Engineering Universe for scientific Research and management
ISSN (Online): 2319-3069
Vol. XIII Issue VIII
August 2021

A REVIEW ON SECURITY AND PRIVACY ISSUES WITH IOT IN HEALTHCARE NETWORK

Shilpi Raghuwanshi[1], Chinmay Bhatt[2], Bharti Chourasia[3]
SRK University, Bhopal, India[1, 2, 3]
shilpiraghu38@gmail.com[1], chinmay20june@gmail.com[2], varsha_namdeo@yahoo.com[3]

ABSTRACT: In medical services, the Internet of Things (IoT) offers many advantages, including having the option to screen patients all the more intently and utilizing information for investigation. With regards to IoT for clinical gadget combination, the center is moved towards the customer end, for example, glucose meters, circulatory strain sleeves, and different gadgets intended to record information on understanding crucial signs. This empowers medical care suppliers to naturally gather data and apply choice help rules to consider prior mediation in the therapy cycle. Lamentably, clinical organizations frequently don't consider the security dangers of interfacing these gadgets to the web. There is plausible that a zero-day exploit in a clinical gadget can be utilized to harm or even kill somebody without being distinguished. The ascent in hackable clinical gadgets has constrained the FDA to give formal direction on how clinical gadget creators should deal with reports about digital weaknesses. This paper intends to investigate the job of IoT in medical care, weaknesses, assaults, and security issues and arrangements.

KEYWORDS: Internet of things, health care, services, applications, networks, security.

1. INTRODUCTION

The Internet of Things (IoT) is a concept reflecting a connected set of anyone, anything, anytime, anyplace, any service, and any network. The IoT is megatrends in next-generation technologies that can impact the whole business spectrum and can be thought of as the interconnection of uniquely identifyable smart objects and devices within today's internet infrastructure with extended benefits. Benefits typically include the advanced connectivity of these devices, systems, and services that go beyond machine to machine (M2M) scenarios [1]. Therefore, introducing automation is conceivable in nearly every field. The IoT provides appropriate solutions for a wide range of applications such as smart cities, traffic congestion, waste management, structural health, security, emergency services, logistics, retails, industrial control, and health care. The interested reader is referred to [1] [5] for a deeper understanding of the IoT.

Medical care and health care represent one of the most attractive application areas for the IoT [6]. The IoT has the potential to give rise to many medical applications such as remote health monitoring, fitness programs, chronic diseases, and elderly care. Compliance with treatment and medication at home and by healthcare providers is another important potential application. Therefore, various medical devices, sensors, and diagnostic and imaging devices can be viewed as smart devices or objects constituting a core part of the IoT. IoT-based healthcare services are expected to reduce costs, increase the quality of life, and enrich the user's experience. From the perspective of healthcare providers, the IoT has the potential to reduce device downtime through remote provision. In addition, the IoT can correctly identify optimum times for replenishing supplies for various devices for their smooth and continuous operation. Further, the IoT provides for the efficient scheduling of limited resources by ensuring their best use and service of more patients. Fig. 1 illustrates recent healthcare trends [7]. Ease of cost-effective interactions through seamless and secure connectivity across individual patients, clinics, and healthcare organizations is an important trend. Up-to-date healthcare networks driven by wireless technologies are expected to support chronic diseases, early diagnosis, real-time monitoring, and medical emergencies. Gateways, medical servers, and health databases play vital roles

in creating health records and delivering on-demand health services to authorized stakeholders.

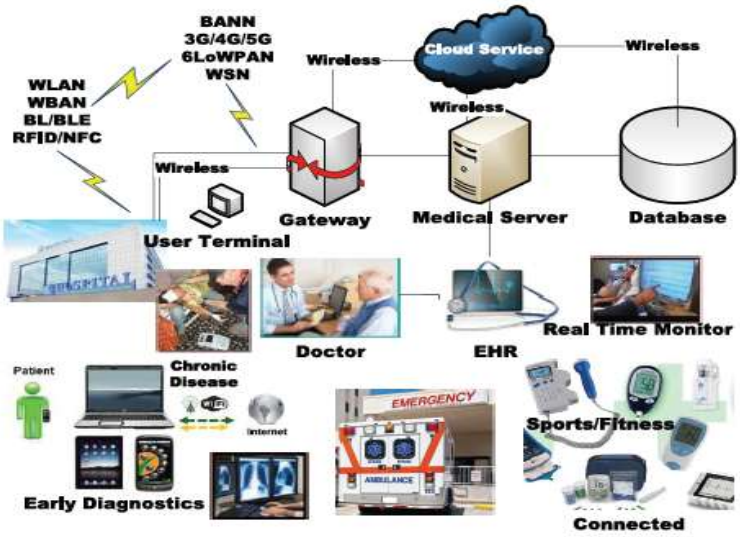

Fig. 1: Healthcare trends.

