View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Abertay Research Portal

International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

A Framework to Detect Cyber-attacks against Networked Medical Devices (Internet of Medical Things): An Attack-Surface-Reduction by Design Approach

Sanaz Kavianpour[1], Bharanidharan Shanmugam[2], Ali Zolait[3] and Abdul Razaq[4]

[1] School of Design and Informatics, Abertay University, Dundee, Scotland, UK
[2] College of Engineering, IT and Environment, Charles Darwin University, Casuarina, Australia
[3] Department of Information System, University of Bahrain, Sakhir, Kingdom of Bahrain
[4]School of Design and Informatics, Abertay University, Dundee, Scotland, UK

E-mail address: s.kavianpour@abertay.ac.uk, bharanidharan.shanmugam@cdu.edu.au, azolait@uob.edu.bh, a.razaq@abertay.ac.uk

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: The majority of medical devices in the healthcare system are not built-in security concepts. Hence, these devices' built-in vulnerabilities prone them to various cyber-attacks when connected to a hospital network or cloud. Attackers can penetrate devices, tamper, and disrupt services in hospitals and clinics, which results in patients' health and lives threatening. A specialist can Manage Cyber-attacks risks by reducing the system's attack surface. Attack surface analysis, either as a potential source for exploiting a potential vulnerability by attackers or as a medium to reduce cyber-attacks play a significant role in mitigating risks. Furthermore, it is necessitated to perform attack surface analysis in the design phase. This research proposes a framework, which integrates attack surface concepts into the design and development of medical devices. Devices are classified as high-risk, medium-risk, and low-risk. After risk assessment, the employed classification algorithm detects and analyzes the attack surfaces. Accordingly, the relevant adapted security controls will be prompted to hinder the attack. The simulation and evaluation of the framework is the subject of further research.

Keywords: Attack surface, Networked medical device, Risk assessment, Internet of Thing, Cyber-attack

1. INTRODUCTION

The evolution of technology has created both opportunities and challenges in the medical industry. Medical devices have changed from a stand-alone mode to network-connected systems [1] [2]. The growth of the ever-growing network of connected devices is fast and extensive in various industries comprising the healthcare industry. The average hospital room includes 15 to 20 connected medical devices nowadays, which can increase to 85,000 in large hospitals [3]. Medical Cyber-Physical System (CPS) implementations are of great value to reduce medical errors and healthcare costs, enhance the safety and quality of care, and improve workflow performance while decreasing medical professionals' workload [4]. However, it also presents vulnerabilities that make medical devices a potential attack vector for cyber threats. The cyber threat landscape is changing because of the proliferation of devices connected to a network. Threats are becoming more ubiquitous and complex. A criminal hacker can use wireless tools to inject commands that alter the devices' functionality or jam the wireless signals to hinder device availability and expected therapy delivery [5] [6]. Medical devices can be used for cyberwar by targeting politicians who use these devices and cause critical health conditions or eventual death [7]. Over 100 patients are injured yearly because of medical device cybersecurity vulnerabilities [8].

Healthcare networks comprise sensitive information that is governed by privacy and security regulations. Moreover, network-connected medical devices are more exposed to security and privacy risks than generic network servers or endpoints because of the diversity of devices. Medical devices are usually responsible for biomedical or

E-mail: s.kavianpour@abertay.ac.uk

clinical engineering departments whose primary duties are calibration and maintenance. As they are not IT organizations, security and data protection and remediation are difficult. Medical devices have long product life cycles and mostly utilize older generations of operating systems. Patching and upgrading these systems is not always possible, and where it is possible, installation is complicated, and acceptance testing is then required. Medical device manufacturers should perform security updates for device control and configuration validation instead of device owners [9]. Lack of access by manufacturers limits security and data protection upgrades and timely solutions. Manufacturers often use customized versions of standard operating systems, as memory space in embedded systems is restricted.

Consequently, the application of software patches and security solutions is complex. Most healthcare providers prefer to use one specific model and manufacturer to reduce the training overhead. Hence, a homogeneous environment will be created in which security breaches disseminate rapidly among systems.

Medical device vulnerabilities are a risk for patient well-being as well as for everything attached to the network. These devices have mostly open TCP/UDP ports and enable protocols such as TFTP, FTP, and Telnet, which are vulnerable to attacks by default [10]. Approaches such as ICMP and NMAP can be utilized to query profile devices, although these will cease working once they are exposed to multicast network traffic created by worms, viruses, and other malware. Moreover, medical devices are not often replaced or removed from service. There are four types of cyberattacks on medical devices: remote, physical by authorized users, physical by unauthorized users, and physical by criminals [11]. Medical devices are vulnerable to wireless-based attacks that encompass jamming, eavesdropping, replay, and injection attacks [12]. Due to the vast amount of software applications in medical devices, the likelihood of software vulnerabilities also has increased [13] [6]. For instance, in Hanna et al., research [6], four vulnerabilities were found in Automated External Defibrillator (AED) as arbitrary code execution because of a buffer overflow vulnerability, weak authentication mechanism, inappropriate credentials' storage, and unauthorized firmware update as improper use of the Cyclic Redundancy Check (CRC).

