Advances in Networks
2021; 9(1): 1-18
http://www.sciencepublishinggroup.com/j/net
doi: 10.11648/j.net.20210901.11
ISSN: 2326-9766 (Print); ISSN: 2326-9782 (Online)

Security Performance of Internet of Medical Things

Taiwo Adenaiye, Waleed Bul'ajoul*, Funminiyi Olajide

School of Science and Technology, Nottingham Trent University, Nottingham, UK

Email address:
bulajoul@gmail.com (W. Bul'ajoul), toyinadenaiye@gmail.com (T. Adenaiye), funminiyi.olajide@ntu.ac.uk (F. Olajide)
*Corresponding author

To cite this article:
Taiwo Adenaiye, Waleed Bul'ajoul, Funminiyi Olajide. Security Performance of Internet of Medical Things. *Advances in Networks.* Vol. 9, No. 1, 2021, pp. 1-18. doi: 10.11648/j.net.20210901.11

Received: January 11, 2021; **Accepted**: January 18, 2021; **Published**: February 2, 2021

Abstract: Internet of Medical Things is the internet connection of medical devices to perform services and processes to support the healthcare sector. Wearable Technology in Healthcare has seen tremendous growth in recent times. This is due to a global increase in the aging population, the need for disease management, and effective patient monitoring. The prevalent technology of wearable devices is Bluetooth technology due to its low cost, low energy, and size. Despite the growth recorded in the adoption of Bluetooth Wearable IoMT, there are concerns by users and other healthcare stakeholders about security and privacy issues with its adoption. Our paper presents a simulation of passive and active attacks on 3 wearable IoMT devices, followed by analysis and evaluation of the experiment outcomes. Thereafter, countermeasures for the identified weaknesses were provided. It was discovered that some of the standard security features of Bluetooth Technology to mitigate privacy and security issues were not implemented in some of the devices, which can result in data compromise in the devices. A security assessment framework was developed to assess the security of Bluetooth IoMT devices using the Bayesian Network model. This is used to rank devices, identify their vulnerabilities, and apply security measures on the identified vulnerabilities. Our paper further provides recommendations on improving the security of Bluetooth IoMT devices.

Keywords: Internet of Medical Things, Man-in-the-Middle Attack, Bluetooth Wearable IoMT, Wearable Device Security, Security Assessment Framework

1. Introduction

Internet of Medical Things is the connection of medical devices to the internet to perform services and processes to support the healthcare sector. Wearable Healthcare devices, a branch of Internet of Medical Things, are regarded as one of the fastest-growing markets in recent times. This growth is expected to continue due to increase in device adoption, popularity, functionality, and innovation [1]. Although, there are security concerns about the continued adoption of IoT devices for healthcare, Internet of Medical Things still accounts for one-third of the Internet of Things [2]. This is because patients' health can be enhanced with IoMT adoption for patient remote monitoring. Also, Muck explains that IoMT devices may be an easy target for attackers to launch a distributed denial-of-service attack on [3].

Recent research shows that there is a dearth of effective IoT security assessment framework in the cyber-security space [4]. Moreover, for security to be implemented, it needs to be measurable. This shows the importance of developing a security assessment framework for Bluetooth Wearable Internet of Medical Things to measure the security posture of the devices. The developed Security Assessment Framework for Bluetooth Wearable IoMT will provide a relevant resource in the cyber-security space specifically for the healthcare sector and assist to mitigate security and privacy risks.

Previous work shows that security and privacy concerns are prevalent in the adoption of healthcare devices [5, 6]. Furthermore, the security assessment frameworks that had been developed previously were broadly for the Internet of things generally however, none of the previous work focused on the security assessment framework for the Bluetooth Internet of Medical Things. Also, these general security assessment frameworks are not designed for specific device security features assessment or vulnerability impact assessment. Thus, they are not effective for assessing the Bluetooth IoMT devices.

The contributions of our paper include the investigation of

the security performance of 3 Bluetooth technology-based IoMT devices and the development of Security assessment framework based on Bayesian Network model and NIST CVE. The Security Assessment Framework was used to assess security levels of the IoMT devices.

2. Related Work

Hale presented an open-source platform (Secuwear) for identifying vulnerabilities in wearable hardware and software [7]. The Secuwear platform is designed in a way to separate the Wearable Systems Network into different domains for ease of testing and isolating the vulnerabilities. This study elaborated on the connection between the wearable device and the mobile application on the Central device. The platform was used to simulate attacks on Bluetooth which included the Denial of Service and Man-in-the-Middle attacks. Our research however focuses on developing security assessment framework for Bluetooth IoMT and associating the implementation or non-implementation of Bluetooth NIST recommended security features. Furthermore, Yaseen describe a framework to detect, analyse, and mitigate Bluetooth vulnerabilities while simulating Man-in-the-middle attacks on No Input No Output (NiNo) devices [8]. Our research describes a framework for assessing security levels of Bluetooth IoMT based on their security features. This assessment framework provides a comparison of the security levels of the Bluetooth IoMT devices.

Melamed discussed Bluetooth technologies and connections. Also, the MitM attack was explained and simulated in the research. Although some Bluetooth vulnerabilities were considered, countermeasures and assessment framework for Bluetooth was not discussed [9].

Alsubaei designed a taxonomy and risk assessment model for security and privacy in IoMT. The study classifies security and privacy issues related to IoMT. The taxonomy used included IoT layers, possible intruders, compromise level e.t.c. [2]. The IoMT layers are mapped with the types of medical devices, the difficulty of attack, CIA compromise, attack method, compromise levels, and attack origin. Furthermore, vulnerability identification and quantification were done, the severity and likelihood of risks computed, and attack probability calculated. The study developed an assessment model where a user defines the weights of risks. Although, our research developed a security assessment framework, it however focuses on Bluetooth IoMT using Bayesian Network Model Methodology.

Conversely, Darwish proposed a model that will enhance risk and threats assessments in the IoMT environment [10]. The study identifies 6 major security goals in IoMT. This includes device integrity, data integrity, confidentiality, availability, privacy, and security usability. Also, the study proposes a taxonomy for the type of target data. These are data disclosure, alternation, inaccessibility, and process/control/code manipulation. The risk and threat analysis standard used was adapted from the HSG ISI. Furthermore, the Focus of interests (FoI) is identified for IoMT devices. This report categorised identified threats into static and dynamic properties. The static attributes are triggered only when a new device is added to the system while dynamic composability property is for regular, periodic assessment of the identified IoMT devices. The threat analysis further integrates the classification of data threats. Although, the drawback of this assessment model is that it does not include device security assessment. However, it focuses more on data security, which is of great importance in the healthcare sector, even though a compromised device may consequently make data less secure [11]. Our research further shows that the implementation of security features in Bluetooth IoMT directly impacts on the security levels of the devices.

Furthermore, Alsubaei developed a web-based assessment framework that identifies IoMT security threats, recommends security measures and further measures, and ranks two or more IoMT solutions by the degree of their security [12]. The Analytic Hierarchy Process multi-criteria decision-making method was used to process the multiple criteria derived from the use of security objectives and the solution security assessment. The limitations of this study include the complexity in defining 260 security attributes and stakeholders finding it difficult to understand them. Also, 3 stakeholders were identified in this study and the general IoMT environment was discussed without addressing specifically the peculiarities in Bluetooth IoMT devices.

