International Journal of Control and Automation
Vol. 12, No. 3 (2019), pp.29-36
http//dx.doi.org/10.33832/ijca.2019.12.3.03

INTERNET OF MEDICAL THINGS (IOMT): TRENDS AND CHALLENGES

Sabah Mohammed[1], Jinan Fiaidhi[2] and Sami Mohammed[3*]

[1]*Department of Computer Science, Lakehead University, Canada*
[2]*Department of Computer Science, Lakehead University, Canada*
[3]*Department of Computer Science, University of Victoria, Canada*
[1]sabah.mohammed@lakeheadu.ca, [2]jfiaidhi@lakeheadu.ca, [3]smohamm@uvic.ca

***Abstract*— Since the transformation from paper records to digitized Electronic Health Records (EHRs), patient data are coonly updated and then sent by doctors to specialists in other hospitals among other transactions. The problem is that caregivers are not banks, where financial information is locked up and not shared. This unencrypted information is vulnerable to profit-hungry hacker attacks. Moreover, healthcare is rapidly moving to a completely digitized environment, and, as a result, many devices have been introduced to the hospital ecosystem and bedside workflows to help extend and streamline care throughout the hospital. As hospitals move to achieve real-time visibility into their different systems and applications, reduce time away from the patient bedside, and increase the quality of care, new technology has come in to play to improve interoperability of these systems and components. Robust tools, ubiquitous devices and clinical modern networks like the IoMT (Internet of Medical Things) have allowed clinicians to become more efficient and mobile with patient care. Unfortunately, this new technology has also opened the door to increased risk and new potential points of exposure for healthcare IT infrastructures. This article discusses the challenges and the suggested steps needed to reduce vulnerabilities against such security attacks.**

***Keywords*— IoMT, Cyber Attacks, Prevention, Medical Devices**

1. INTRODUCTION

The Internet of Medical Things (IoMT) is an emerging wave of technologies that contributes to the establishing connected healthcare systems. It consists of smart devices, such as wearables, sensors technology, smart algorithms and medical/vital monitors, strictly for health care use on the body, in the home, or in community, clinic or hospital settings; and associated real-time location, telehealth, networking and other connectivity services like blockchain. It can reduce unnecessary hospital visits and the burden on healthcare systems by connecting patients to their physicians and allowing the transfer of medical data over a secure network. According to Frost & Sullivan analysis [1], the global IoMT market was worth $22.5 billion in 2016; it is expected to reach $72.02 billion by 2021, at a compound annual growth rate of 26.2%. However, the accelerated adoption of IoMT requires careful considerations as they must be robust against the security vulnerabilities affecting medical devices that IoMT uses, a landscape of uncertain liability, new standards and emerging policies and regulations. Consequently, medical device manufacturers should keep abreast of current minimum security standards

Received: November 26, 2018
Reviewed: January 28, 2019
Accepted: March 4, 2019
* Corresponding Author

ISSN: 2207-6387 IJCA

to prevent cyberattacks like the "WannaCry" ransomware attack in May 2017 [2]. These security vulnerabilities highlight the importance of developing standards, using best practices for compliance. The existing broad, ambiguous standards regulating the IoMT invite litigation, and precise legal boundaries have yet to be drawn. In an effort to regulate the IoMT and ensure public safety, the US Food and Drug Administration (FDA) has issued premarket and postmarket cybersecurity guidance in October 2018, providing nonbinding recommendations to device manufacturers [3]. However, many questions remains to be answered regarding IoMT standards and security such as [4]:

- What is the reasonable standard of care in creating a secure IoMT device?
- What constitutes a design defect or failure to warn?
- Are security vulnerabilities considered a design defect?
- For how long must device manufacturers provide security monitoring and software updates after selling a product?
- Does user failure to download security updates act as a superseding cause or a failure to mitigate in cases of liability for defective software?
- Will these security vulnerabilities mean an uptick in shareholder derivative actions?