Threats to medical devices can be accidental or intentional and arise from insiders, outsiders and natural events [14]. According to Arney et al. [15], threats are classified as passive and active. Passive threats comprise information gathering, interception, and sniffing network data. Active threats encompass disruption of device communications, social engineering, data breach, spoofing or impersonation, phishing, denial of service, malicious code, intellectual property theft, physical destruction, escalation of privileges, and patient information loss.

Some of the extreme threats to medical devices are ransomware, malware, and cryptojacking [16]. Ransomware is one of the most common threats which compromise data and block users or clinical access to their system, demanding the high price of a patient's sensitive data (a ransom) to restore access. The data may be removed automatically if the commanded ransom is not paid in time. Around 78% of healthcare providers have been targeted by either malware or ransomware, or both in the past 12 months. Via crypto-jacking, a compromised device processing power will be controlled to mine cryptocurrency leading to lifetime reduction and threaten patient safety. Medical device vulnerabilities need to be remediated to prevent or mitigate potential cyber threats to medical devices. Hence, a proactive approach is required during all stages of the device's lifecycle. This paper presents such an Attack-Surface-Reduction-by-Design approach. The contributions in this research work are as follows.

a. A new security framework for networked medical devices.

b. Classification of attack surfaces and applying the relevant security controls to mitigate the attack's effect or hinder the attack completely.

c. Declaration of how the proposed solution can address medical devices' risks in the early stage of development and before vulnerabilities exploitation.

The remainder of this paper is organized as follows. Section two illustrates the challenges of CPS in healthcare. The related works on protection strategies in medical devices are discussed in Section three. Section four presents an overview of the Attack-Surface- Reduction by the design approach for medical devices. Finally, the conclusions are described in Section five with the discussion of future research.

2. CHALLENGES OF CPS IN HEALTHCARE

The emergence of sophisticated CPS shifts medical devices' tendency towards active devices consisting of computational embedded systems with sensors and actuators while sustaining passive devices [17]. Medical devices are either Implantable Medical Devices (IMDs) or wearable devices capable of communicating via wireless capabilities. CPS applications have various communication technologies consist of different protocols, wired and wireless technologies. Medical devices mostly used wireless communication. IMDs use low frequency (LF) signals known as Medical Implant Communication Service (MICS), while wearable devices utilize Body Area Network (BAN) such as Bluetooth and ZigBee [18]. Most of the security threats to wireless communication consist of impersonation, eavesdropping, and jamming, which can be exploited to compromise the healthcare CPS [19].

Healthcare-related CPS such as IMDs, BAN, and wearable devices with limited computational capability, communication intricacy, and challenged battery life, privacy, and security play a significant critical role [5] [18]. The level of security in each system is different according to the information sensitivity and control system. Design, development and implementation of a robust CPS in application domains such as healthcare pose various hurdles and restrictions because of inadequate standard interfaces and communication protocols [20]. Challenges of CPS in healthcare encompass software reliability, medical devices interoperability, data extraction, prototype architecture, complex query processing, security and privacy, and system feedback [21] [22] [23]. Figure 1 specifies the challenges pertinent to CPS in healthcare.

