Security of connected healthcare devices

Jasvindir Singh
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
jas9199@live.com

Vinesha Selvarajah
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
vinesha@apu.edu.my

Chandra Reka Ramachandiran
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
chandra.reka@apu.edu.my

***Abstract*—The healthcare industry is evolving at a rapid pace. Through the development of newer technologies, patientcare is improving and is currently the best it has ever been. However, the rapid growth of this industry has led to the development of numerous medical devices that only prioritize functionality. Disregarding other aspects such as security and privacy, these devices are easy targets for hackers, and pose a major risk to patients' well-being. In this paper, we discuss several security issues and challenges faced by medical device manufacturers, as well as several proposed techniques to mitigate these flaws.**

Keywords—security, privacy, healthcare, IoT, blockchain

I. INTRODUCTION

The healthcare industry is one of the largest and fastest-growing industries worldwide [1]. It is composed of subsectors that primarily deal with four responsibilities – prevention, diagnosis, treatment, and rehabilitation of medical conditions. The healthcare industry is constantly faced with numerous risks and challenges, as it is an industry that requires constant innovation and improvement while dealing with increased and tighter regulations. Modern healthcare increasingly relies on technology that is networked. This modernization is good for patient care, as it facilitates data integration, patient engagement, and clinical support. However, these technologies are often vulnerable to cyberattacks and bring about numerous risks to the patient and healthcare provider. Patient data is at risk of being stolen, connected devices may be hijacked for other purposes and may even be at risk for ransomware attacks. An example of such incidents is the WannaCry attack against the United Kingdom's National Healthcare Service in 2017, where thousands of hospital computers and diagnostic equipment was hijacked by ransomware. The healthcare industry is plagued by a myriad of cybersecurity risks.

II. SECURITY ISSUES AND CHALLENGES

The number of medical devices connected to the Internet is growing and to accomplish a strong security and privacy system for these devices is becoming increasingly difficult. Due to the sensitivity of data in the health sector, the lack of adequate security and privacy not only puts patients' privacy at risk but may also involve their very livelihood. As a rapidly growing and newer industry, healthcare manufacturers rapidly adapt solutions without regard to security ramifications [15]. This inevitably leads to the rise of new security issues regarding confidentiality, integrity, and availability. Healthcare devices contain sensitive information and can always be connected to the internet, thus making these devices a prime target for attackers.

Newaz et al. [1] presented an overview of the existing security and privacy research in healthcare systems. According to their research, there are multiple trends that are emerging in the growth of healthcare device applications. Such trends include the rise in functional complexity, increased programmability in included software, and the general growth of wireless network connectivity in healthcare devices. However, these rise in trends also bring about increased vulnerability with regards to security and privacy. A discussion by Qadri et al. [2] has broadly classified the security level of a network into three key factors: confidentiality, integrity, and availability. A typical 3-tier architecture of healthcare-based devices and services include a processing layer, a transmission layer, and a device layer. The device layer essentially consists of wearables that measure body parameters such as blood pressure or blood glucose levels. These sensors then send the data via the device through the transmission layer, which connects the nodes to the processing layer. At the processing layer, the received data is analyzed and stored for further use. Newaz et al. [1] has included a comprehensive list of attacks to healthcare devices and applications:

TABLE I. LIST OF ATTACKS TO HEALTHCARE DEVICES AND APPLICATIONS

Attacks	Attack Type	Target Medical Devices	Target Component
Hardware	Hardware Trojans	Active Therapeutic Devices	Sensor
Software	Malware	Active Therapeutic Devices	Device, Data, Healthcare provider
	Ransomware	Active Therapeutic Devices	Data, Healthcare provider
	Outdated Operating Systems	Active Therapeutic Devices	Device, Data, Healthcare provider
	Electroencepha -lography (EEG)	Non-invasive Devices	Device
	Counterfeit Firmware Update	Invasive Devices, Non-invasive Devices	Data, Healthcare provider
System-level	Weak Authentication Schemes exploitations	Invasive Devices, Non-invasive Devices, Active Therapeutic Devices	Device, Data, Healthcare provider
	Privilege Escalation	Invasive Devices	Device, Data
Side-channel	Electromagnetic Interference	*Invasive Devices*	Sensor
	Sensor Spoofing	Invasive Devices	Sensor
	Differential Power Analysis	Non-invasive Devices	Device
Communication Channel	Eavesdropping	Invasive Devices, Non-invasive Devices	Network
	Replay	Non-invasive Devices	Network
	Impersonation	Non-invasive Devices	Network
	Denial-of-service	Invasive Devices, Non-invasive Devices, Active Therapeutic Devices	Network
	Multiple Input and Multiple Output	*Invasive Devices*	Device
	Man-in-the-middle	Invasive Devices, Non-invasive Devices	Network
	Battery depletion	Invasive Devices, Non-invasive Devices	Device

Longras et al. [9] brings up a major concern regarding the devices used in healthcare today. They mention that these devices connect to the internet via computers running old versions of Windows XP. In such cases, using an older operating system would increase the vulnerability of these devices due to the extensive lists of exploitable vulnerabilities that can be easily found online. These devices can be easily found via search engines such as Shodan, leaving them exposed to brute-force attacks and attacks using hard-coded logins.

