e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.327

Volume 7, Issue 4, April 2019

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Distributed Denial of Service (DDoS): A Threat to Medical Internet of Things

"A review on MIoT mitigation scheme against DDoS attacks"

Bren C. Bondoc, MSIT
Faculty, College of Information Communications Technology,
Nueva Ecija University of Science and Technology
Palayan City, Nueva Ecija, Philippines

Abstract: ***The medical field is an integral part of the Internet of Things. This study determined the various DDoS vulnerability of MIoT devices, and determined the impact of DDoS attacks on MIoT. Further to compared and evaluated existing DDoS mitigation schemes of MIoT devices. This material has been sourced from scientific databases, related business manuals and journals. Relatively suitable records were chosen for considering medically implanted IoT products Based on the gathered literature, the researcher drawn three conclusions. First, it has been disclosed that there are already cyber vulnerabilities in MIoT devices that endanger the safety and security of users/patients. Thus, it is suggested that stringent periodic system protection patches should be given since most bugs have been triggered by obsolete security devices. Second, it can be inferred that an attack on MIoT devices can cause life-threatening incidents. Thus, it is recommended that a nation reviews the legislative system to ensure sufficient protections for cyber security to prevent crimes. Third, there are DDOS mitigation schemes that can be used by healthcare providers. In order to maximize its security and minimize the risks of DDOS attacks, it is advised to build, develop and utilize these preventive programs.***

Keywords: Medical Internet of things, Distributed Denial of Service.

I. INTRODUCTION

Internet of Things or IoT would be a series of interconnected devices using linked sensors and machine learning to share data over a network [1]. It has been gaining popularity almost everywhere in the world as the need for seamless human interaction increases. It has been utilized by different fields, especially in the field of medicine known as the Medical Internet of Things (MIoT). However, the present IoT devices are vulnerable and insufficiently developed because of the scarce resources in IoT devices, immature requirements, and the absence of stable hardware and software design, development, and implementation [2].

The medical field is an integral part of the Internet of Things. With the use of MIoT devices, capturing health data, monitoring, and communication was made easy. It benefits not only the healthcare providers but also the patients as it revolutionizes the way of providing treatments. Further, in assisting the physicians and medical staff to track the care of patients, create customized health resources like alarm and medications reminder, and provide personalized access to information on the health information accessible on the Internet this modern integration architectural model can be used [3]. Hence, these medical IoT devices need to be studied and reexamined by regulators and medical networks to raise understanding of possible privacy breaches [4].

With the increasing number of MIoT devices, it faces new challenges such as threats to privacy and security. A common threat is the DDoS attack, which aims to overpower a target server by sending large amounts of requests. The large volume of and widespread presence of IoT devices has attracted a wide array of bad actors, especially those orchestrating DDoS attacks [5]. In addition, as devices and software implementations shift constantly, it poses the issue of continuing validity of any risk and threat evaluation [6].

In the light of the above, the researcher analyzed the academic papers on the protection of MIoT to contribute awareness to the society.

II. Objectives

The primary focus of this paper is to analyzed academic papers on the protection of MIoT to contribute awareness to society. It aims to determine various DDoS Vulnerabilities of MIoT devices and determine their impact on MIoT devices. Moreover, this paper leans to compare and evaluate existing DDoS mitigation schemes of MIoT devices.

III. Methodology

One purpose of this study is to examine and outline existing threat environment that is faced by health providers, physician associations, and hospitals that handle medical IoT. Literature review serve as a framework for awareness creation, establish guidance for policy and practice, provide proof of an impact, and theoretically encourage new directions in the field [7]. This material has been sourced from scientific databases, related manuals and journals. Relatively suitable records were chosen for considering medical IoT products. A broad range of scholarly papers and industrial research are accessible to the author. The following keywords were used to search on papers indexed by Google Scholar: 'MIoT,' 'DDoS,' 'DDoS vulnerability,' and 'DDoS mitigation.' Searches is limited to peer reviewed articles and conference papers with published dates within 15 years (2005-2020). The databases (e.g. IEEE, FDA, arXiv, Sensors) in this paper have been deliberately chosen from technical and medical literature. Hence, the articles cited in this paper were those of free access or open access journals. Further, the chosen journal articles have at least 5 citations as enhancement to its credibility. Thus, the MIoT devices vulnerable to DDoS attacks were already reported and proven as these were communicated through FDA Safety Communications.