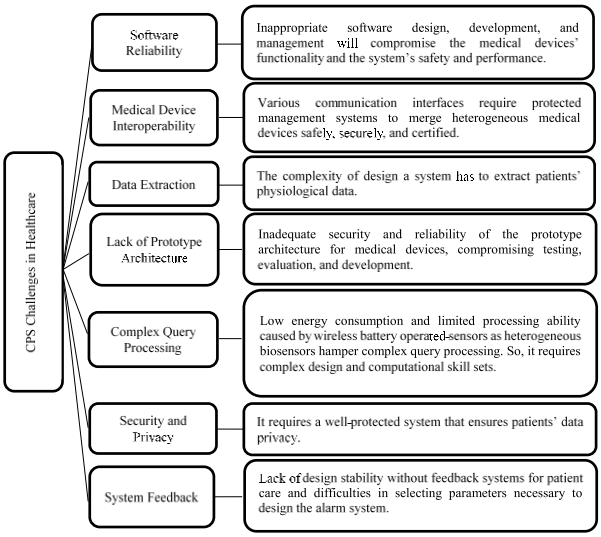


Figure 1: Challenges of CPS in healthcare

3. RELATED WORKS ON MEDICAL DEVICES PROTECTION STRATEGIES

Halperin et al. [24] presented a mechanism that hinders unauthorized access to patients' IMDs, using cryptographic-based authentication and key-exchange. This mechanism depends on external radio frequency instead of consuming batteries. Out-of-Band (OBB) authentication with additional channels was employed in wearable and implantable devices [5]. Biometrics also was used to encrypt communication in the body sensor network (BSN). Gollakota et al. [23] presented an external wearable device (the shield) to exploit jam signals and commands by an unauthorized party to an IMD. Their design jam the IMD's messages and thwart others from decoding them. The Shield can decode them by itself. Furthermore, it allows jamming unauthorized commands, including those that try to modify the shield's own transmissions. Its implementation was in radio software and was evaluated with commercial IMDs. Remote capabilities used for interaction between remote physicians and patients' devices enable attackers to penetrate networks. Hence, manufacturers should disable remote capabilities from sending commands and limit them to receive measures and logs that reduce the usability of such devices [25]. Mitchell and Chen [26] proposed a behavior-rule specification-based technique for IDS to determine sensors and actuators that compromise patients' safety. Their proposal was for stand-alone medical devices. IMDGuard was introduced by Xu et al. [27] to defend against jamming and spoofing attacks. Hayajneh et al. [28] proposed an approach based on the Rabin authentication algorithm to enhance its signature signing process to hinder the unauthenticated and remote commands on the patients' IMDs. Guo et al. [29] adopted the distributed nature of the e-Health system, permitting patients and physicians to perform authentication. The proposed attribute-based authentication scheme framework called PAAS is designed to preserve higher privacy levels on attributes and attribute values even though it has more computation cost and communication resources.

Secure authentication and key agreement scheme for a cloud-assisted wireless body area networks (WBAN) system using extended chaotic maps were proposed by Li et al. [30]. This scheme encrypts the collected health items before diffusion. This scheme is practical for the patient's authentication in medical care systems. Lounis et al. [31] implemented an access control based on cipher text-policy attribute-based encryption (CP-ABE) for wireless sensor networks. This technique decreased the management overhead and the encryption/decryption time. This model delineates scalability, efficiency, and it is fine-grained. Gao and Thamilarasu [32] developed feature sets to employ IMD devices being tested through three different algorithms such as decision tree, Support Vector Machine (SVM), and K-means algorithms. Liu and Li [33] presented a clustering method using k-anonymity. The most similar records will be assigned to the same clusters, which strengthens identity privacy preservation. The similarity between the two records is measured in regard to the Euclidean distance in which the parameters are determined based on the actual requirement.

Table 1 delineates the strength and drawbacks of various relevant works. Although these schemes and techniques employed different security controls to enhance feasibility and preserve medical devices' privacy and security, they have some drawbacks that emphasize the necessity for further investigation and improvement. For instance, Gao and Thamilarasu [32] assessed the machine learning models' effectiveness in detecting attacks. Although their model showed the highest detection accuracy and low false-positive rate compared to all other algorithms, it failed to detect the insider attacker who has more information and access to the medical device. Hence,

it requires further investigation for this type of attack surface to mitigate or preclude the cyberattacks. Furthermore, the reported attacks against security controls employed in healthcare CPS applications delineate these mechanisms' insufficiency in securing information and communication [34]. Medical Devices are vulnerable to attacks; hence, the need for designing and developing an appropriate security mechanism arises. The goal is to define a suitable mechanism, which provides both security and privacy. Security assures that only the authorized entities can access, identify and configure devices, and privacy assures the protection of devices' private information.

A well-protected medical device requires accurate security mechanisms that consider threat landscape alterations. All possible attack surfaces within the medical device environment must be considered in the design phase. The main requisite in the product development lifecycle for medical devices is security-by-design. Vora and Schaeffer [11] reported that, some security mechanisms such as access control, network scanning, attack surface reduction, the root of trust, the digital signature, encryption methods, and software updates, among others can be used to either thwart attacks or attenuate the impact on medical devices. The implementation of all these mechanisms in a single platform is not feasible. According to risk management, a set of several mechanisms can be integrated to provide strong protection against cyber threats. The advantage of the proposed framework is that it can detect the insider attacker who has more information about the medical device and mitigate the relevant attack surfaces, but Gao and Thamilarasu's [32] method failed to detect insider attackers.

Table 1: Comparison of related works

Author	*Method*	*Strength*	*Drawbacks*
Halperin et al. [24]	Presented three new zero-power (zero-power notification, zero-power authentication, and sensible key exchange) defenses according to RF power harvesting in which two of these defenses are human-centric.	Mitigates the privacy violation and patient data and therapy settings malicious modifications without instantaneously drawing power from a battery.	Failure modes without addressing by some present-day design strategies and certification processes.
Gollakota et al. [23]	Proposed a physical layer solution called the shield employing a novel radio design that can act as a jammer-cum-receiver.	It provides confidentiality for IMDs' transmitted data and shields IMDs from unauthorized commands efficiently with no changes to the IMDs themselves.	Lack of usability of wearable devices.
Xu et al. [27]	Researchers introduced IMD Guard using two tailored techniques.		No transmit and receive at the same time. Lack of confidentiality.
Guo et al. [29]	Researchers proposed a framework called PAAS in e-Health networks that control users' verifiable attributes to authenticate users' eHealth systems. It includes only two end users instead of centralized infrastructures for authentication.	It is efficient in preserving the privacy and practicality of eHealth systems.	It does not preserve user anonymity and the inefficiency of double-secret keys.