Our paper focuses on developing a security assessment model for assessing security in Bluetooth IoMT devices. The assessment model ranks and assesses the devices based on the implementation of security features. The paper also presents additional measures to increase the security of the IoMT devices.

3. Experiment Design and Methodology

The paper investigates the security features in Bluetooth IoMT devices based on the NIST Recommendations and Bluetooth Standard Specifications. Experiments were carried out on 3 Wearable IoMT devices to assess the security features integrated into them. Also, vulnerabilities in the devices were identified and a security assessment framework was developed to assess the security levels of the IoMT devices.

The design and implementation of the experiment investigated the security features and vulnerabilities of the wearable IoMT devices.

Figure 1 shows the design of the experiment conducted. The CSR 8510 USB dongles were used to simulate the Clone Peripheral and Clone Mobile device. The btlejuice tool was installed and setup on 2 Kali Linux Virtual machines. Also, the central device (Mobile device) and the IoMT devices (Fitbit Charge 3, 116Plus Smart watch and Braun iCheck7 Wrist Blood Pressure Monitor) are the BLE Wearable IoMT devices represented in the design.

These IoMT devices were termed Device A, Device B, and Device C.

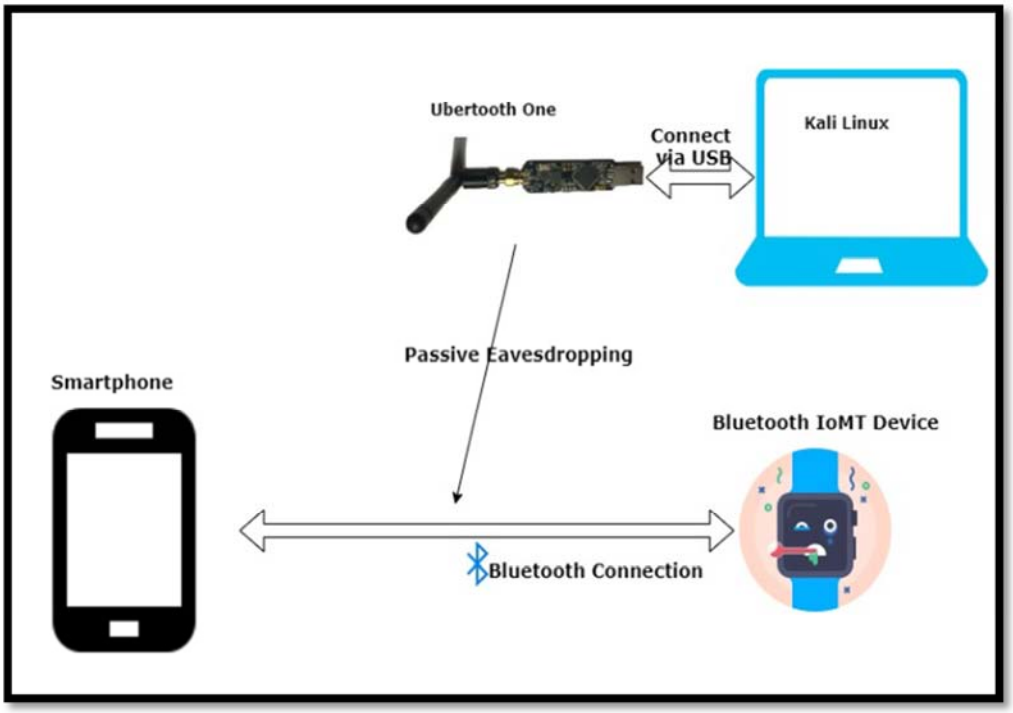

Figure 1. *Project Experiment Design*

Reconnaissance and information gathering on the IoMT devices was done using bettercap tool, gattool and hcitool.

Figure 2 shows the Passive Eavesdropping which was conducted first to sniff Bluetooth Packets between the connected Bluetooth devices (IoMT and the Mobile Device) while the active eavesdropping attack/ MitM attack was performed to connect with the Bluetooth devices and access confidential health data. The passive eavesdropping experiment was conducted using Ubertooth One, and packet Monitoring Tool (Wireshark) to capture Bluetooth Packet and analyse the packets. Furthermore, the MitM attack was simulated using btlejuice framework installation setup on 2 Kali Linux Virtual Machines and 2 CSR USB dongles.

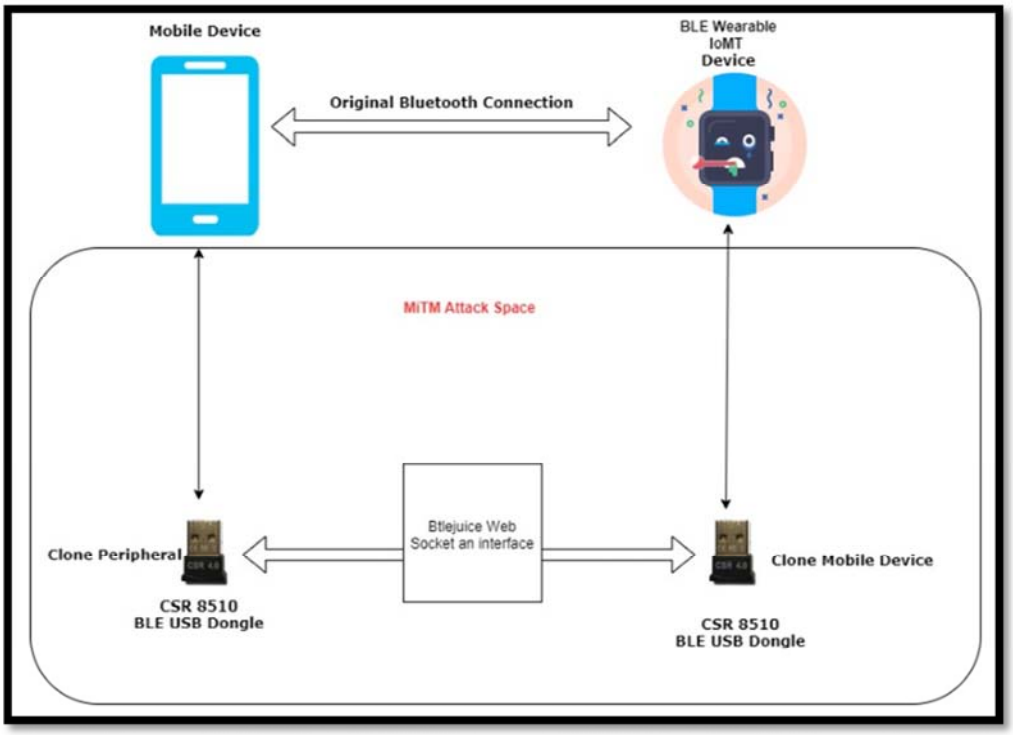

Figure 2. *Design showing the Ubertooth One sniffing Bluetooth Packet in the Communication (Peripheral) and the Mobile Device (Central).*