Craig Badrick estimates that of every 1,000 IoT devices in use, 164 are subject to attacks. As hospitals discover more and more applications for the IoMT, many are beginning to add devices that may actually be putting their operations — and even patient lives — at risk [5]. In fact, the healthcare industry is rapidly moving to a completely digitized environment, and, as a result, devices have been introduced to the hospital ecosystem and bedside workflows to help extend and streamline care throughout the hospital as well as many devices are incorporated to monitor remotely patients at home or work. While using robust medical devices and mobile smartphones have allowed clinicians to become more efficient and mobile with patient care. Unfortunately, this new technology has also opened the door to increased risk and new potential points of exposure for healthcare IT infrastructures. Without enforcing rigorous standards for safely using these medical devices within the new IoMT platform, then each network-connected medical device within a health provider's ecosystem will opens up the possibility for patient health information exposure as well as the potential for other unauthorized use of critical systems and applications. This article addresses the challenges and solutions available for developing or adopting robust IoMT.

2. CHALLENGES IMPACTING IOMT ADOPTION

In recent article published by Deloitte [6], the authors listed the most important challenges including:

- **Interoperability** – for interoperability to work effectively, the direction of travel should be towards open platforms, based on open data standards. This will enable payers, providers and technology vendors to come together to make data more available to each another.
- **Cyber security** – the increasing numbers and capability of connected medical devices present additional risks for data security. The scale and cost of breaches is often significant and far reaching.
- **Regulatory change** – managing the raft of regulatory change occurring is imperative for both developing connected medical devices and the success of the IoMT.

- **Digital talent and building digital capability** – there is increasing concern among key stakeholders that a growing skills gap will delay the deployment of IoMT solutions and constrain market growth.
- **Maintaining trust in a digital age** – as medtech companies develop strategies and services based on the generation and transmission of patient data, they need to ensure they demonstrate clearly to patients, the public and health care professionals how their data is being used to reduce the risk of undermining the benefits that access to data can bring.
- **Funding, business and operating models** – different types of innovation will require different business models, and progress will depend on both the innovators themselves working in new ways to take on risks and rewards.
- **Scale** – a key challenge for medtech is ensuring that health care organizations, clinicians and patients understand the added-value of connected medical devices and use them at scale to drive better economics and patient outcomes.

The cyber security challenge is the most sever one of all as healthcare is promoting more mobile medical devices in their setting. Every medical device then become as a "back door" into a hospital's IT network and attackers are now exploring a new strategy called "destruction of service," or DeOS, which will completely incapacitate the network. This issue needs further consideration as the healthcare setting include variety of easily compromised medical devices — Some of the medical devices were built 20 years ago but still work, believe it or not. Sadly, many of these tools are still being used by hospitals (often to save money). However, those medical devices, including pacemakers, X-ray machines and CT scanners, use outdated security software that isn't automatically updated. This leaves hospitals and patients very vulnerable. Moreover, regulatory agencies like the FDA-issued security recommendations are not mandates — Quite simply, without a firm mandate to follow, manufacturers and healthcare organizations struggle to follow the FDA's did not provide decisive guidelines to reduce device security risks, especially if it costs more money and resources. According to a 2017 study conducted by the Ponemon Institute, only 51 percent of medical device manufacturers and 44 percent of healthcare organizations follow FDA guidelines [7]. The pacemaker recall of 465,000 devices by the FDA in August 2017 is an example of the cybersecurity vulnerabilities on these sensitive medical devices where it could allow a hacker to take over the medical device that controls heart rhythm [8].

3. IOMT SECURITY VULNERABILITIES

The IoMT has extended the traditional perimeter of healthcare security. Once a threat is successfully inside, there are usually few security measures in place to detect it or slow it down. This is one reason why IoMT devices are popular attack vectors. These internal endpoints have been authorized to access the network as an authorized user. Once deployed inside the perimeter defenses, IoMT devices have largely unquestioned access to the network's data [9].