Mitchell and Chen [26]	Researchers presented a methodology to transform behavior rules to a static machine in which a device that is being monitored for its behavior can easily be monitored if it delineates abnormal behavior.	This technique has feasible trade false positives for a high detection probability of coping with more sophisticated and hidden attackers to support ultra-safe and secure MCPS applications. Furthermore, it outperforms two existing anomaly-based techniques used for abnormal patient behavior detection in pervasive healthcare applications.	Only support stand-alone medical devices. No adversary modeling and intrusion defense modeling research based on the accumulation of deviation from good states to increase detect rate.
Hayajneh et al. [28]	Researchers proposed a lightweight public-key-based authentication protocol for wireless Medical Sensor Networks (MSNs) with an enhanced signature signing process to be proper for delay-sensitive MSN applications.	Can deliver secure, prompt, and authenticated commands from the medical staff to the MSN nodes. Furthermore, it decreases the delays up to 80 % that is a severe issue in MSN applications.	

Li et al. [30]	Researchers presented a secure cloud-assisted architecture to access and monitor health items collected by WBAN using the Diffie-Hellman key exchange notion.	Ensures patient privacy and system confidentiality as well as preserving the minimum computation for either medical treatment or remote medical monitoring. It achieves desirable security functionalities consist of mutual authentication, session key agreement, perfect forward secrecy, and non-repudiation in doctor diagnosis. Furthermore, its implementation is useful for mobile emergency medical care systems.	Not preserving backward secrecy. No mutual and strong anonymity.
Lounis et al. [31]	Researchers proposed a new architecture to collect and access vast generated data by medical sensor networks. Moreover, presented an operative and flexible security mechanism using Ciphertext Policy Attribute-based Encryption (CP-ABE).	It provides an effective, fine-grained and scalable access control in normal and emergency situations.	It does not attain practical computation outsourcing as an entire trusted entity does data encryption.
Gao and Thamilarasu [32]	Assessed the practicability of employing machine learning models in attack detection, developed feature sets to precisely profile a medical device, and checked any deviations.	It achieves the maximum detection accuracy, low false positive-rate, as well as prompt training and prediction pace.	It failed to detect the insider attacker who has more information about the medical device.
Liu and Li [33]	Researchers presented a definite threat model for wearable devices' data sharing process, using a K-anonymity method.	It provides sufficient anonymity and identity disclosure protection. It preserves IoT devices' data privacy and usability.	Vulnerable to Background knowledge and homogeneity of attacks.

4. ATTACK-SURFACE-REDUCTION BY DESIGN APPROACH

A. Attack Vectors

The possible attack vectors that lead to security breaches are described by Yaqoob et al., [35] as in the following Figure two.

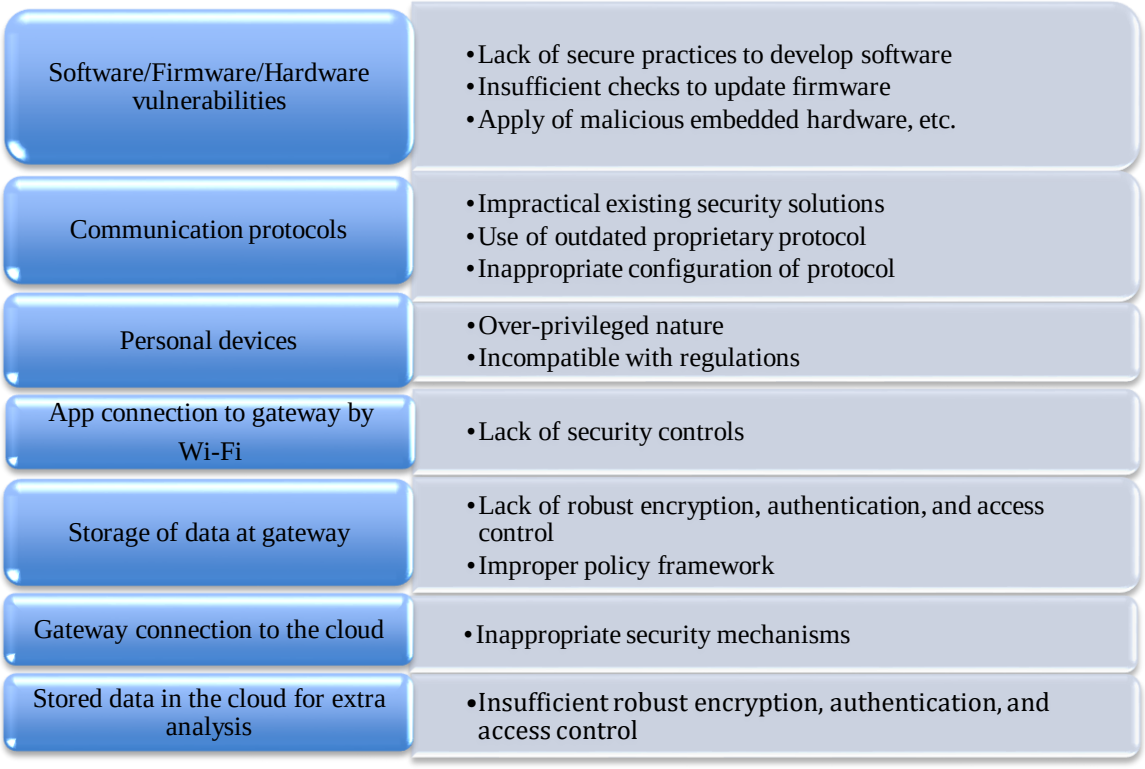


Figure 2: Attack vectors.