In the last few years, this field has attracted wide attention from researchers to address the potential of the IoT in the healthcare field by considering various practical challenges. As a consequence, there are now numerous applications, services, and prototypes in the field. Research trends in IoT-based health care include network architectures and platforms, new services and applications, interoperability, and security, among others. In addition, policies and guidelines have been developed for deploying the IoT technology in the medical field in many countries and organizations across the world. However, the IoT remains in its infancy in the healthcare field. At this stage, a thorough understanding of current research on the IoT in the healthcare context is expected to be useful for various stakeholders interested in further research. This paper examines the trends in IoT-based healthcare research and uncovers various issues that must be addressed to transform healthcare technologies through the IoT innovation.

2. THE ROLE OF IOT IN HEALTHCARE

Healthcare is defined as the act of taking preventative or necessary procedures to improve a person's well-being. This may be done with surgery, the administering of medicine, or other alterations in a person's lifestyle. These services are typically offered through a health care system made up of hospitals and physicians. There are several areas in healthcare that IoT is playing an important role.

- Elder care, which involves tracking elderly residence/patients at nursing home and hospital
- Data gathering, which is the most mature area in healthcare, it involves many equipment that we see at bedside in hospitals like the EKG monitor, this is an area that continues to expand with new innovations happening in the world of IoT
- Real-time location is used to track people and assets at a lower cost

As the presence of IoT in the healthcare sector increases, it is going to benefit both patients and healthcare providers. Treatments that patients receive can be enhanced by remote monitoring and communication, areas where IoT can play a big role.

Another use of healthcare IoT is mobile medical applications or wearable devices that allow patients to capture their health data. Much of this can be attributed to the data revolution which is empowering us to live healthier lives by using connected devices such as tablets, wearable and hand-held devices. The analysis of the data collected through electronic medical records, diagnostic information gathered through imaging equipment and hand-held personal devices will enhance the decision-making powers. This will allow patients to take a more active role in managing their personal health.

In the future, this data-rich personalized analysis of our health will become the standard. Patients will be provided with tailor-made strategies to fight illness.

From the data generated, we will learn how to improve our wellbeing and we will be motivated to take control of our life. There is a whole new industry around clinical decision support software, a growing sector related to IoT that boosts the role of connected devices by tying their use more directly to clinical decisions.

The Food and Drug Administration (FDA) has already done quite a bit of work in establishing universal device identifiers for medical devices in IoT applications. There should be tagging of the metadata generated by connected devices that would allow data to be closely tracked as it travels between devices or between devices and networks. Doctors do not have to wonder about the data. They will be able to trust this data and will know that it is really from their patient. The Healthcare sector remains one of the fastest to adopt the Internet of Things. Integrating IoT features into medical devices improves the quality and effectiveness of service rendered, this is very valuable for patients who have chronic conditions, the elderly, and those requiring constant care. According to a study conducted by McKinsey Global Institute, spending on the Healthcare IoT solutions will reach $1 trillion by 2025 (see Fig.2). It is possible that this could set the stage for highly personalized, accessible, and on-time healthcare services for everyone.

Fig. 2: Economic impact of IoT Devices by 2025

Hospitals have been adopting the Internet of Things for many years. It is very common to see IoT devices in patient rooms, electronic medical records and other cloud-based resources. At most healthcare organizations networking new devices is an ongoing initiative. However, the biggest challenge is the interoperability of devices which can lead to a network being exposed to new security vulnerabilities and additional risk.