Actually these vulnerabilities will never be fully prevented as the technology never stays still and neither do hackers. The new developments in protecting patient data and patients themselves will not be the end of healthcare cybersecurity, nor will they guard against every possible way of hacking IoMT devices. However, it is important to develop and implement medical device security and IoMT security strategies. These strategies need to include not only a screening and threat mitigation standard for current devices but also a plan for maintaining security on a continuing basis. These strategies must not disrupt clinical workflow but it should provide clinicians with the proper knowledge on what to do if a data compromise occurs. Figure 1 illustrates the types of security

attacks that may imposed on IoMT devices and networks. The outage attack stops an IoMT device (e.g. pacemaker) from working and may result in death or physical injury to the patient. With the physical attacks, hackers need to physically install a pseudo sensor in the IoMT architecture and in order to receive unauthorized health information. The hacker may physically alter the device to state false readings, resulting in the patient receiving heavier medication for example. The message corruption attack is the result of inserting a virus with IoMT data when sent to the physician causing corruption of the original data. In the false node attack one patient data may be replaced with other patient data and would unknowingly cause inaccurate diagnosis to both patients. While in the passive information gathering attack the hacker would collect the data as they are sent to clinicians as an intermediary and may store all patient data in a geographical area and sell that data to insurance companies or other beneficiaries. In the routing attack the hacker could create an infinite loop between the various sensors in the IoMT network and the data would constantly overwrite itself. The monitoring and eaves dropping attack the hacker could use the wearable IoMT device to track the patient's voice commands and listen on personal conversations. Those conversations could be recorded and used to blackmail the patient. The traffic analysis attack happens when a patient sends data from their IoMT device to their family or friends, the hacker could send additional messages to the recipients. In the Denial of service attack, the hacker may lock the medical device with a password encryption and prevent a patient from using it. The hacker would provide the password only if the ransom is paid. Finally, in the node malfunction attack, the hacker may erase emergency phone numbers on an emergency response sensor and prevent patients from calling emergency services.

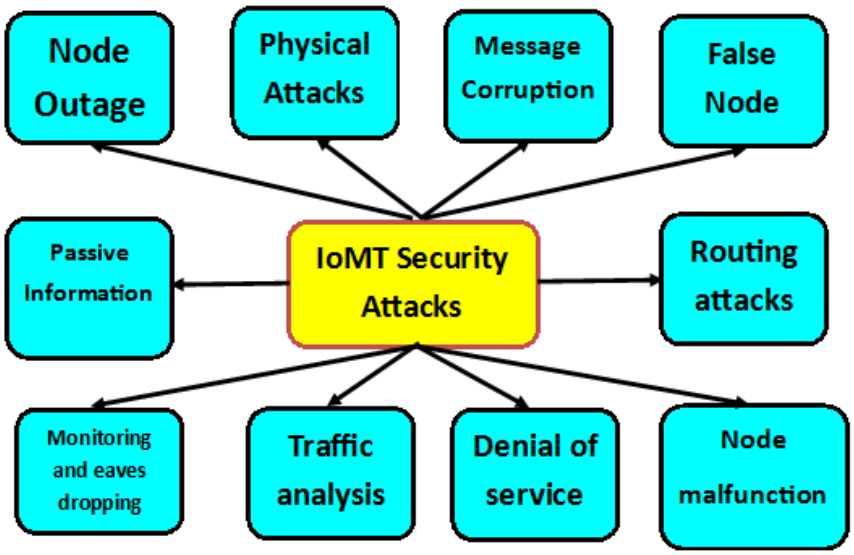

Fig. 1 Types of Expected Attacks on IoMT

There are many popular brands that be subjects to these attacks especially if they were used within the healthcare IoMT settings. Examples may include Medtronic MyCareLink[1] which is an app that uses a reader to receive pacemaker data. The data are sent from the Smartphone to the patient's clinic. The Reveal LINQ[2] is another example which uses a tiny insertable monitor placed just under the skin and the MyCareLink™ Patient Monitor — a bedside unit that collects heart rhythm data from the insert and sends it to your doctor. The OmniPod Insulin Management System[3] is a third example which