(Source: Yaqoob et al., [35])

B. A Proposed Secure Framework

Medical devices need to be classified at an early stage to identify their significant level of risk. For instance, if the device malfunction will affect the patient life, it delineates that this device security and privacy preservation should be done at the highest level to prevent any source of disruption or mitigate the possibility of attacking this device to the least level. In this paper, a secure framework is proposed to detect cyber-attacks against networked medical devices. The proposed framework can reduce attack-surfaces by design. There are three types of devices in this framework: high-risk, medium-risk, and low-risk [35].

a. High-risk devices. These devices pose the highest security risks and vulnerabilities and entail the most rigid and precise controls.

b. Medium-risk devices. These devices, which are less prone to security risks than high-risk devices, are vulnerable to effectiveness and safety.

c. Low-risk devices. These devices are simple and are released from regulatory controls.

This classification is based on the FDA categorization of medical devices concerning the risks associated with them. Medical devices need to be classified at an early stage to identify their significant level of risk. For instance, if the

device malfunction will affect the patient life, it delineates that this device security and privacy preservation should be done at the highest level to prevent any source of disruption or mitigate the possibility of attacking this device to the least level.

Hence, devices will go through risk assessment to be specified whether the risk impact is critical, major, or minor. The risks are posed to humans by devices and require various security controls to ensure safety and efficiency. After the risk assessment, the attack surfaces are checked.

Attack surface is a list of system inputs that an attacker can use to compromise a system. If the attack surface is reduced as much as possible, the system can be more resilient to be compromised. According to the attack surface analysis, attacks can be from humans, networks, systems, and any combination [36].

a) **Human attack surface**: This surface is the potential for insider threats, fraud, and social attacks such as phishing and social engineering. It encompasses any accidental activity or any deliberate malicious activity performed by an authenticated insider and can bypass the system and compromise its safety.

b) **Network attack surface:** The communication protocols can be used as a source of attacks consisting of, among others, the DoS, man-in-the-middle, and spoofing.

c) **System attack surface:** This surface constitutes physical attacks comprised of reverse engineering, hardware attacks, side-channel attacks, malicious USB key, etc. Also, software attacks can occur by malicious code comprising worms, and run time attacks.

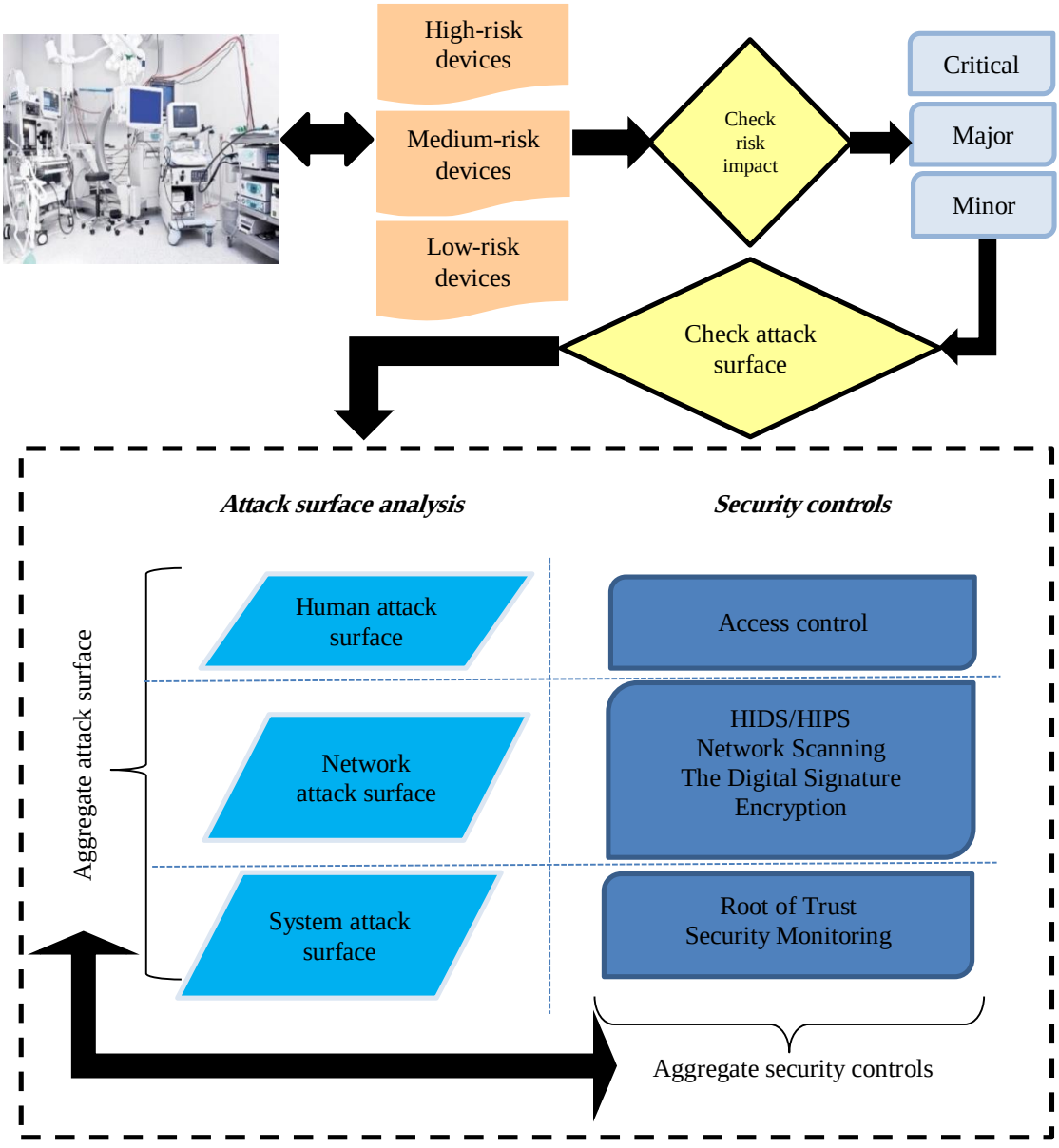
d) **Aggregate attack surface**: Any integration of humans, networks, systems surface can be used as a source of attacks.

