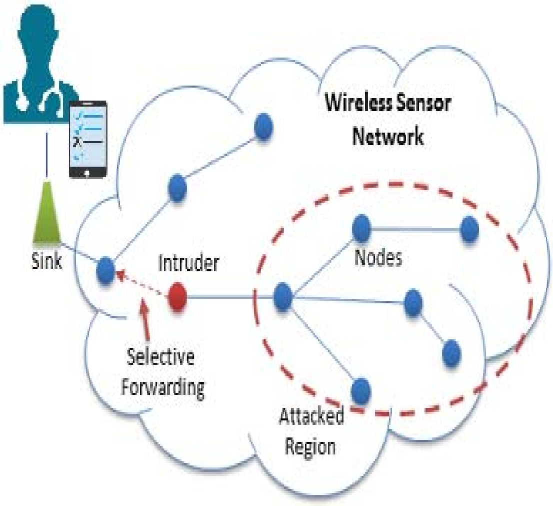

Fig.6 Select Forwarding Attack to Smart Health System.

E. Sensor Attack

Due to the accidental failure of sensors in the wireless network and the malicious activities performed by the external attackers, sensor frequently left or join the network. In the wireless network due to lack of power sensor may die. In this case, the smart attacker can easily replace the sensor with the real one and enter in the network, can perform malicious activities easily. Therefore, the patient data if not well places at multiple sensor then the attacker can change the data as far as intruder wants. Also, false data can be inserted or served as legal due to lack of authentication schema. Pietro et al tended to the information survival issue in wireless sensor systems. The attacker is thought to be alert of the beginnings of the objective information, and can negotiation a subset of sensor/nodes in every round as shown below in Figure.7 [16, 17, 22].

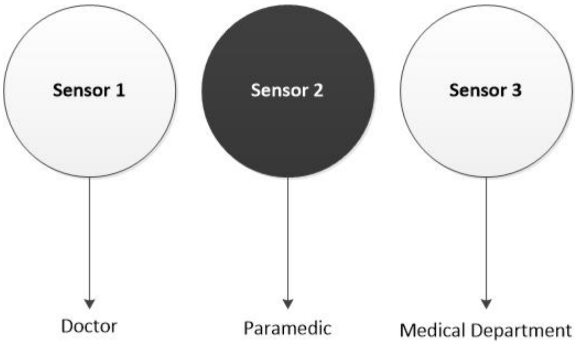

Fig.7 Sensor/Node Attack to Smart Health Application.

F. Replay Attack

A replay attack can mitigate when an intruder gets un-authorized access to system. The intruder examines the activities on system and then send message to receiver when the transmitter stops to send data at that point it start to send signal as first sender. The main objective of the intruder in this attack is to build trust in network. The attacker sends a message to receiver that is mostly use in the access process. [18]. A replay assault is portrayed as a rupture of security in which some data is stored with no authorization and afterward retransmitted to the receiver keeping in mind the end goal to trap the last into unauthorized, for example, false recognition or verification or a duplicate transaction [19, 20].

Every attack has some impact on the system in some way. The major effects on health monitoring system are un-Authorized access, Data modification, Denial of continuous monitoring, Change the route of data destination and Data drop. The Table. 1 provides the comparative analysis of different attacks in terms of effectiveness, security requirements as suggestive measures and approach [24].

TABLE I. COMPARITIVE ANALYSIS OF ATTACKS ON SMART HEALTH

Attack	**Effectiveness**	**Security Requirements**	**Approach**
Denial of Service	Disable system services	Early Intrusion detection	Distributed attack uses and deny the system' service.
Routing Attack	Change route Information	Continuous Route Monitoring	Change the routing table information and drop packet to own end.
Sensor Attack	Data modification	Node Failure and Replacement Detection	Attacker finds a sensor with low power or failure. Then replace the sensor and enter in network.

Replay Attack	Unauthorized access, duplicate transmission	Secure authorization	Evaluate the system activities then send message to receiver after completion of transmitter message.
Select forwardi-ng Attack	Drop data packets	Sensor detection	Intruder drops data packets at desire location by behave as destination end.
FATS	Malicious activities	Control the transmission	Attacker examines the all data traffic by sensor then attach fingerprint to every message to specific transmitter.