In addition, Jangid et al. [4] stress upon the security issues of automated healthcare devices. As a given example, the vulnerability of implantable pacemakers is discussed in brief. The connectivity of a device to the internet inevitably leads to an open port of attack for hackers. Devices that transmit radio signals can be breached via the transmitter itself. The inclusion of medical devices into the Internet of Things (IoT) increases the risk of compromise of said device. Cloud security may not be as secure as once thought and can compromise patient data and confidential information. [4] also includes possible workarounds to such scenarios, including the use of run-time verification and data encryption. [4],[5], and [9] stress the importance security in devices such as insulin pumps and pacemakers with regards to their link to the IoT today.

In the case of wearable sensors, additional security and address authentication will directly increase power consumption of medical devices. Since these sensors usually have small battery sizes, the security measures that are to be implemented must be adequate to accomplish its goals as well as to not hinder the performance of the device.

III. SECURITY AND PRIVACY GOALS

While improving technology can increase the overall quality of healthcare, the benefits must be weighed against the security and privacy concerns for the patient. Security and privacy goals have been thoroughly discussed in [1],[3] and have been summarized as below. The following properties must be considered throughout the lifecycle of the system:

A. Security goals:

1) Authentication: the process of verifying the identity of a user or process.

2) Confidentiality: protecting information from being accessed by unauthorized persons.

3) Integrity: ensuring that the information is not altered.

4) Non-repudiation: the assurance that someone cannot deny the validity of something

5) Availability: access to information by authorized users.

B. Privacy goals:

1) Device anonymity: hiding the identity of the device
2) Data anonymity: preventing unauthorized users from identifying the user and their data
3) Communication anonymity: preventing unauthorized users from identifying connections between the user and system
4) Unlinkability: preventing the relationship between data and sender to be traced

The introduction of laws such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) ensure the compliance of manufacturers to current standards for security and privacy with regards to healthcare devices. However, these laws are not strictly enforced and implemented during the development stages of new devices.

IV. PROPOSED MITIGATION TECHNIQUES

As suggested by [9], validation of security firmware installed on the device should be implemented to prevent unauthorized modification. The firmware must also be encrypted to prevent content decryption. Next, authentication processes can be improved by limiting the number of requests to the system. This would directly prevent system overloading and therefore prevent denial of service attacks. [9] also mentions the encryption of all communication packets, data integrity checking, anti-replay features, and usage restrictions. Implementation of a traffic monitoring system would enable the control of system logs, and monitoring power variations on devices.

Tawalbeh et al. [6] explains the use of blockchain in current IoT security models. The transactions may be represented using Merkle tree. Transactions are stored sequentially, and each have a cryptographic hash code which is stored in the leaf node. Contiguous leaf nodes are then concatenated, and new root hashes are generated until the final root hash is created and stored on the blockchain. Essentially, the application of blockchain in security is to guarantee data integrity. This paper also includes the usage of fog and edge computing environments for providing faster and more secure cloud services. The addition of security policies to these networking layers will indirectly enhance security frameworks in the IoT. This paper also suggests security not only on the device itself, but on the cloud layer. Network protocol between the edge nodes and sensors should be secured. Data spying can be reduced with the use of point-to-point encryption and certificates. [6] introduces the idea of using Amazon Web Service as a cloud computing platform for development of the necessary IoT tools.

The applications of blockchain in healthcare are further discussed by [8] and [10], where an example of such is the use of Patient Master Identifier (MPI). [10] introduces the idea of a Smart Healthcare System (SHS) which comprises of the following: Internet of Things, artificial intelligence, mobile and wearable devices, cloud computing, robotic surgeries, big data analytics, machine learning, and wireless sensor networks. The SHS itself is faced with its own set of challenges, namely system failure, malicious actions, human errors, supply chain issues, data availability, data and information security, energy consumption, patients privacy, billing and claims, and data ownership. They then introduce the Secured and Smart Healthcare System (S2HS) framework to mitigate the vulnerabilities of such systems. [14] also introduces a smart healthcare framework as a solution for security and privacy concerns for SHS.