IV. Results and Discussions

This section presents the findings on articles that have been collected and examined.

TABLE I DDoS vulnerability of MIoT devices.

Title	MIoT Device	Description	Vulnerability	Cause of Vulnerability
[8]	Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems	remote devices that continually distribute anesthetic and/or medicinal medications can be configured directly through a healthcare provider's local area network	If an unauthorized party has access to the infusion pump, they will remotely change the dose it provides, which may result in over-or under-injection of such drugs	May harm the user/patient using the MIoT device
[9]	St. Jude Medical implantable cardiac devices and St. Jude Medical Merlin@home Transmitter	uses an embedded cardiac unit that wirelessly connects with computers in a facility to read the data stored on the implant.	An altered Merlin@home transmitter could give unnecessary pacing signals to the embedded device, which could result in rapid battery fatigue and/or the	Stoppage of MIoT device

			application of shocks.	
[10]	Abbott's Implantable Cardiac Pacemakers	ECG pads are inserted under the skin by positioning it in the upper chest region, and have connecting insulated wires called leads that go into the heart.	Unauthorized access would allow alteration of programming commands to the implanted defibrillator, which may result in the unsafe transmission of shocks to the patient	May harm the user/patient using the MIoT device
[11]	Medtronic CareLink Programmer (model 2090) and MyCareLink Monitor (models 24950 and 24952)	used during implantation and follow-up appointments, and for wireless connection to the patient's implanted unit, for Medtronic ICDs and CRT-Ds, respectively.	The protection measures of the new configuration include: only the patient's physician will trigger the procedure, activation times differ by patient, and an unauthorized person will need to be near to the computer, console or clinic programmer to take advantage of the vulnerabilities	Interruption in monitoring/tracking the user/patient
[12]	Medtronic MiniMed Insulin Pumps	helps manage insulin levels and take on some of the responsibilities associated with diabetes management to allow patients to focus more on their everyday lives.	It is possible that an unauthorized person might link wirelessly to a nearby MiniMed insulin pump and adjust the settings to either over-deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or avoid insulin transmission, leading to high blood sugar and diabetic ketoacidosis	May harm the user/patient using the MIoT device
[13]	URGENT/11	Remotely helps users to remotely monitor the medical system and adjust its function.	If these devices are tampered with, they can cause denial of service, or information leaks or logical flaws, which may prevent their use.	Interruption in monitoring/tracking the user/patient
[14]	GE Healthcare Clinical Information Central Stations and Telemetry Servers	used in hospitals to provide information including medical data so that healthcare	In the configuration of a medical system, these vulnerabilities may cause the	Interruption in monitoring/tracking the user/patient

		employees can determine the condition of patients from a central location.	intruder to gain control over the equipment and adjust the alarms.	
[15]	SweynTooth	With Bluetooth technology, two devices can pair and transmit information to one another while maintaining maximum battery power.	Crashing the system may stop communicating or stops running, blocking the device may freeze and stop working properly, and bypassing protection to control the device features usually only accessible to an approved user	Stoppage of MIoT device

Table 1 shows different MIoT devices are classified as vulnerable (V) to DDoS attacks. This lead to a review of the inherent hazards and weaknesses of MIoT systems. Most of MIoT devices could compromise the privacy and protection of the user if successfully ddos attacked.