Attack surfaces are unavoidably visible across various abstraction layers and can lead to privacy breaches and information leakage as well as bypassing security controls. Hence, their detection is significant for alleviating vulnerabilities and remediating the risks via prevention and mitigation strategies and measures to reduce the attack surface associated with networked medical devices.

In this framework, the decision tree learning algorithm (optimized implementation of the C4.5) is applied to classify the attack surfaces. Decision trees are a very popular tool for predictive analytics as they are relatively easy to use, provide highly interpretable output and explicit visualization in a tree diagram [37]. Furthermore, classification is fast once rules are developed with not much computation. Classification is based on the features that provide the most information to be used to assign the attack surfaces to the accurate class.

After detecting the attack sources, the relevant security controls will be called and used to mitigate the attack's effect or hinder the attack completely. Security controls are set based on the attack surfaces classification. For instance, if attacks are detected from the network, security controls that are explicitly relevant to network protection such as HIDS/HIPS, network scanning, the digital signature, and encryption will help manage the protection and block attack tools techniques. If attacks are from the system, system authentication or authorization methods are employed to decrease process and data resources disclosure [37]. Also, attacks can be detected from the system. In this case, the root of trust and security monitoring techniques are applied to provide protection. Attacks can be detected from a combination of any of the mentioned surfaces, called an Aggregate attack surface. For Aggregate attack surfaces, various security controls from different surfaces are recalled mitigating an attack.

Ensuring security is an intricate task as attackers endeavor to manipulate the system context to gain access. Employing the proposed framework can provide a comprehensive understanding of medical devices' elements, the parts that can be breached for an attack, when and how the attack surface changes, and what this means from a risk perspective. Hence, risks to medical devices can be addressed in the early stages of development and before vulnerability exploitation. This will result in the patients' security enhancement. Figure 3 depicts the research proposed framework [38].



5. CONCLUSIONS AND FUTURE WORK

The adoption and integration of wired and wireless networked medical devices in the healthcare industry have created the risk of cyber-attacks. Medical devices are insecure by design and can be exposed to risks due to the increase in cyber threats' number and complexity. These threats can be used as an access point for entry to a hospital or health care networks if their vulnerabilities are not addressed and remediated. Cyber threats represent a large attack surface, which could interfere with health care and even endanger patients' lives. The likelihood of exposure to attack surfaces and vulnerabilities to malicious attackers grows with the increasing numbers of connected medical devices. Incorporating security strategies to decrease attack surfaces at the design phase is an example of best practice to counteract cyberattacks. An attack-surface-reduction framework that integrates the attack surface concepts into medical devices' design is proposed in this research. In this research, the conceptual framework, which incorporates attack surface concepts into the design and development of medical devices, is presented. The simulation and the evaluation of the proposed framework are the subjects of future research. This framework is practical in assessing cyber risks and providing a feasible approach to mitigate cyber-attacks. Using this framework prevents or alleviates the cyber threat impacts on medical devices.

The proposed framework can advance the medical device interoperability safely and securely in addition to addressing security and privacy challenges of CPS in healthcare that are required for ensuring patients' data privacy. This framework acts as a protected management system in which medical devices can communicate in a protected and secure interface. The prototype architecture for medical devices has insufficient security and reliability that compromise testing, evaluation, and development.

One of the proposed framework outputs introduces the relevant categorization of risks as critical, major, and minor that are evaluated based on the risk impact. Via the proposed framework, classifying medical devices into high-risk, medium-risk, and low-risk and applying the relevant security controls based on their class can provide adequate security and reliability.