Table 1. *Tools.*

S/N	Name	Purpose of use
1	BtleJuice	This was used to perform a MitM attack simulation on Bluetooth Low Energy devices. It was selected for use because it comprises an interception core, interception proxy, a dedicated web interface, python and Node.js bindings.
2	Ubertooth One	This device was selected for the experiment because of its cost-efficiency and its effectiveness for sniffing Bluetooth packets. This hardware device was used to sniff Bluetooth packets in the project experiments.
3	Wireshark	Open-Source Network Protocol/ Packet Analyser. Wireshark was used with the Ubertooth One device to capture Bluetooth Low Energy packets. The Wireshark tool was selected being an effective network monitoring tool.
4	Gattacker	This is used to simulate a MitM attack by creating a copy of the attacked device as a clone, tricks the mobile application to connect to it, and then forward data exchanged on the cloned device with the mobile application.
5	CSR 8510	CSR 8510 are USB Bluetooth dongles used to simulate a man-in-the-middle test environment. One of the dongles was used to simulate the fake peripheral while the second was used to simulate the central device. These dongles were chosen for the experiment as they are fit for purpose and cost-effective.
6	Bettercap	Bettercap: This tool was used for Bluetooth LE reconnaissance tasks.
7	Gattool	Gatttool: This is an open-source tool used to access the services and characteristics running on the Bluetooth device. Special GATT commands were selected because it can discover, read, and write Bluetooth device characteristics using this tool.
8	HCITool	Hcitool: This is an open-source tool used to send special commands to Bluetooth devices. It was used in this experiment because it can identify the Bluetooth BD-ADDR addresses and names of the Bluetooth devices used for the experiment and within range.
9	2 Fitness Trackers and 1 Blood Pressure Monitor (Fitbit Charge3, 116Plus Smart watch and Braun iCheck7 Blood Pressure Wrist Monitor)	2 Fitness Trackers and 1 Blood Pressure Monitor (Fitbit Charge 3, 116Plus Smart watch and Braun iCheck7 Blood Pressure Wrist Monitor) are the devices on which the experiments were conducted. These 3 devices were chosen because they use Bluetooth Technology. The Bluetooth Wearable Blood Pressure monitor used was relatively cost-effective and was investigated as a certified medical device. Although, the two other devices are fitness trackers and were chosen because recent articles report that users consider them as Personal Healthcare devices and may be relevant in personal health monitoring (Henriksen et al., 2018). They are also used to measure health data such as heart rate, SpO_2, and Sleep quality. However, they are not approved medical devices for healthcare monitoring.

Table 2. *NIST Bluetooth Security Features and Recommendations.*

S/No	NIST Recommended Security Feature
1.	Authentication – Authentication deals with identifying the communicating devices. NIST recommends that authentication implemented in communication between the devices however, user's authentication is not provided in Bluetooth security standard. AES-CCM is used in Bluetooth low energy to provide packet authentication
2.	Confidentiality – This is preventing data compromise caused by eavesdropping and preventing unauthorised access to device and data. AES-CCM is used in Bluetooth low energy to provide confidentiality,
3.	Authorization - AES-CCM is used in Bluetooth low energy to provide confidentiality as well as per-packet authentication and integrity
4.	Message Integrity - AES-CCM is used in Bluetooth low energy to provide message integrity.
5	Pairing or Bonding – Pairing options recommended are Passkey Entry and Out of Band (OOB) which provides MitM protection. Just Works pairing should not be used for pairing.
6.	Security Mode 1 Level 4 with Secure Connections authenticated pairing and encryption using AES-CMAC and P-256 elliptic curve.
7.	Privacy Feature should be implemented to prevent devices associated with users over time.

Zhang described Bluetooth Privacy feature which assigns a unique 48-bit BD_ADDR bluetooth device address to a Bluetooth device [13]. The public device address is a 48-bit long number representing the company IP and unique ID assigned by the company. The random address on the other hand can be either a static random address or private random address. The random address is also called resolvable private address.

Zuo discussed the types of attacks as passive and active attacks [14].

In the experiments, the passive attacks are passive fingerprinting and passive eavesdropping - This is achieved through sniffing of the BLE packets communications between the 2 connected Bluetooth devices while the active attack is presented through the unauthorised access attack to the data transmission between the Central and Peripheral Bluetooth devices.

The 3 IoMT devices investigated operate in Bluetooth 4.0 technology.

The experiment screenshots only show data relevant to this research while other device specific data and other confidential data not relevant to this research has been hidden.

The passive fingerprinting and eavesdropping were done using Ubertooth One and wireshark

The Ubertooth One was used to capture Bluetooth Packets and was displayed with the Wireshark application. A pipe was created using the command mkfifo /tmp/pipe and in the Wireshark interface to capture the Bluetooth packets in Wireshark. The command ubertooth-btle -f -c /tmp/pipe was used to capture the ble packets in Wireshark.

Figure 3 shows the successful implementation of passive fingerprinting and eavesdropping. This is accomplished using the Ubertooth one device and packets are captured with the Wireshark tool.

Gatttool: This tool was used to access the Bluetooth services and characteristics of the IoMT devices. Also, the characteristics data was retrieved using the gatttool commands; gatttool -b BDR_ADDR -I random (public), connect, and characteristics command. Also, the char-read-hnd command was used to read the characteristics handle data and the write

command was used to write to the characteristics. This is depicted in Figure 4 while the gattacker tool scan was seen in Figures 5 and 6.

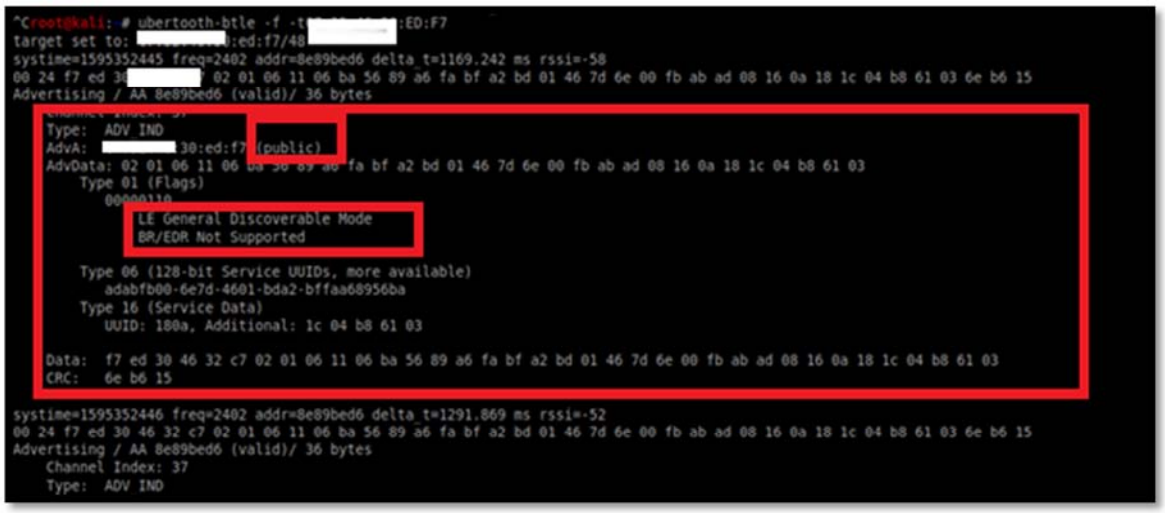

Figure 3. *Ubertooth One capturing advertisement data.*

Device A (Figures 4 – 7).