Based on Table 1, three MIoT devices which configures the system may cause interruption in tracking a patient. One of worst possible case scenarios is "…when the intruder gain control over a medical system [14]." This could lead to uncertainty for employees whose role is to track a patient, particularly when issuing or updating the patient's chart. Further, "… schedule and follow up appointments may differ [11]" and "…which may prevent their use (i.e. monitor the medical system and adjust its function) [13].

Certain MIoT devices have vulnerability which may harm the patient if there is unauthorized access are the following: "…they will remotely change the dose it provides [8]," "…alteration of commands…may result in unsafe transmission of shocks to the patient [10]," and "…deliver insulin to patients…which may result to low or high blood sugar [12]." This means that the infiltration of MIoT instruments will aggravate the illness of the patient. Thus, the patient's condition will worsen.

In addition, one of the vulnerabilities is causing MIoT devices to freeze or cease such as "…which could result in rapid battery fatigue and/or application of shocks [9]" and "…may stop communicating or stop running, blocking the device may freeze and stop working properly [15]." It means that stopping MIoT devices if they are unnoticed, particularly those life-sustaining medical devices, will lead to one's death.

TABLE III Impact of DDOS attacks to MIoT devices

Title	MIoT device	Impact of DDOS Attacks
[16]	Medical Devices with S-Health Fingerprinting	Attackers can emulate the s-health actions of traffic compromising protection in fingerprints and authentication techniques.
[17]	Medical Wearable Devices	Attacks aimed to manipulate the contact between customers and providers in a cloud environment when they access user accounts and use legal access afterwards.
[18]	Insulin Pump	Attackers can alter wireless pump commands previously emitted, create unauthorized wireless pump commands, modify software or configuration from a remote location, and deprive the pump system of any contact.
[19]	Pacemakers and Implantable Cardiac Defibrillators	By exploiting these radio-frequency powered embedded computers attackers are able to track chronic diseases and modify patients automated therapies.

Table 2 shows the possible impact of ddos attacks to MIoT devices. The privacy and data security are two essential components of health care because we take care of peoples' privacy and confidentiality [16]. If there has been a breach of the security or the data have been monitored, the data will be used for more malicious activities or to build a victim's profile [17]. An intruder may gather information about the person using the MIoT system, as well as information about themselves and combine it with their other smartphone data to create comprehensive profiles about the user, including possible health problems. Sensitive patient information was collected from wearable medical devices networked through fiber cables and wireless connections [17]. For instance, a malicious actor may prevent the pump from interacting with the insulin control, and prevent the patient from injecting insulin as required, possibly resulting in death [18]. Further, these computers and radios are used to communicate with machines outside the body, providing the malicious agent with ability to intercept the signals and interfere with the operation of the medical system [19]. In light of the foregoing results, it can be inferred that an attack on MIoT devices can cause life-threatening incidents.

TABLE III Existing DDOS mitigation scheme

Title	Contribution of Study
[20]	This study indicated that infringements like TCP transmission can be overcome by applying the AllowTcpForwarding No to the global ssh configuration file and advised connection to every TCP port safely via the Internet without the use of port transmission.
[21]	This study suggested the use of Ethereum blockchain smart contracts to defend and monitor in a way that is decentralized and vulnerable to popular cybersecurity attacks.
[22]	The study proposed that the Machine Learning approach would provide an effective atmosphere to dramatically managed DDoS attack.
[23]	This paper proposed an adaptive and intelligent secure framework that can detect and mitigate DDoS attacks.
[24]	The paper outlines a network management framework that offers on-demand DDoS mitigation capabilities to ISP users, making it easier for them to collaboratively thwart DDoS attacks.
[25]	This paper suggested an algorithm for detecting and preventing Distributed Denial of Service (DDoS) attacks with the proposed SD-IoT Platform.
[26]	This paper suggested a lightweight DDoS mitigation mechanism at the edge of the network utilizing the restricted resources of low-cost computers.
[27]	The present study developed a taxonomy in which techniques for mitigating DDoS attacks using SDN technologies in IoT environments were identified and characteristic.
[28]	This paper introduces a blockchain-based DDoS mitigation scheme called CoChain-SC that incorporates intra-domain and inter-domain mitigation.