The BYOD devices are a potential issue, without proper monitoring they can very easily become part of a network and represent an immense target for attack. Since it is difficult to control the quality of the operating systems or the code that runs on these devices, organizations must monitor the use of these devices, log when they access or extract data. As healthcare systems become interconnected, especially as numerous wireless medical devices start connecting to web-enabled IT systems they become increasingly vulnerable. This vulnerability is not just from malicious hackers, but from other threats such as malware and the computer virus.

3. IOT HEALTHCARE SECURITY

The IoT is growing rapidly. In the next several years, the medical sector is expected to witness the widespread adoption of the IoT and flourish through new eHealth IoT devices and applications. Healthcare devices and applications are expected to deal with vital private information such as personal healthcare data. In addition, such smart devices may be connected to global information networks for their access anytime, anywhere. Therefore, the IoT healthcare domain may be a target of attackers. To facilitate the full adoption of the IoT in the healthcare domain, it is critical to identify and analyze distinct features of IoT security and privacy, including security requirements, vulnerabilities, threat models, and countermeasures, from the healthcare perspective (Fig. 3).

A. SECURITY REQUIREMENTS

Security requirements for IoT-based healthcare solutions are similar to those in standard communications scenarios.

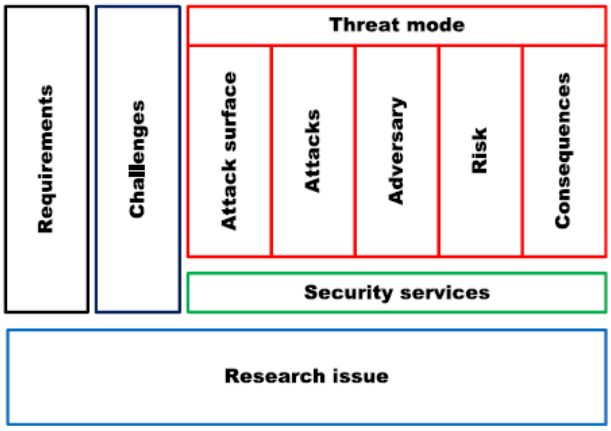

Fig. 3: Security issues in IoT-based health care.

Therefore, to achieve secure services, there is a need to focus on the following security requirements.

1) CONFIDENTIALITY

Confidentiality ensures the inaccessibility of medical information for unauthorized users. In addition, confidential messages resist revealing their content to eavesdroppers.

2) INTEGRITY

Integrity ensures that received medical data are not altered in transit by an adversary. In addition, the integrity of stored data and content should not be compromised.

3) AUTHENTICATION

Authentication enables an IoT health device to ensure the identity of the peer with which it is communicating.

4) AVAILABILITY

Availability ensures the survivability of IoT healthcare services (either local or global/cloud services) to authorized parties when needed even under denial-of-service attacks.

5) DATA FRESHNESS

Data freshness includes data freshness and key freshness. Because each IoT healthcare network provides some time varying measurements, there is a need to ensure that each message is fresh. Data freshness basically implies that each data set is recent and ensures that no adversary replays old messages.

6) NON-REPUDIATION

Non-repudiation indicates that a node cannot deny sending a message sent earlier.

7) AUTHORIZATION

Authorization ensures that only authorized nodes are accessible for network services or resources.

8) RESILIENCY

If some interconnected health devices are compromised, then a security scheme should still protect the network/ device/information from any attack.

9) FAULT TOLERANCE

A security scheme should continue to provide respective security services even in the presence of a fault (e.g., a software glitch, a device compromise, and a device failure).

10) SELF-HEALING

A medical device in an IoT healthcare network may fail or run out of energy. Then remaining or collaborating devices should enable a minimum level of security.

B. SECURITY CHALLENGES

Because IoT security requirements are not ensured by traditional security techniques, novel countermeasures are needed to address new challenges posed by the IoT. Challenges for secure IoT healthcare services include.

1) COMPUTATIONAL LIMITATIONS

IoT health devices are embedded with low-speed processors. The central processing unit (CPU) in such devices is not very powerful in terms of its speed. In addition, these devices are not designed to perform computationally expensive operations. That is, they simply act as a sensor or actuator. Therefore, finding a security solution that minimizes resource consumption and thus maximizes security performance is a challenging task.

2) MEMORY LIMITATIONS

Most IoT healthcare devices have low on-device memory. Such devices are activated using an embedded operating system (OS), system software, and an application binary. Therefore, their memory may not be sufficient to execute complicated security protocols.