[12] introduces the Threat identification, ontology-based Likelihood, severity Decomposition, and Risk integration (TLDR) methodology for information security risk assessment for medical devices. The methodology uses the following steps:

- Identifying the potential vulnerable components

- Identifying the potential attacks
- Mapping the discovered attacks
- Estimating the likelihood of the mapped attacks
- Computing the likelihood estimates of each attack
- Decomposing each attack into severity aspects and weighting them
- Assessing the magnitude of impact of each attack
- Computing the composite severity assessments for each attack
- Prioritizing the attack based on its risk

The paper concluded that ransomware attacks pose the highest risk for medical devices, followed by a disruption of patient-to-image linkage attack, and alteration of the imaging examination results. Jellen [7] proposes several approaches to increase security for medical devices:

TABLE II. APPROACHES TO INCREASE SECURITY FOR MEDICAL DEVICES

Security Solution	Approaches	Attacks Addressed
Biometric Approaches	Biometric authentication, key generation from biometrics	Eavesdropping, Man-in-the-middle
Distance / Proximity Based Approaches	Sound detection through piezoelectric element, Near Field Communication (NFC) tag	Eavesdropping, Replay
Key Management	Symmetric key cryptography, Public (asymmetric) key cryptography	Denial of service, Eavesdropping, Man-in-the-middle, Replay
Audit Mechanisms	Maintenance and alerting on device audit logs	Non-repudiation
Anomaly Detection	SVMs to classify network activities	Internal attacks, Resource depletion, Malicious communication
External device methods	IMD Guardian - external device using electrocardiogram signals, IMD Shield - full duplex radio device with receiver and jamming antenna, Cloaker - external device which shares master key to authenticate device and caregiver	Eavesdropping, Device capture
Lightweight encryption and key management techniques	Vibration-based key exchange protocols	Eavesdropping, Man-in-the-middle

[6] introduces deep learning-based security schemes for implantable medical devices. It applies the principle of the human brain where it tries to protect the body and applies this learning to securing cyberphysical systems. Deep learning is a subset of machine learning that learns from inherent patterns in data for solving a diverse set of problems. It is used to provide security at the sensor, communication, and application layers using novel techniques.

V. CONCLUSION

There is room for further research involving security of medical devices that can also secure the battery life of the device. Power consumption is directly linked with the level of security of the device, being that processor load is always dependant on the active processes running on the device. Alternative models that propose power replenishment with methods such as wireless charging may be a key factor in eliminating the drawbacks of power consumption on these devices.

A multitude of proposed mitigation techniques mostly focus on one major technique. There is a lack of research done that combines multiple techniques (i.e. blockchain and artificial intelligence) together to produce an effective framework. The combination of these techniques may yet provide increased coverage in terms of security. However, these untested techniques might not be without undiscovered security flaws.

Medical devices today increasingly depend on the use of wireless communications technology and the internet. Security of these devices must be of utmost priority during the development stages, only second to functionality. Focus must be placed on the secure encryption of patient data. Security and privacy are a significant concern; however, with limited resources available to these devices, implementing traditional security measures may prove impractical.

VI. LITERATURE REVIEW MATRIX

TABLE III. LITERATURE REVIEW MATRIX

Article	Scope	Outcomes	Limitations
A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac May 2020	A Survey on Security and Privacy Issues in Modern Healthcare Systems.	Side effects of increasing advancements in technology leads to increasingly vulnerable healthcare devices to security and privacy issues.	N/A
Y. A. Qadri, R. Ali, A. Musaddiq, F. Al-Turjman, D. W. Kim, and S. W. Kim Jan 2020	The limitations in the state-of-the-art countermeasures against the security threats in Healthcare-IoT.	Proposed framework for mitigating Selective Forwarding and Wormhole attacks in IoT systems.	Multiple limitations for specific counter measures are listed in the paper. Major limitations of H-IoT include latency and data integrity.
J. J. Hathaliya and S. Tanwar March 2020	An exhaustive survey on security and privacy issues in Healthcare 4.0	Multiple insights regarding security and privacy issues of Healthcare 4.0.	N/A
Jangid, P. K. Dubey, and B. R. Chandavarkar Jan 2020	Security issues and challenges in Healthcare Automated Devices	General solutions for IoT devices.	N/A