Increasing security features for on-board devices is one potential way to decrease botnet accesses to target's computers. For that reason, based on the results that were analyzed, it was suggested that education should make protection for its students a fundamental move, not an afterthought. Pre-development developers should address the right tools such as the OWASP (Open Internet Application Security Project) with parts such as 'IoT bugs' and the 'IoT Security Guide [20].'

Blockchain is intended to address problems related to user security and access control for MIoT devices, without the intervention of trusted intermediaries or centralized agencies. Based on the results, almost all security integrity, functionality, and accountability goals are met except for confidentiality. Therefore, solution uses Ethereum, a public or transparent blockchain network, in which all activities are simple to check and validate their content through public minder nodes. However, privacy can be accessed by means of the private or approved Ethereum network if documents and transactions are expected to be confidential [21].

If the IoT devices do not have any basic software running in them, like network administrator needs, the gateways which link the devices to the networks must come up with basic security features allowed such as WPA2, DNSSEC, etc to improve and update both network and devices security features. Approaches to Machine Learning (ML) can be used for attack detection.

For example, an automatic solution has been built to bypass cyberattacks and is combined with DPI that detects even unknown attacks in both inbound and outbound traffic [22].

Based on a suggestion from any detection module, the REST program compiles rules collection, and applies rules for attack traffic, regular traffic and unknown traffic to the application FLOW RULE Generator; the rules are then pointed through the SDN controller using the PUSH REST API. Thus, the switching table of Openflow switch are modified based on flow rate rules presented by the SDN controller. This will restrict how much an attacker is capable to hack and still deliver the service to the authorized user. Further, this is particularly useful for the cost-benefit analysis of deterrence of threats [23].

SDN controllers use behavior-based protocols and complex modifications to manage malicious and suspicious flows. Authentication and checking of security policies and regulations is required before they are implemented on data plane network devices in order to safeguard the SDN infrastructure from attacks by means of northern bound APIs. The research is therefore restricted to the actual system, but the study aims to evolve expanded to one-to-more than one-mode, i.e., through requisitioning several ISSPs for a mitigation of attacks, by correctly solving the scalability of controllers and rule dispute issues [24].

The proposed method will classify the target of a DDoS attack from an IoT computer within a shorter time span, easily manage and minimize the DDoS attack, and eventually improve the unveiled glaring weaknesses in IoT. Further, the proposed algorithm will locate the IoT system from which a DDoS attack is initiated within a shorter period of time based on the simulation results, easily manage and minimize the DDoS attack, and eventually strengthen the discovered glaring shortcomings in IoT, in which the terminal devices have limits on computing and memory specifications [25].

Based on the study, it was possible to build a control node explicitly for extra demand in storage space. In addition, in an IoT end network, it may also enter local police traffic and respond quickly to an old archived intruder. Usually, for a community of operating nodes in a local network, one control node is used. Therefore, to compensate for the reduced space of the operating nodes, it is permissible to provide larger processing power and power supply. Therefore, the control node should be able to alert the operating nodes of the situation after finding archived intruder operations on the local network. [26].

Through random shuffling of queue allocation, this process detects malicious flows and the packets of detected flows are discarded without queuing. Based on the proposed method, it makes it easy to track and minimize ddos attack such as UDP floods quickly. Via computer simulation, it was verified that when using 7 pools for queue allocation, the proposed algorithm detected more than 100 flows. With the proposed method, even on low-cost computers with minimal resources, DDoS attacks will simply be mitigated. [26].