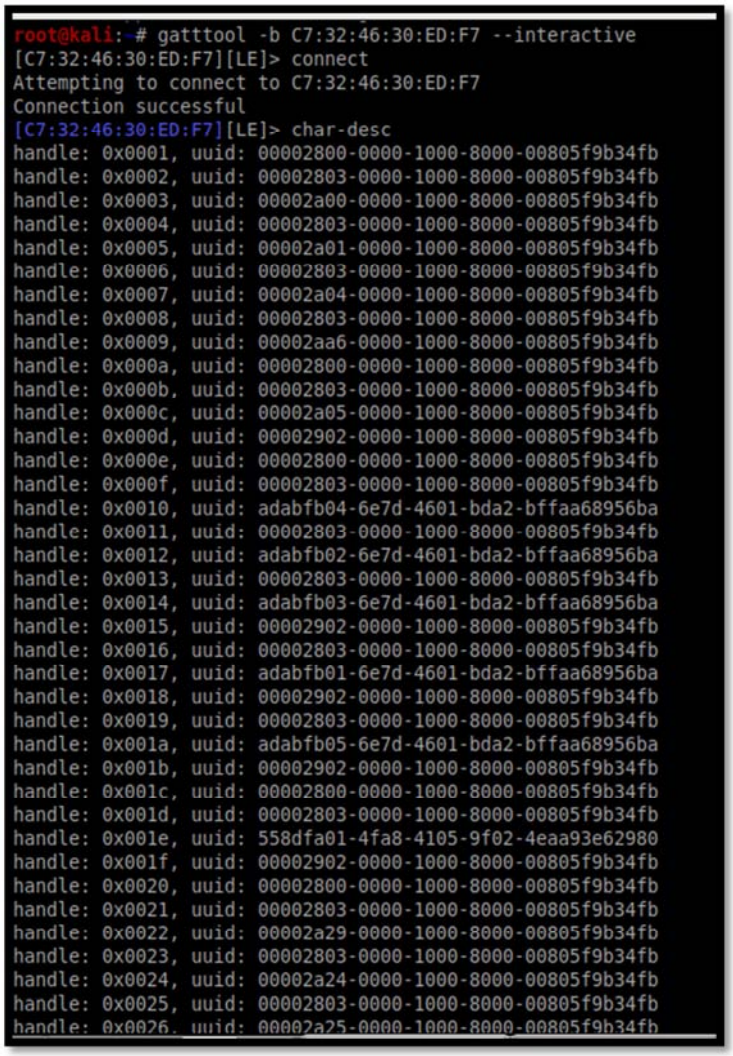

Figure 4. *Gattool on Device A.*

Figure 5. *Gattacker Tool on Device A.*

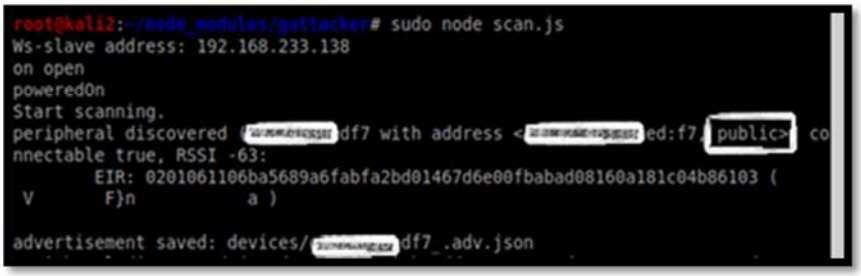

Figure 6. *Gattacker tool scan on Device A (contd).*

In this experiment, Figure 7 shows the process of attempting to access the data in IoMT device A using the btlejuice tool. This was not successful.

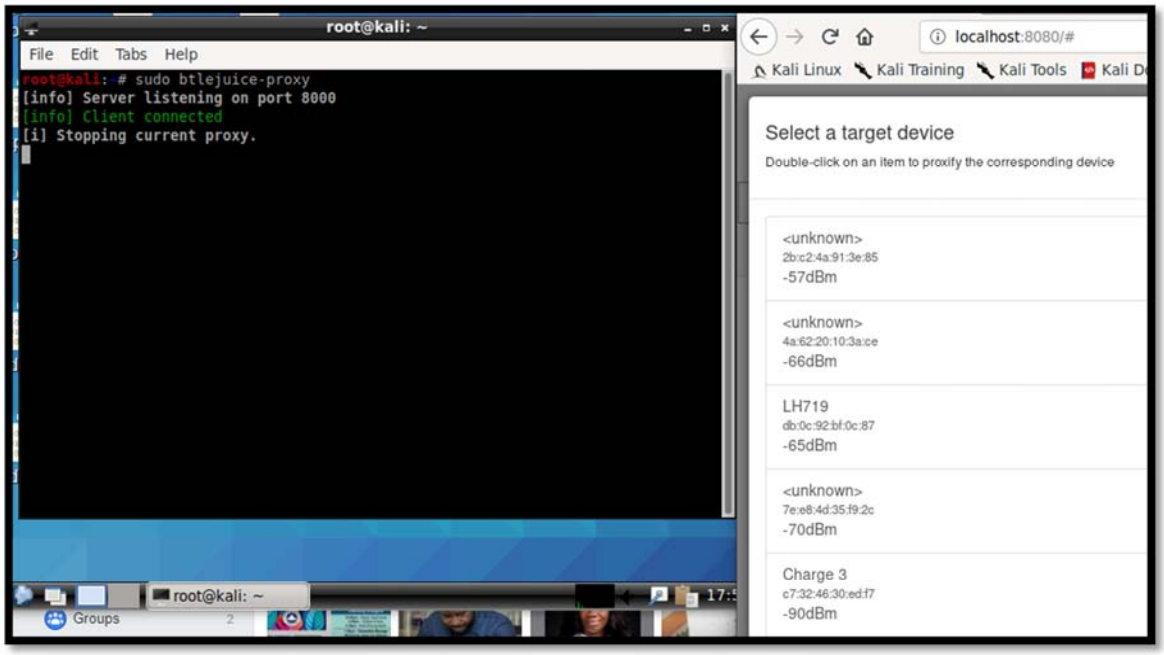

Figure 7. *Btlejuice tool attempted connection to Device A.*

Device B (Figures 8 – 12).