[1] https://global.medtronic.com/xg-en/mobileapps/patient-caregiver/cardiac-monitoring/mycarelink-heart-app.html
[2] https://www.medtronic.com/us-en/patients/treatments-therapies/heart-monitors/our-monitors/reveal-linq-icm.html
[3] https://www.myomnipod.com/home

include a tubeless Pod and a handheld Personal Diabetes Manager that allows the patient to wireless program insulin delivery. The CardioNet wEvent[4] is a fourth example that uses a wireless cardiac event monitor to collect asymptomatic and symptomatic events to detect heart arrhythmias. These data are automatically transmitted wirelessly through a cellular network to the physician. Finally the Welch Allyn Home Blood Pressure Monitor[5] with the Blood Pressure App to send readings directly to doctors and stores to track results. Figure 2 illustrate the most vulnerable IoMT devices as investigated in reference [10].

Device	Vulnerability
Wireless Pacemakers, Cardiac Defibrillators	-Access to patients' medical information -Turning off device -Delivering electric shock to patients
Insulin Pump	-Releasing lethal dose of insulin without alerting patient -Access to device without knowledge of serial number
Wireless Pacemaker	-Remote control of device -Disabling wireless functionality
Bluetooth Enabled Defibrillators, Wireless Infusion Pumps, X-Rays, CT scans	-Remote control of devices -Unencrypted and unauthenticated communication between devices -Easy to access hand-coded passwords
Infusion Pump	-Remote control of pump -Releasing lethal dose of insulin without alerting patient
Cardiac Implants	-Remote control of cardiac device -Rapid battery depletion if accessed -Releasing inappropriate pacing or shocks if accessed

Fig. 2 Type of IoMT devices most vulnerable to security attacks

4. PREVENTING THE IOMT FROM THE SECURITY ATTACKS

Hacker meddling in the IoMT operations not only costs lots of time, money and operational downtime, but threatens lives. It's a dire situation that must be addressed. Hospitals and other healthcare providers must practice better cybersecurity hygiene. For starters, healthcare organizations must improve the speed and thoroughness of software patching and update processes. As much as possible, organizations also need to use threat intelligence and automation, as well as institute cyber-awareness training programs to protect against social media attacks and other attack vectors. According to [11] there are some foundational activities that healthcare organizations can take to ensure they are protected against such attacks:

[4] https://www.myheartmonitor.com/device/wevent/
[5] https://www.welchallyn.com/en/products/categories/welch-allyn-home/connected-blood-pressure-monitors/home-bp-monitor.html

- **Practice Diligent Cyber Hygiene.** Among other cyber hygiene best practices, healthcare organizations need to improve the speed and thoroughness of software patching and update processes. Where possible, organizations need to prioritize patching using threat intelligence and automation and institute cyber-awareness training programs to protect against social engineering and other attack vectors. This also needs to include keeping an inventory of all devices, especially IoMT, in order to track and cross-reference them against announced vulnerabilities and/or exploits.
- **Reinforce Network Segmentation.** With the proliferation of IoMT devices, which are often "headless" and cannot be updated to protect against new vulnerabilities and multi-vector attacks, organizations need to more strongly segment and even micro-segment their networks, applications, users, and data. This requires the kind of network segmentation where Next Generation Firewalls (NGFW) are not only placed to handle north-south segmentation, but to inspect traffic moving laterally across the network as well, between network zones, or across different domains such as cloud or remote offices. A segmented strategy enables organizations to institute checks and policies at various points of the network to control users, applications, and data flow. Network segmentation also gives organizations the ability to identify and isolate a threat before it spreads to additional segments of the network. These techniques help organizations stop or minimize intrusions, especially ransomware, before they have a broader impact.
- **Achieve Transparent Visibility and Control.** Due to the elasticity and complexity of today's modern healthcare networks, the need for collaborative information sharing across internally and externally situated users and departments, and the number of regulatory requirements that need to be complied with, healthcare organizations must have transparent visibility across the entire attack surface, especially into the multi-cloud, to understand their threat posture and quickly respond to new vulnerabilities and attacks, while simultaneously demonstrating compliance. A fabric-based cybersecurity architecture breaks down network, data, application, and user silos, and enables security to adapt and respond as an integrated system to detected changes in the network or threat landscape.
- **Use Advanced Threat Intelligence.** The time available to organizations to patch vulnerabilities, identify threats, and remediate intrusions and breaches is shrinking. Traditional security approaches, such as signature-based detection, static, perimeter-based security, or isolated security devices, cannot keep pace with the speed and intensity of the current threats or even the rate of change occurring within the network itself. This is where advanced threat intelligence is a requisite. Threat intelligence can identify tactics and techniques being used to exploit vulnerabilities, and offer effective options for such things as prioritizing patching, accelerating remediation efforts, or broadening forensic analysis after a cyber event. Furthermore, rapidly advancing artificial intelligence and machine learning capabilities can self-detect anomalies and communicate information about them across all points of the network in real time, shrinking attack, intrusion, and breach windows.