Furthermore, a secure medical devices network will ultimately facilitate greater patient confidence, lead to better care coordination, enhance information exchange, and improve patient care. Lastly, the simulation and evaluation of the framework is the subject of further research in the future. The security threats to connected medical devices are occurred because of forging, tampering, data injection, and spoofing attacks. A simulated sample of these attacks will be tested to evaluate the framework's feasibility and effectiveness in detecting attacks. The assumption in the attack scenario is that an attacker manipulates medical devices, targeting to read or modify patient data. Medical devices should be classified into the relevant category (High-risk, Medium-risk, and Low-risk) accurately via the proposed framework. The feasibility of the framework in detecting attack surfaces will be tested, and the effectiveness of the employed security controls in mitigating or blocking the attacks will be evaluated. The result of the decision tree learning will be compared with other learning algorithms, such as the support vector machine, to test the classifier's performance.

6. REFERENCES

[1] M. A. Rahman and A. T. Asyhari, "The emergence of Internet of Things (IoT): connecting anything, anywhere," *Computers*, vol. 8, no. 40, 2019.

[2] A. L. King, L. Feng, O. Sokolsky and I. Lee, "Assuring the safety of on-demand medical cyber physical systems. In: ,," in *1st International Conference on Cyber-Physical Systems, Networks and Applications* , Taipei, Taiwan, 2013.

[3] A. Uzialko, "The security of connected medical devices," https://www.businessnewsdaily.com/, 2019. [Online]. Available: https://www.businessnewsdaily.com/15031-connected-medical-devices-healthcare-cybersecurity.html. [Accessed 8 March 2021].

[4] A. Alamri, "Ontology middleware for integration of IoT healthcare information systems in EHR systems.," *Computers*, vol. 7, no. 4, p. 51, 2018.

[5] M. Rushanan, A. D. Rubin, D. F. Kune and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," in *2014 IEEE Symposium on Security and Privacy,*, 2014.

[6] S. Hanna, Rolles, R., , Molina-Markham, A., and Poosankam, P., Fu,, "Take two software updates and see me in the morning: the case for software security evaluations of medical devices," in *Proceedings of the 2nd USENIX Workshop on Health Security and Privacy*, San Francisco, CA., 2011.

[7] L. Vaas, "Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking," nakedsecurity by sophos, 22 October 2013. [Online]. Available: https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/. [Accessed 10 May 2021].

[8] E. Sweeney, "New research shows patients harmed by medical device breaches," Questex LLC. , 13 June 2018. [Online]. Available: https://www.fiercehealthcare.com/tech/ucsd-medical-device-cybersecurity-patient-harm-advamed-legacy-devices. [Accessed 10 May 2021].

[9] A. Wirth, "Cybercrimes Pose Growing Threat to Medical Devices," *Biomed Instrum Technol*, vol. 45, no. 1, pp. 26-34, J 2011.

[10] R. Staynings, "Security : Securing Medical Devices – The Need for a Different Approach – Part 1," Cisco Blogs, 18 April 2017. [Online]. Available: https://blogs.cisco.com/security/securing-medical-devices-the-need-for-a-different-approach-part-1. [Accessed 10 May 2021].

[11] K. Vora and M. Schaeffer, "A platform approach to securing your medical devices. White Paper,," Renesas Electronics., 5, 2017 Nov 2017. [Online]. Available: https://www.renesas.com/us/en/application/healthcare. [Accessed 1 May 2021].

[12] J. Radcliffe, "Hacking medical devices for fun and insulin: breaking the human SCADA system," in *Black Hat Conference presentation slides*, 2011.

[13] K. Fu and J. Blum, " Controlling for cybersecurity risks of medical device software.," *Communications of the ACM*, vol. 56, no. 10, pp. 35-37, 2013.

[14] K. Stouffer, J. Falco and K. Scarfone, "Guide to industrial control systems (ICS) security," National Institute of Standards and Technology (NIST)., Gaithersburg, 2013.

[15] D. Arney, Venkatasubramanian, K., Sokolsky, O. and Lee, I. , "Biomedical devices and systems security," in *33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC '11)*, 2011.

[16] J. Rabinowitz, "Protecting patients with cybersecurity. Healthcare GLOBAL.," 2018. [Online]. Available: https://www.healthcareglobal.com/technology/protecting-patients-cybersecurity.. [Accessed 1 May 2021].

[17] T. Savage, "The implications of RoHS on active implantable medical devices.," in *2011 International Reliability Physics Symposium*, 2011.

[18] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao and V. Leung, "Body Area Networks: A Survey. Mobile Networks and Applications," vol. 16, no. 2, pp. 171-193, 2010.

[19] Z. Ankarali, O. Abbasi, A. F. Demir, E. Serpedin and Qaraq, "A comparative review on the security research for wireless implantable medical devices," in *4th International Conference on Wireless Mobile Communication and Healthcare*, 2014.

[20] Lee, I., O. Sokolsky, S. Chen, J. Hatcliff, Jee, E, Kim, B, King, A, M. Mullen-Fortino, Park, S., Roederer, A and K. K. Venkatasubramanian, "Challenges and research directions in medical cyber–physical systems.," *Proceedings of the IEEE*, vol. 100, no. 1, 2012.