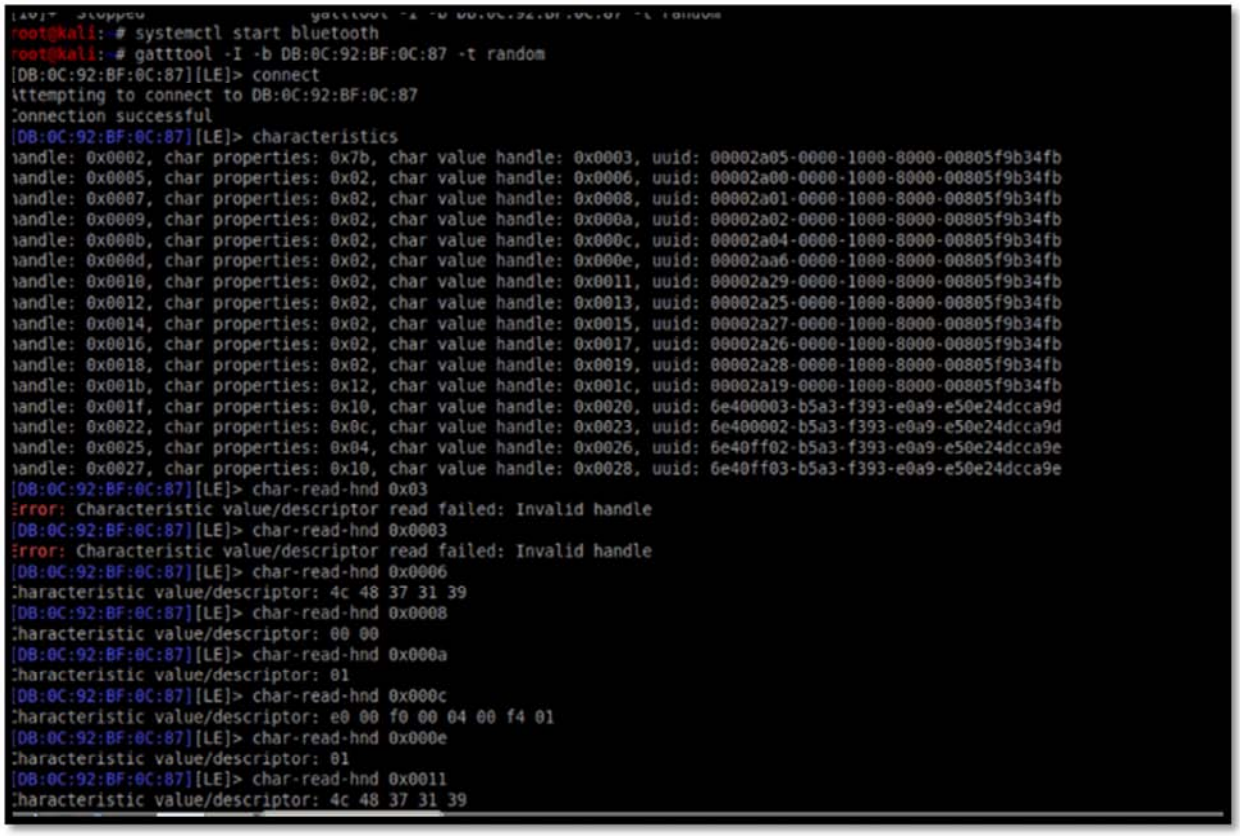

Figure 8. *Gattool scan for device B.*

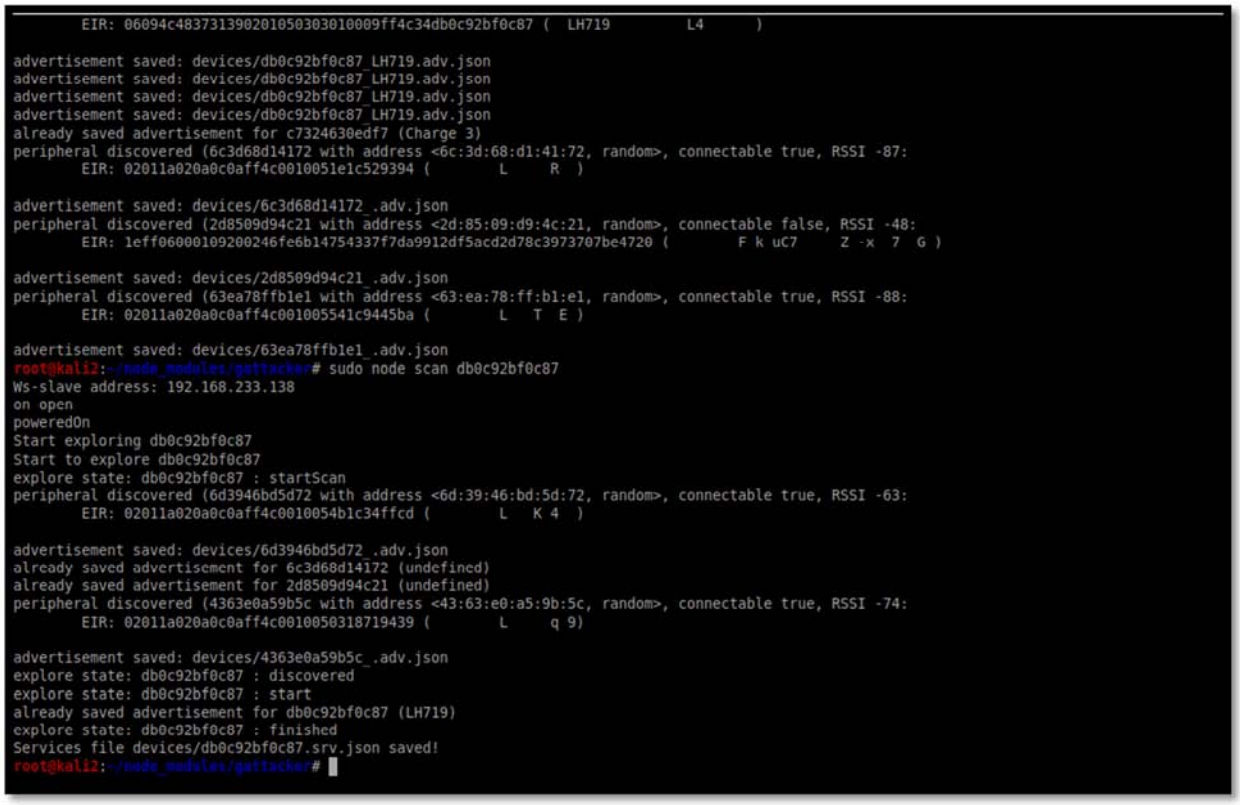

Figure 9. *Gattacker scan for device B.*

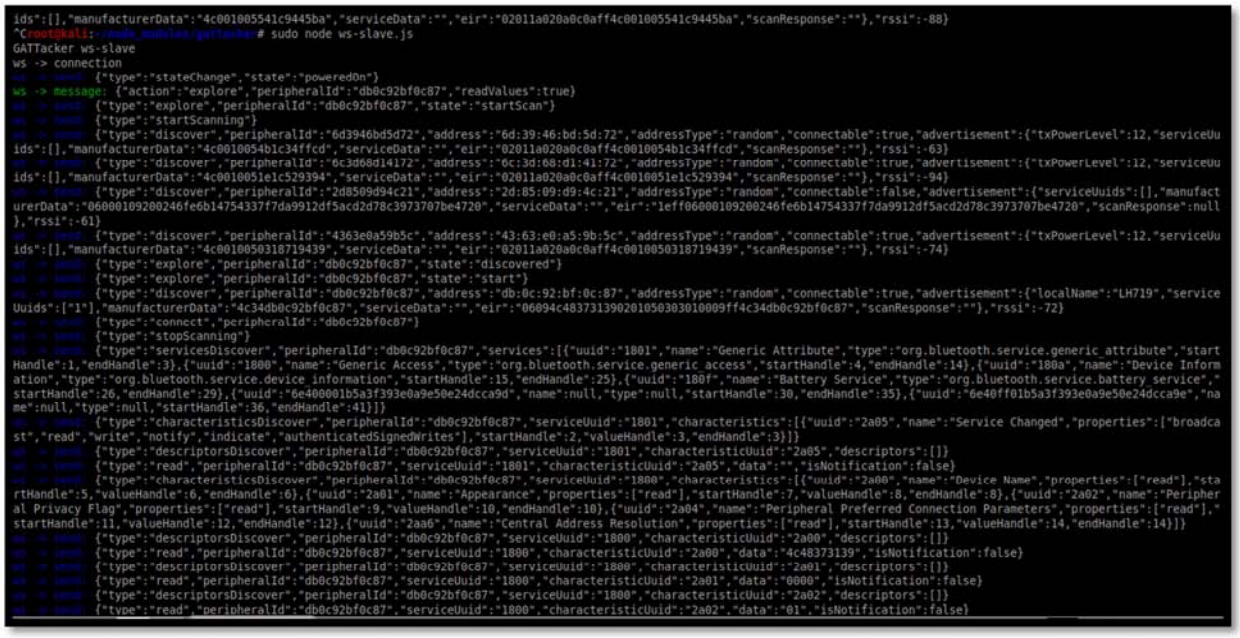

Figure 10. *Gattacker scan for device B (contd).*

Figures 8 shows the gattool scan of device B while Figures 9 and 10 show the gattacker scan of Device B.

Figures 11 and 12 show successful connection to Device B using Btlejuice tool which reveals communication between the devices.

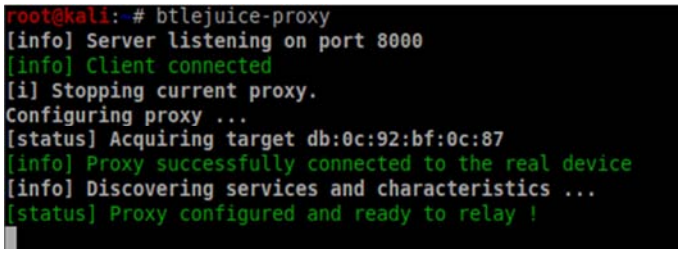