3) ENERGY LIMITATIONS

A typical IoT healthcare network includes small health devices of limited battery power (e.g., body temperature and BP sensors). Such devices conserve energy by switching on the power-saving mode when no sensor reading needs to be reported. In addition, they operate at a low CPU speed if there is nothing important to be processed. Therefore, the energy constraint property of IoT health devices makes finding an energy-aware security solution challenging.

4) MOBILITY

In general, healthcare devices are not static but mobile in nature. Such devices are connected to the Internet through IoT service providers. For example, a wearable body temperature sensor or a heart monitor may be connected to the Internet and notifies the concerned caregiver of the user's conditions. Such wearable's are connected to the home network when the user is at home, whereas they are connected to the ofce network when he or she is at ofce. Different networks have different security configurations and

settings. Therefore, developing a mobility-compliant security algorithm is a serious challenge.

5) SCALABILITY

The number of IoT devices has increased gradually, and therefore more devices are getting connected to the global information network. Therefore, designing a highly scalable security scheme without compromising security requirements becomes a challenging task.

6) COMMUNICATIONS MEDIA

In general, health devices are connected to both local and global networks through a wide range of wireless links such as Zigbee, Z-Wave, Bluetooth, Bluetooth Low Energy, WiFi, GSM, WiMax, and 3G/4G. Wireless channel characteristics of these networks make traditional wired security schemes less appropriate. Therefore, it is difcult to find a comprehensive security protocol that can treat both wired and wireless channel characteristics equally.

7) THE MULTIPLICITY OF DEVICES

Health devices within an IoT health network are diverse, ranging from full-edged PCs to low-end RFID tags. Such devices vary according to their capability in terms of their computation, power, memory, and embedded software. Therefore, the challenge lies in designing a security scheme that can accommodate even the simplest of devices.

8) A DYNAMIC NETWORK TOPOLOGY

A health device may join an IoT health network anywhere, anytime. In addition, it can leave a network either gracefully (with proper exit notification) or disgracefully (abruptly). Temporal and spatial admission characteristics of medical devices make the network topology dynamic. Therefore, devising a security model for this type of dynamic network topology is a difcult challenge.

9) A MULTI-PROTOCOL NETWORK

A health device may communicate with other devices in the local network through a proprietary network protocol. In addition, the same IoT device may communicate with IoT service providers over the IP network. Therefore, security specialists find it difficult to devise a sound security solution for multi-protocol communications.

10) DYNAMIC SECURITY UPDATES

To mitigate potential vulnerabilities, there is a need to keep security protocols up-to-date. Therefore, updated security patches are needed for IoT health devices. However, designing a mechanism for the dynamic installation of security patches is a challenging task.

11) TAMPER-RESISTANT PACKAGES

Physical security is an important part of IoT health devices. An attacker may tamper with devices and then may later extract cryptographic secrets, modify programs, or replace those with malicious nodes. Tamper-resistant packaging is a way to defend against such attacks, but it is challenging to implement in practice.

4. CONCLUSION

So far, there are no known cases in which malicious hackers have attacked a pacemaker, but researchers have proved it's possible. In addition, research firm Forrester has predicted that in the near future we will see ransomware for a medical device or wearable. The systems those devices connect to in hospitals often have a lot of legacy equipment that are running outdated operating systems and software that cannot be updated. In the transient environment of a healthcare provider devices can enter in many ways, many times how they enter are unknown, BYOD is a good example.

When this happens, it becomes difficult to figure out the life cycle management of that device and identify the operating system. Standalone devices that attach to the network may have developed networks and connectivity glitches. Since these devices do not come through normal channels there is a lack of awareness of these vulnerabilities that attackers could take advantage. When a vendor, rogue IT staff member or even a hacker can put standalone devices on an isolated network many of these devices in healthcare lack evidence capture and forensic logging capabilities; therefore there is no way to track what is happening.

It is understood that IoT devices are her to stay because they help cut cost and make it easier to perform important functions. It is important to make sure that the networks run automated work flows, give quick access to critical information while keep everything secure. This can be accomplished with enforceable security policies and implementing solutions that focus on vulnerabilities, configuration assessments, malware defenses, as well as activity and event monitoring.