[21] S. Haque, S. Aziz, and M. Rahman, "Review of Cyber-Physical System in Healthcare.," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[22] M. Rostami, W. .Burleson, A. Juels, and F. Koushanfar, "Balancing security and utility in medical devices?," in *50th ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2013.

[23] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM 2011 conference (SIGCOMM '11)*, 2011.

[24] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, , T. Kohno and W. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Symposium on Security and Privacy (sp 2008)*, 2008.

[25] G. Chen and E. Rodriguez-Villegas, "System-level design trade-offs for truly wearable wireless medical devices.," in *Annual International Conference of the IEEE on Engineering in Medicine and Biology Society (EMBC)*, 2010.

[26] R. Mitchell and Chen, I.R., "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 16-30, 2014.

[27] F. Xu, Qin, Z., Tan, C., Wang, B. and Li, Q., "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *IEEE International Conference on Computer Communications (INFOCOM 2011)* , 2011.

[28] T. Hayajneh, Mohd, B., Imran, M., Almashaqbeh, G. and Vasilako, "Secure authentication for remote patient monitoring with wireless medical sensor networks.," *Sensors*, vol. 16, no. 4, p. 424, 2016.

[29] L. Guo, Zhang, C., Sun, J. and Fang Y., "PAAS: a privacy-preserving attribute-based authentication system for eHealth networks," in *32nd International Conference on Distributed Computing Systems*, 2012.

[30] C. Li, Lee, C. and Weng, C.A. , "secure cloud-assisted wireless body area network in mobile emergency medical care system.," *Journal of Medical System*, vol. 40, no. 1, 2016.

[31] A. Lounis, Hadjidj, A., Bouabdallah, A. and Challal, Y. , "Healing on the cloud: secure cloud architecture for medical wireless sensor networks.," *Future Generation Computer Systems*, vol. 55, no. 1, pp. 266-277, 2016.

[32] S. Gao and Thamilarasu, G. , "Machine-learning classifiers for security in connected medical devices.," in *26th International Conference on Computer Communication and Networks (ICCCN), 2017*, 2017.

[33] F. Liu and Li, T., "A clustering k-anonymity privacy-preserving method for wearable IoT devices," *Security and Communication Networks,*, Vols. 2018:1-8, 2018.

[34] A. Humayed, Lin, J., Li, F. and Luo, B., "Cyber-physical systems security– a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802-1831, 2017.

[35] T. Yaqoob, Abbas, H. and Atiquzzaman, M., "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices - a review.," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723-3768.

[36] L. Deka and Chowdhury, M. , Transportation cyber-physical systems., Elsevier, 2018.

[37] T. Patil and Sherekar, S.S., "Performance analysis of Naive Bayes and J48 classification algorithm for data classification.," *Int. J. Comput. Sci. Appl*, vol. 6, no. 2, p. 256–261, 2013.

[38] S. Kavianpour, , Shanmugam, B., Azam, S., Zamani, M. and Samy, G.N., "A systematic literature review of authentication in internet of things for heterogeneous devices.," *Journal of Computer Networks and Communications*, vol. 2019, no. 5747136, 2019.

Sanaz Kavianpour Lecturer in Cybersecurity within the Division of Cybersecurity, in the School of Design and Informatics at Abertay University. Dr. Kavianpour teaches machine learning applications in cybersecurity for 4th year students in Ethical Hacking and Master Students in Ethical Hacking and Cyber Security. She is currently collaborating in research with NHS Scotland and other partners on the project, which aims to preserve patient data security in Safe Haven environments. Her core expertise is in the fields of information security, social networks, cyber-physical system, and the Internet of things security. She designed and developed the privacy-preserving model for social networks to enhance users' privacy in her empirical research.

Bharanidharan Shanmugam Lecturer in School of Engineering and Information Technology at Charles Darwin University. Dr. Shanmugam's teaching activities focus on information security, programming, IT management, and organizational security enterprise IT management. His research interests are in information, application and network security, risk and policy, and the Internet of Things (IoT).

Ali Hussein Zolait Assistant Professor of Management Information Systems (MIS) at the College of Information Technology – Department of Information System – University of Bahrain. Dr. Zolait is a senior member of IEEE and the Chair IEEE Bahrain section (Jan 2020-2022), and he is the Editor-in-Chief of the International Journal of Technology Diffusion (IJTD). Dr. Zolait served as Visiting Research Fellow from 2007 to 2010 for the University of Malaya in Malaysia. Currently, Dr. Zolait teaches, researches, and supervises undergraduate and master students in cybersecurity and system analytics. He acted as an invited speaker to several conferences and seminars and as an external assessor (examiners) for many Ph.D. theses and the government's small and medium-founded projects. Zolait has published three books and more than sixty research papers. He has published on Information Security, Information Security Risk Management (ISRM), Assessment of Information Security Maturity, and Information Security Landscape.

Abdul Razaq Lecturer at Abertay University. He holds PhD and Master Degree in Computer Science. He has a software engineering background in scalable software architectures and systems integration. His experience includes low-level programming, firmware design, device drivers and kernel development. He has experience in full development lifecycle including project planning, team development, product testing and rollout. His research interests include digital communication, operating systems, system engineering, and embedded systems.