Figure 11. *Btlejuice connection to Device B.*

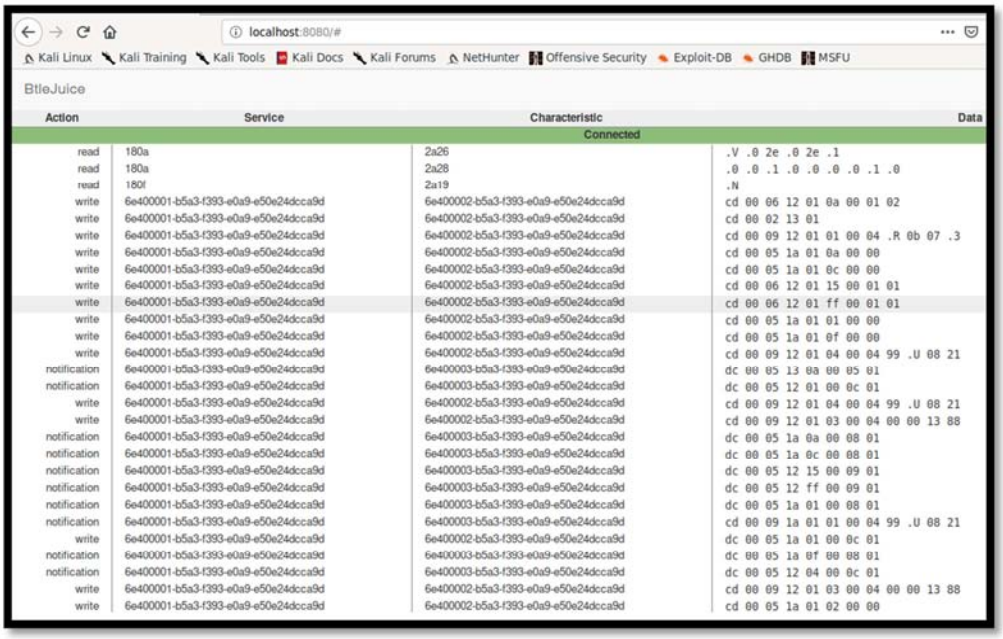

Figure 12. *Btlejuice web interface for device B – contd.*

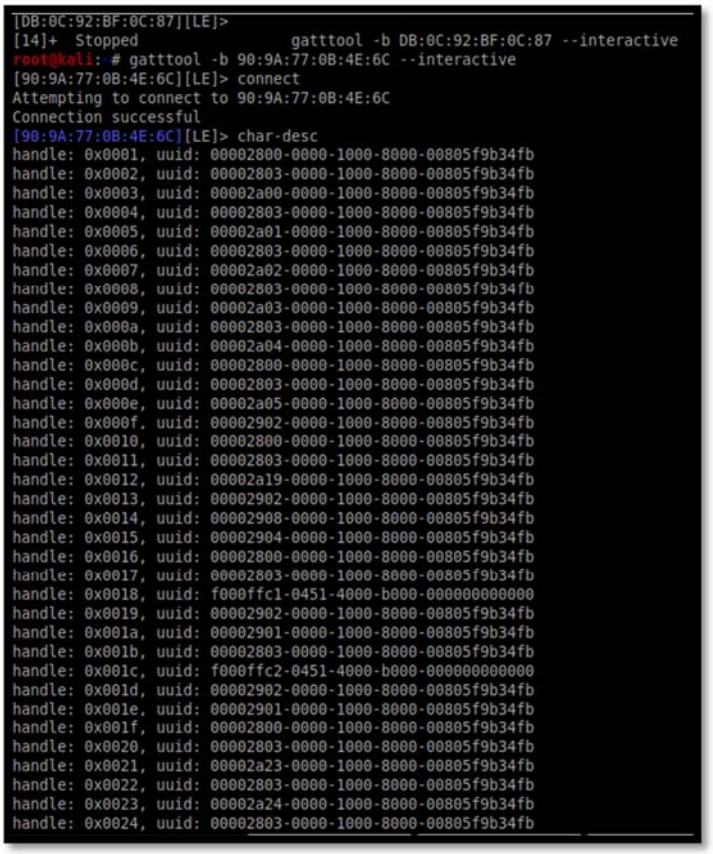

Figure 13. *Gattool scan for device C.*

Device C (Figures 13 – 16).

Figure 13 shows Gattool scan of device C while Figure 14 shows the gattacker scan of Device C.

Figures 15 and 16 show successful access of the data in the IoMT device C which includes the health data of the user and the name of the user in plain text as highlighted.