REFERENCES

[1] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Amsterdam, The Netherlands: Elsevier, 2014.

[2] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, ``Smart objects as building blocks for the Internet of Things," IEEE Internet Comput., vol. 14, no. 1, pp. 4451, Jan./Feb. 2010.

[3] K. Romer, B. Ostermaier, F. Mattern, M. Fahrmair, and W. Kellerer, ``Real-time search for real-world entities: A survey," Proc. IEEE, vol. 98, no. 11, pp. 18871902, Nov. 2010.

[4] D. Guinard, V. Trifa, and E. Wilde, ``A resource oriented architecture for the Web of Things," in Proc. Internet Things (IOT), Nov./Dec. 2010, pp. 18.

[5] L. Tan and N. Wang, ``Future Internet: The Internet of Things," in Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE), vol. 5. Aug. 2010, pp. V5-376V5-380.

[6] Z. Pang, ``Technologies and architectures of the Internet-of-Things (IoT) for health and well-being," M.S. thesis, Dept. Electron. Comput. Syst., KTH-Roy. Inst. Technol., Stockholm, Sweden, Jan. 2013.

[7] K. Vasanth and J. Sbert. Creating solutions for health through technology innovation. Texas Instruments. [Online]. Available: http://www.ti.com/lit/wp/sszy006/sszy006.pdf, accessed Dec. 7, 2014.

[8] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, ``Wireless sensor networks for healthcare," Proc. IEEE, vol. 98, no. 11, pp. 19471960, Nov. 2010.

[9] H. Alemdar and C. Ersoy, ``Wireless sensor networks for healthcare: A survey," Comput. Netw., vol. 54, no. 15, pp. 26882710, Oct. 2010.

[10] L. Mainetti, L. Patrono, and A. Vilei, ``Evolution of wireless sensor networks towards the Internet of Things: A survey," in Proc. 19th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM), Sep. 2011, pp. 16.

[11] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, ``Wireless sensor networks and the Internet of Things: Selected challenges," in Proc. 8th GI/ITG KuVS Fachgespräch `Drahtlose Sensornetze', Aug. 2009, pp. 3134.

[12] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, ``Wireless sensor networks and the Internet of Things: Do we need a complete integration?" in Proc. 1st Int. Workshop Security Internet Things (SecIoT), Nov. 2010.

[13] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, ``IOT gateway: Bridging wireless sensor networks into Internet of Things," in Proc. IEEE/IFIP 8th Int. Conf. Embedded Ubiquitous Comput. (EUC), Dec. 2010, pp. 347352.

[14] I. Gronbaek, ``Architecture for the Internet of Things (IoT): API and interconnect," in Proc. Int. Conf. Sensor Technol. Appl., Aug. 2008, pp. 802807.

[15] H. Viswanathan, E. K. Lee, and D. Pompili, ``Mobile grid computing for data- and patient-centric ubiquitous healthcare," in Proc. 1st IEEE Workshop Enabling Technol. Smartphone Internet Things (ETSIoT), Jun. 2012, pp. 3641.

[16] W. Zhao,W. Chaowei, and Y. Nakahira, ``Medical application on Internet of Things," in Proc. IET Int. Conf. Commun. Technol. Appl. (ICCTA), Oct. 2011, pp. 660665.

[17] N. Yang, X. Zhao, and H. Zhang, ``A non-contact health monitoring model based on the Internet of Things," in Proc. 8th Int. Conf. Natural Comput. (ICNC), May 2012, pp. 506510.

[18] S. Imadali, A. Karanasiou, A. Petrescu, I. Sifniadis, V. Veque, and P. Angelidis, ``eHealth service support in IPv6 vehicular networks," in Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob), Oct. 2012, pp. 579585.

[19] R. S. H. Istepanian, ``The potential of Internet of Things (IoT) for assisted living applications," in Proc. IET Seminar Assist. Living, Apr. 2011,pp. 140.

[20] G. Yang et al., ``A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 21802191, Nov. 2014.

[21] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, ``Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of Things," in Proc. IEEE Int. Conf. Trust, Security Privacy Comput. Commun. (TrustCom), Jun. 2012, pp. 18111818.

[22] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, ``Ubiquitous data accessing method in IoT-based information system for emergency medical services," IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 15781586, May 2014.