VI. Conclusion

The internet of things (IoT) is emerged with many research areas to make the global smart like smart cities, smart traffic, and smart health. In the smart health monitoring systems the update information about the patient's health is forwarded by sensors at a specific location with the objective to improve the health quality and secure the patient's life in an emergency situation. Many systems have developed to support the continuous monitoring of patient's health but it becomes quite difficult to maintain the continuously monitor due to some security threats by the attackers. In this paper, we comparatively analyze attacks with there effectiveness, approach and security requirements as suggestive measures to secure the system. These security threats impact on system like denial of system's services, data stealing, data update, change the data route and data drop. Therefore, it requires to adopt some security guidelines for system's design and development for secure health monitoring. Future of this research will focus on how a smart healthy monitoring system can be preventive from these kinds of attacks by mitigation of new security strategies to provide continuous monitoring of patient health.

ACKNOWLEDGMENT

This research work is supported and funded by Software Engineering, Communication & Network Lab (SECON), PIEAS University, Pakistan and Universidad De La Costa, Barranquilla Columbia.

References

[1]. Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L. (2017). IoT technologies for smart cities. *IET Networks*, *7*(1), 1-13.

[2]. Lee, A., Wang, X., Nguyen, H., & Ra, I. (2018). A Hybrid Software Defined Networking Architecture for Next-Generation IoTs. *KSII Transactions on Internet & Information Systems*, *12*(2).

[3]. Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for the internet of things: A survey. *Journal of Network and Computer Applications*, *66*, 198-213.

[4]. Banda, G., Bommakanti, C. K., & Mohan, H. (2016). One IoT: an IoT protocol and framework for OEMs to make IoT-enabled devices forward compatible. *Journal of Reliable Intelligent Environments*, *2*(3), 131-144.

[5]. Choi, S. K., Yang, C. H., & Kwak, J. (2018). System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats. *KSII Transactions on Internet & Information Systems*, *12*(2).

[6]. Mathur, A., Newe, T., & Rao, M. (2016). Defence against the black hole and selective forwarding attacks for medical WSNs in the IoT. *Sensors*, *16*(1), 118.

[7]. Kavita, M. E. G., & Bala, A. P. K. (2018). Security and Privacy Issues in EHR Systems Towards Trusted Services.

[8]. Jamal, T., Amaral, P., Khan, A., Zameer, A., Ullah, K., & Butt, S. A. (2018). Denial of Service Attack in Wireless LAN. *ICDS 2018*, 51.

[9]. Gope, P., & Hwang, T. (2016). BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sensors Journal*, *16*(5), 1368-1376.

[10]. Ünsal, E., & Çebi, Y. (2013, January). DENIAL OF SERVICE ATTACKS IN WSN. In *International Symposium on Computing in Science & Engineering. Proceedings* (p. 24). GEDIZ University, Engineering and Architecture Faculty.

[11]. Babu, M. R., Dian, S. M., Chelladurai, S., & Palaniappan, M. (2015). Proactive alleviation procedure to handle black hole attack and its version. *The Scientific World Journal*, *2015*.

[12]. Reinbrecht, C., Susin, A., Bossuet, L., Sigl, G., & Sepúlveda, J. (2017). Timing attack on NoC-based systems: Prime+ Probe attack and NoC-based protection. *Microprocessors and Microsystems*, *52*, 556-565.

[13]. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. *IEEE Access*, *3*, 678-708.

[14]. Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. *IEEE Access*, *3*, 678-708.

[15]. Niksaz, P., & Branch, M. (2015). Wireless body area networks: attacks and countermeasures. *Int. J. Sci. Eng. Res*, *6*(9), 556-568.

[16]. Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, *17*(1).

[17]. Aliberti, G., Di Pietro, R., & Guarino, S. (2017). Epidemic data survivability in Unattended Wireless Sensor Networks: New models and results. *Journal of Network and Computer Applications*, *99*, 146-165..

[18]. Behrooz, S., & Marsh, S. (2016, July). A trust-based framework for information sharing between mobile health care applications. In *IFIP International Conference on Trust Management* (pp. 79-95). Springer, Cham..

[19]. Rughoobur, P., & Nagowah, L. (2017, December). A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In *Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), 2017 International Conference on* (pp. 811-817). IEEE.

[20].T. Jamal, and SA Butt, “Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations”, In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.

[21]. Jamal, T., & Butt, S. A. (2018). Malicious node analysis in MANETS. *International Journal of Information Technology*, 1-9.

[22].SA Butt, and T. Jamal, “Study of Black Hole Attack in AODV”, in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.

[23]. Kumar, P., & Lee, H. J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. *sensors*, *12*(1), 55-91.

[24]. Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016, August). Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd International Conference on Electronic Design (ICED)* (pp. 321-326). IEEE.

[25].T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[26]. Ahmed, N., Ishaq, A., Shoaib, M., & Wahab, A. (2017). Role of Expert Systems in Identification and Overcoming of Dengue Fever. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 8(10), 82-89.

[27]. T. Jamal and Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. arXiv:1810.11070 [cs.NI], Oct. 2018.