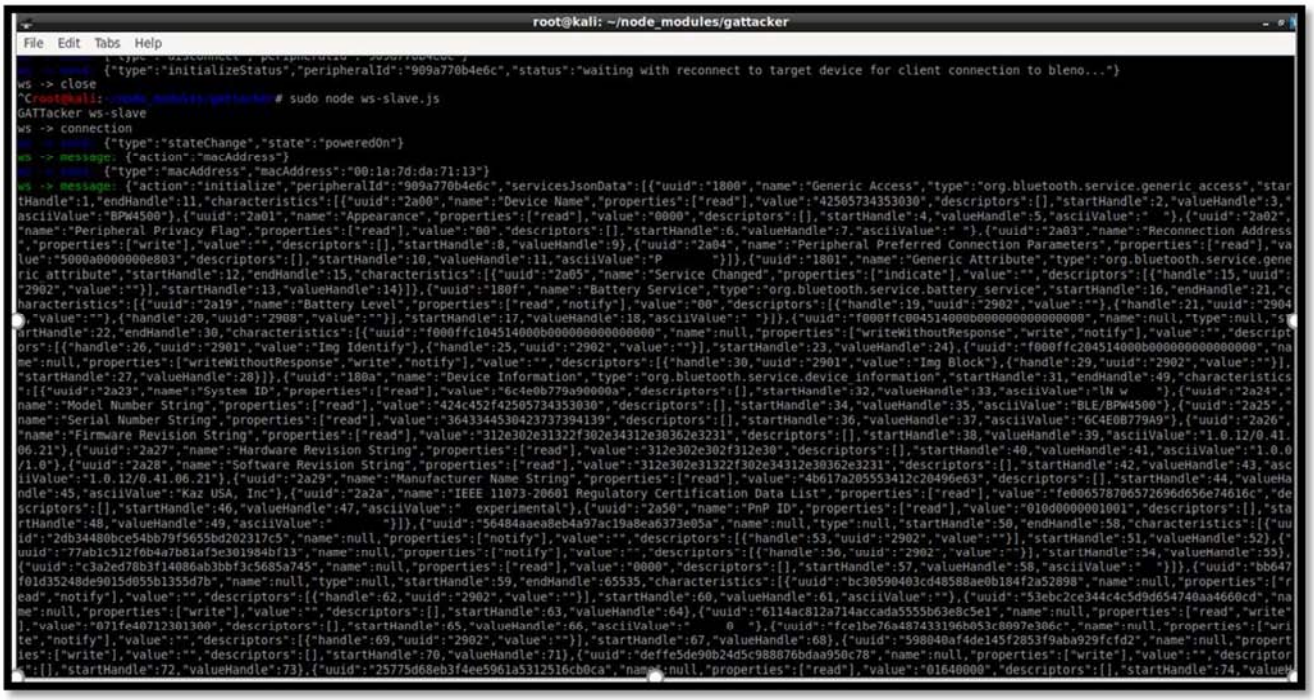

Figure 14. *Gattacker scan on Device C.*

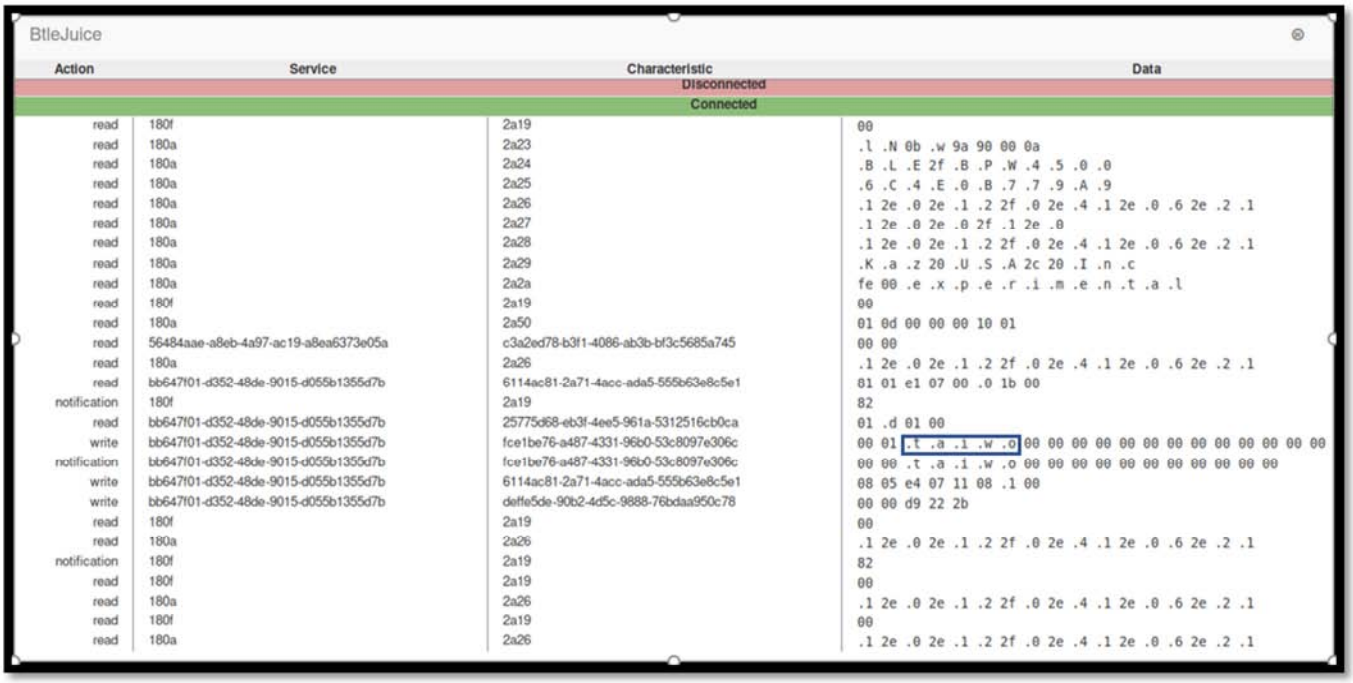

Figure 15. *Btlejuice web-interface for device C.*

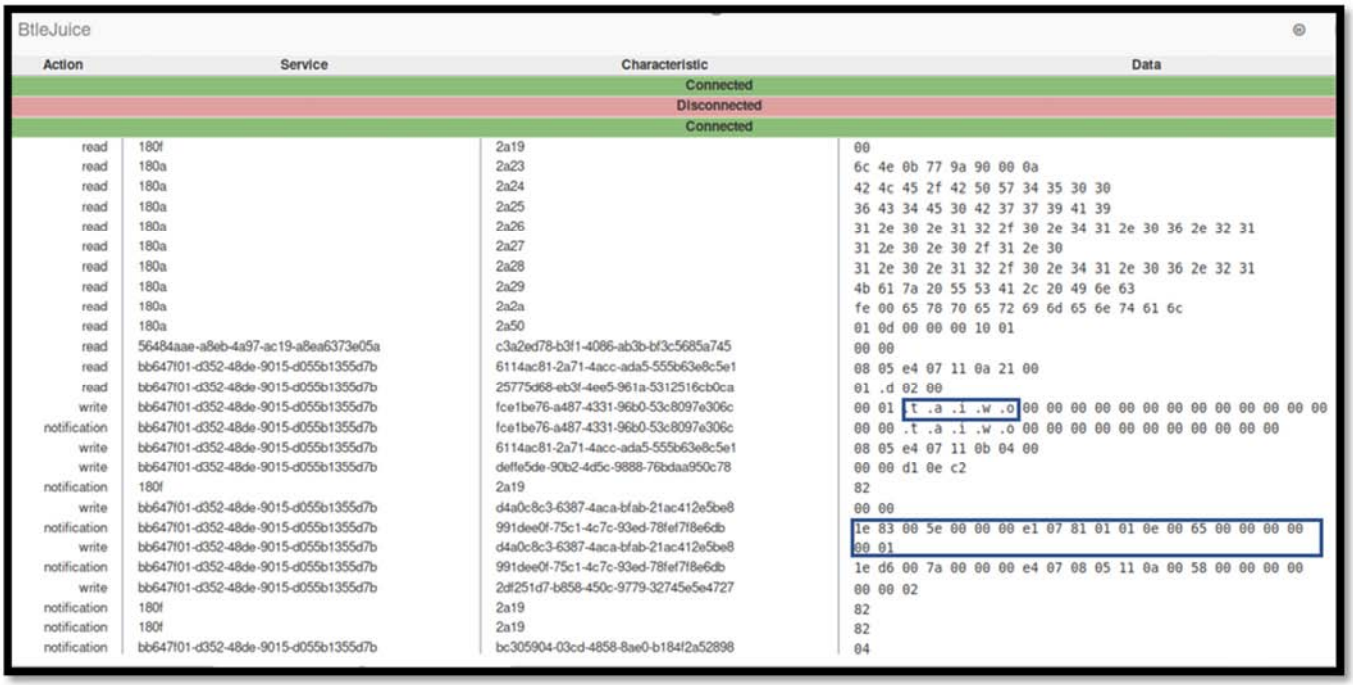

Figure 16. *Figure showing successful connection to Device C.*

4. Development of Security Assessment Framework for Bluetooth IoMT Devices

There are security features in Bluetooth technology that can be implemented to increase the security of the devices. The NIST security recommendations and Bluetooth features are used in Table 3 and Figures 3 – 16 to model the probability of a successful MitM attack and design of the security assessment.

Table 3. *Bluetooth Security Requirements versus the Experiment Results for the IoMT devices. The tables below shouldn't be side by side – it doesn't read well when every other word is split up.*

Security Objectives	Device A	Device B	Device C
Privacy feature Implementation	Device A MAC address is public. This implies that privacy feature is not implemented. The full name of the device, the firmware, and relevant information on the device was also seen in the experiments.	Device B shows the MAC address as Private in the Adv_IND Packet captured in Wireshark. The device however did not randomise Bluetooth the MAC Address as required in a device with privacy feature enabled. Therefore, this shows that although the privacy feature was enabled in the experiment, the required functionality of randomising the MAC address was not seen working all through the experiment.	The privacy feature is disabled in Device C. MAC Address of device C is Public. The name of the device user was seen in clear text when the MitM attack was launched on the connection between the wearable IoMT device and the mobile device. Furthermore, Device C is a blood pressure device and the user's health data (blood pressure and heart rate) was captured as le 83 00 5e 00 00 00 e1 07 81 01 01 00 65 00 00 00 00 which is interpreted from Hex to decimal as 14 131 0 94 0 0 0 225 7 129 1 1 0 101 0 0 0 0 where the blood pressure is 131/94 and the heart rate is 101. This shows that the confidentiality and privacy of the user and the data have been compromised with the success of the MitM attack.
Device Data Integrity	Based on the experiment carried out, unauthorised access/ MitM Attack with replay was not successful on Device A. The device in comparison to the other 2 is more resistant against data manipulation. The experiment showed that device authentication is required to read data from this device.	Unauthorised access to communication between the Bluetooth devices were seen in experiments	Unauthorised access to communication between the Bluetooth devices were seen in experiments
Device Authentication	Based on the experiment carried out authentication is required to read the user's data from Device A. Also, the IO Capability set for this connection is keyboard and display which allows the Passkey Pairing method. The experiment shows that a 4-digit passkey was required for pairing in this connection. The Bluetooth 4.2 Core Specification however recommends a 6-digit passkey for pairing.	Also, the author observed that the pairing of the Wearable IoT device with the mobile device did not use the Passkey Pairing, passkey was not required for pairing. Although the wearable device has a display and the mobile device has keyboard capability, the author observed that the most insecure pairing method (Just Works) was used for pairing this device to the mobile device. Furthermore, the device IO Capabilities was set to NiNo (No Input, No Output) as seen in the experiment.	The experiment shows that Device C does not ensure authentication in read or write operations to and from the device. Although, experiment shows that read not permitted flag which should have enhanced the security of the device by initiating authentication whenever a read operation occurs. The experiment conducted on this device, however, shows the successful implementation of a MitM attack. Just as was observed with Device B, Device C did not use the Passkey Pairing, passkey was not required for pairing. Although the wearable device has a display and the mobile device has keyboard capability, the authors observed that the most insecure pairing method (Just Works) was used for pairing this device to the mobile device.