D. Zaldivar, L. A. Tawalbeh, and F. Muheidat Jan 2020	Investigating the Security Threats on Networked Medical Devices	Vulnerabilities of infusion pumps, insulin pumps, pacemakers discussed.	a. N/A
M. Tawalbeh, M. Quwaider, and L. A. Tawalbeh April 2020	Authorization Model for IoT Healthcare Systems: Case Study	Strength and weakness points for different block-chain models are shown and compared to a newer authorization model that improves upon previous points.	N/A
I. Jellen June 2020	TOWARDS SECURITY AND PRIVACY IN NETWORKED MEDICAL DEVICES AND ELECTRONIC HEALTHCARE SYSTEMS	Survey of current approaches to e-health security and privacy. Case study utilizing device classifications to implement improved security system.	- N/A
F. Alam Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid April 2020	Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development	Multiple proposed layers applicable to traditional blockchain, including precision medicine workflow	Does not discuss security of medical devices, only data.
A. Longras, H. Oliveira, and S. Paiva June 2020	Security Vulnerabilities on Implantable Medical Devices	Multiple vulnerabilities as well as modes of attack on implantable medical devices are given	- N/A
G. Tripathi, M. A. Ahad, and S. Paiva Nov 2019	S2HS- A blockchain based approach for smart healthcare system	Proposed smart healthcare system based on blockchain architecture	N/A
S. Selvaraj and S. Sundaravaradhan Dec 2019	Challenges and opportunities in IoT healthcare systems: a systematic review	Various research activities involved in the IoT based healthcare system are analysed.	N/A
T. Mahler, Y. Elovici, and Y. Shahar Feb 2020	A New Methodology for Information Security Risk Assessment for Medical Devices and Its Evaluation	Methodology for risk assessment of medical devices.	N/A
H. Rathore, A. Mohamed, and M. Guizani Jan 2020	Deep learning-based security schemes for implantable medical devices	Deep-learning algorithms for securing cyberphysical systems such as implantable medical devices.	N/A
Y. Lu and R. O. Sinnott Jan 2020	Security and privacy solutions for smart healthcare systems	Systematic evaluation of selected security and privacy solutions in s-health systems.	N/A
D. Sharma and R. C. Tripathi April 2020	Performance of Internet of Things (IOT) Based Healthcare Secure Services and Its Importance: Issue and Challenges	Trends in IoT-based health research and discover several problems that need to be addressed to transform health technologies through IoT innovation.	N/A
		Common healthcare security threats and data security issues are addressed.	

REFERENCES

[1] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses," arXiv:2005.07359 [cs], May 2020.

[2] Y. A. Qadri, R. Ali, A. Musaddiq, F. Al-Turjman, D. W. Kim, and S. W. Kim, "The limitations in the state-of-the-art counter-measures against the security threats in H-IoT," Cluster Computing, Jan. 2020.

[3] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," Computer Communications, vol. 153, pp. 311–335, Mar. 2020.

[4] A. Jangid, P. K. Dubey, and B. R. Chandavarkar, "Security issues and challenges in Healthcare Automated Devices," IEEE Xplore, 01-Jan-2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9027291.

[5] D. Zaldivar, L. A. Tawalbeh, and F. Muheidat, "Investigating the Security Threats on Networked Medical Devices," IEEE Xplore, 01-Jan-2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9031212.

[6] M. Tawalbeh, M. Quwaider, and L. A. Tawalbeh, "Authorization Model for IoT Healthcare Systems: Case Study," IEEE Xplore, 01-Apr-2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9078998.

[7] I. Jellen, "Towards Security and Privacy in Networked Medical Devices and Electronic Healthcare Systems," Master's Theses, Jun. 2020.

[8] F. Alam Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," Sustainable Cities and Society, vol. 55, p. 102018, Apr. 2020.

[9] A. Longras, H. Oliveira, and S. Paiva, "Security Vulnerabilities on Implantable Medical Devices," IEEE Xplore, 01-Jun-2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9141043.

[10] [G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS- A blockchain based approach for smart healthcare system," Healthcare, p. 100391, Nov. 2019.

[11] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," SN Applied Sciences, vol. 2, no. 1, Dec. 2019.

[12] T. Mahler, Y. Elovici, and Y. Shahar, "A New Methodology for Information Security Risk Assessment for Medical Devices and Its Evaluation," arXiv:2002.06938 [cs], Feb. 2020.

[13] H. Rathore, A. Mohamed, and M. Guizani, "Chapter 6 - Deep learning-based security schemes for implantable medical devices," ScienceDirect, 01-Jan-2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128190456000066.

[14] Y. Lu and R. O. Sinnott, "Chapter 8 - Security and privacy solutions for smart healthcare systems," ScienceDirect, 01-Jan-2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128190432000083.

[15] D. Sharma and R. C. Tripathi, "Performance of Internet of Things (IOT) Based Healthcare Secure Services and Its Importance: Issue and Challenges," papers.ssrn.com, 01-Apr-2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3565782.

[16] D. N. Mohan, S. S. Gowda, and I. S. Vikyath, "Cyber Security in Health Care," in International Journal of Research in Engineering, Science and Management, vol. 3, no. 1, pp. 551-553, January 2020.