Malicious flow filters have succeeded in minimizing DDoS attacks when heavy traffic is present, but struggle to reduce DDoS attacks with low traffic volumes. In order to provide an optimum evaluation calculation, suitable main performance index such as KPIs are needed depending on the specific resource constraints in the IoT infrastructure. High-precision analysis and observations from these real-world experiments would have the ability to further improve the new proposed taxonomy. [27].

Further, it is necessary to protect the pseudonymity and anonymity of the address of the collaborators so as to prevent traceability of the identity of the author of the letter; otherwise, they would be a direct object of a DDoS attack. The suggested approach for intra-domain merged I-ES with I-BS to track illegitimate flows in real-time, and I-DM to efficiently minimize illegitimate flows within the domain. A smart contract-based platform that allows use of Ethereum's smart contract technologies was proposed for interdomain to promote collaboration among SDN-based domain peers. [28].

V. Conclusion and Recommendation

Based on the gathered literature, the researcher drawn three conclusions. First, it has been disclosed that there are already cyber vulnerabilities in MIoT devices that endanger the safety and security of users/patients. There were three cases of

vulnerability discussed in this study: (1) it may cause interruption on medical system, (2) it may harm the patient using MIoT, and (3) it may cease the medical device to operate. Thus, it is suggested that stringent periodic system protection patches should be given since most bugs have been triggered by obsolete security devices. Second, it can be inferred that an attack on MIoT devices can cause life-threatening incidents. Thus, it is recommended that a nation reviews the legislative system to ensure sufficient protections for cyber security to prevent crimes. Third, there are DDOS mitigation schemes that can be used by healthcare providers. In order to maximize its security and minimize the risks of DDOS attacks, it is advised to build, develop and utilize these preventive programs.

References

1. Rahman, M. A., & Asyhari, A. T. The emergence of internet of things (Iot): Connecting anything, anywhere. MDPI. 2019.
2. Khan, M. A., & Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018.
3. El Kafhali, S., & Salah, K. Performance modelling and analysis of Internet of Things enabled healthcare monitoring systems. IET Networks, 2018.
4. Wood, D., Apthorpe, N., & Feamster, N. Cleartext data transmissions in consumer iot medical devices. 2017
5. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. DDoS in the IoT: Mirai and other botnets. Computer, IEEE. 2017
6. Darwish, S., Nouretdinov, I., & Wolthusen, S. D. (2017). Towards composable threat assessment for medical IoT (MIoT). Procedia computer science, 2017.
7. Ramalho, R., Adams, P., Huggard, P., & Hoare, K (2015). Literature review and constructivist grounded theory methodology. Forum Qualitative Sozialforschung Social Research. 2015.
8. Administration, U.S.F.a.D. LifeCare PCA3 and PCA5 Infusion Pump Systems by Hospira: FDA Safety Communication - Security Vulnerabilities. 2015 [Online]. Available: https://wayback.archiveit.org/7993/20170112164109/http:/www.fda.gov/ Safety/MedWatch/SafetyInformation/SafetyAlert sforHumanMedicalProducts/ucm446828.htm [Accessed: 2019]
9. Administration, U.S.F.a.D. Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication. 2017 [Online]. Available: https://www.fda.gov/medical-devices/safetycommunications/cybersecurity-vulnerabilitiesidentified-st-jude-medicals-implantable-cardiacdevices-and-merlinhome. [Accessed: 2019]
10. Administration, U.S.F.a.D. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. 2019. [Online]. Available: https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals. [Accessed: 20119]
11. Administration, U.S.F.a.D. Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication. 2019 [Online]; Available: https://www.fda.gov/medical-devices/safetycommunications/cybersecurity-vulnerabilitiesaffecting-medtronic-implantable-cardiac-devicesprogrammers-and-home. [Accessed: 2019]
12. Administration, U.S.F.a.D. Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication. 2019. [Online]. Available: https://www.fda.gov/medicaldevices/safety-communications/certainmedtronic-minimed-insulin-pumps-havepotential-cybersecurity-risks-fda-safetycommunication. [Accessed: 2019]
13. Administration, U.S.F.a.D. URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication. 2019. [Online]. Available: https://www.fda.gov/medical-devices/safetycommunications/urgent11-cybersecurityvulnerabilities-widely-used-third-party-softwarecomponent-may-introduce. [Accessed: 2019]
14. Administration, U.S.F.a.D. Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: FDA Safety Communication. 2019. [Online]. Available: https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-ge-healthcare-clinical-information-central-stations-and. [Accessed: 2019]
15. Administration, U.S.F.a.D. SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication. 2019. [Online]. Available: https://www.fda.gov/medicaldevices/safety-communications/sweyntoothcybersecurity-vulnerabilities-may-affect-certainmedical-devices-fda-safety-communication. [Accessed: 2019]
16. A. A. Abdellatif, A. Mohamed, C. F. Chiasserini, M. Tlili and A. Erbad, "Edge Computing for Smart Health: Context-Aware Approaches, Opportunities, and Challenges," in IEEE Network, 2019.
17. Langone, M., Setola, R., & Lopez, J. (2017). Cybersecurity of wearable devices: An experimental analysis and a vulnerability assessment method. In 2017 IEEE 41st Annual Computer Software and Applications Conference
18. Nathanael Paul et al., A Review of the Security of Insulin Pump Infusion Systems, 5 J. OF DIABETES SCI. & TECH. [Online] Available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3262727. 2011. [Accessed: 2019]
19. Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., ... & Maisel, W. H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. IEEE. 2008.
20. J. Wei, Final Project, 2016.