5. CONCLUSIONS

Compounding the threat are prevalent and vulnerable Internet of Medical Things (IoMT) devices, which integrate components and software from dozens of suppliers with minimal concern for security. Even individual patients can be targeted. It's a dire situation that must be addressed. Hospitals and other healthcare providers must practice

better cybersecurity hygiene. This article surveyed the possible attacks on the new IoMT and provided some suggested remedies to prevent such attacks.

REFERENCES

[1] Frost & Sullivan, Internet of Medical Things Spurs Home Healthcare Industry Growth Through Enabling Wearables and e-Skin Devices, September 07, 2018, Available Online: https://ww2.frost.com/news/press-releases/internet-medical-things-spurs-home-healthcare-industry-growth-through-enabling-wearables-and-e-skin-devices/

[2] Zlata Rodionova, Healthcare is now top industry for cyberattacks, the Independent, Thursday 21 April 2016, Available Online: https://www.independent.co.uk/news/business/news/healthcare-is-now-top-industry-for-cyberattacks-says-ibm-a6994526.html

[3] Suzanne Schwartz, Premarket Submissions for Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Staff, Food and Drug Administration (FDA), October 18, 2018, Available Online:https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf

[4] Mildred Segura, Christopher M. Butler, Farah Tabibkhoei and Reed Smith, The Internet Of Medical Things Raises Novel Compliance Challenges, Medical Devices Online, January 3, 2018, Available Online: https://www.meddeviceonline.com/doc/the-internet-of-medical-things-raises-novel-compliance-challenges-0001

[5] Craig Badrick, Best Practices in IoMT Security, Turn Key Technologies, January 4th, 2019, Available Online: http://www.turn-keytechnologies.com/blog/network-solutions/best-practices-iomt-security

[6] John Haughey, Karen Taylor, Michael Dohrmann and Glenn Snyder, Medtech and the Internet of Medical Things: How connected medical devices are transforming health care, Deloitte 2018, Available Online: https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html

[7] Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend, White Paper May 2017, Available Online: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf

[8] Amy Young, What Internet of Medical Things (IoMT) Devices Mean for Healthcare Cybersecurity Vulnerable IoMT devices, April 2018, Available Online: https://healthtechmagazine.net/article/2018/04/The-Internet-of-Medical-Things-Opens-Health-Organizations-Up-to-More-Threats

[9] Jonathan Nguyen-Duy, Healthcare's Secret Weapon for Securing the IoMT, CSO Report, FEBRUARY 01, 2018, Available Online: https://www.csoonline.com/article/3252150/healthcare-s-secret-weapon-for-securing-the-iomt.html

[10] Murugan Anandarajan and Sarah Malik, Protecting the Internet of medical things: A situational crime-prevention approach, Cogent Medicine (2018), 5: 1513349, Available Online: https://www.cogentoa.com/article/10.1080/2331205X.2018.1513349.pdf

[11] Ladi Adefala, Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries, CSO ONLINE, MARCH 06, 2018, Available Online: https://www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html