21. M. Alblooshi, K. Salah, and Y. Alhammadi, "Blockchain-based Ownership Management for Medical IoT (MIoT) Devices," IEEE, 2018. [Online]. Available: https://www.researchgate.net/profile/Khaled_Salah7/publication/328828331_Blockchain-based_Ownership_Management_for_Medical_IoT_MIoT_Devices/links/5be52e2d92851c6b27b13456/Blockchain-based-Ownership-Management-for-Medical-IoT-MIoT-Devices.pdf. [Accessed: 2019].
22. D. Gurusamy, D. Priya M, B. Yibgeta, and A. Bekalu, "DDoS Risk in 5G Enabled IoT and Solutions," International Journal of Engineering and Advanced Technology (IJEAT), 2019.
23. A. Alshamrani, A. Chowdhary, S. Pisharody, D. Lu, and D. Huang, "A Defense System for Defeating DDoS Attacks in SDN based Networks," Proceedings of the 15th ACM International Symposium on Mobility Management and Wireless Access, 2017. [Online]. Available: https://www.researchgate.net/profile/Ankur_Chowdhary/publication/321087803_A_Defense_System_for_Defeating_DDoS_Attacks_in_SDN_based_Networks/links/5b5f48c0458515c4b2532382/A-Defense-System-for-Defeating-DDoS-Attacks-in-SDN-based-Networks.pdf. [Accessed: 2019].
24. Sahay, R., Blanc, G., Zhang, Z., & Debar, H. Towards autonomic DDoS mitigation using software defined networking. NDSS Workshop on Security of Emerging Networking Technologies, 2015.
25. Yin, D., Zhang, L., & Yang, K. A DDoS attack detection and mitigation with software-defined Internet of Things framework. IEEE Access, 2018.
26. Zhang, C., & Green, R. Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. In Proceedings of the 18th Symposium on Communications & Networking, 2015.
27. Shameli-Sendi, A.; Pourzandi, M.; Fekih-Ahmed, M.; Cheriet, M. Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing. J. Netw. Comput. Appl. 2015
28. B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, ''A blockchain-based architecture for collaborative ddos mitigation with smart contracts,'' in Security of Networks and Services in an All-Connected World, D. Tuncer, R. Koch, R. Badonnel, and B. Stiller, Eds. Cham, Switzerland: Springer, 2017.