Resilience/Protection against the MitM Attack	The experiment shows that the MitM flag was set to true for Device A in this connection. This implies that the security feature for MitM protection was integrated into the device A design. The Btlejuice MitM attack was not successful on Device A and the device data was not accessed.	The MitM attack was successful on this device with the attacker having access to the communication between the central and slave devices. Also, Experiment shows that the MitM flag was set to false for this device.	The MitM attack was successful on Device C with the attacker having access to the users' data on the wearable IoMT device.

CVSS (Common Vulnerability Scoring System) can be used to assess the vulnerabilities of a system [15].

According to Padgette, Bluetooth standard specifies 5 basic security features namely, Authentication, Confidentiality, Authorization, Message Integrity and Pairing or Bonding [16].

4.1. Bayesian Networks and Application in Security Assessment Framework

Bayesian Network is part of probabilistic graphical model which uses directed acyclic graph to depict cause and effect relationships. BN is a causal probabilistic model that is used for cyber security risk assessment because it captures complex interdependencies in the risk factors and data capture based on expert judgement [17].

Bayes' theorem is written as:

$$p(A|B) = p(B|A) * p(A)/p(B)$$

p(A|B) is the posterior, i.e., the probability of event A occurring given that event B has occurred.

P(A) is the prior, i.e., the probability of event A occurring.

Bayesian Networks is used to develop a security assessment framework for Bluetooth IoMT devices based on the cause effect relationship model. This shows that the implementation of security features has corresponding effect on the security levels of the device.

Table 4. *List of Vulnerabilities and NIST CVE Value.*

S/No	Security Recommendations / Features	Vulnerability for Non-Implementation of Security Features.	NIST CVE Value	Device A	Device B	Device C
V1	Confidentiality – Privacy Feature	6.5 (Medium)	Not Implemented	6.5 (Medium)	Not Implemented	6.5 (Medium)
V2	Integrity and Availability	Non-implementation of MitM flag – V2 CVE-2019-2225	8.8 (High)	Implemented (0)	Not Implemented (8.8)	Not Implemented (8.8)
V3	Device Authentication through secured pairing	Use of fewer than 128 bits for BLE pairing – V3 CVE-2020-11957	7.5 (High)	Implemented (0)	Not Implemented (7.5)	Not Implemented (7.5)
V4	Resilience against MitM attack	Use of Just Works – V4 CVE-2019-2225	8.8 (High)	Implemented (0)	Not Implemented (8.8)	Not Implemented (8.8)
V5	Authentication	Non-implementation of authentication – V5 CVE-2020-10134	6.3 (Medium)	Pending	Pending	Pending

*Pending applies to future implementation of one of the recommendations (Section 6.2 below).

The overall security of a Bluetooth IoMT device is the summation of all the security features that the device has. A device that has more of the Bluetooth security features implemented is expected to be more secure than another device with less security feature implementation. Hence, the developed framework can be used to assess the security of the devices.

This implies that the more the Vulnerabilities found in a device design the less secure the device is.

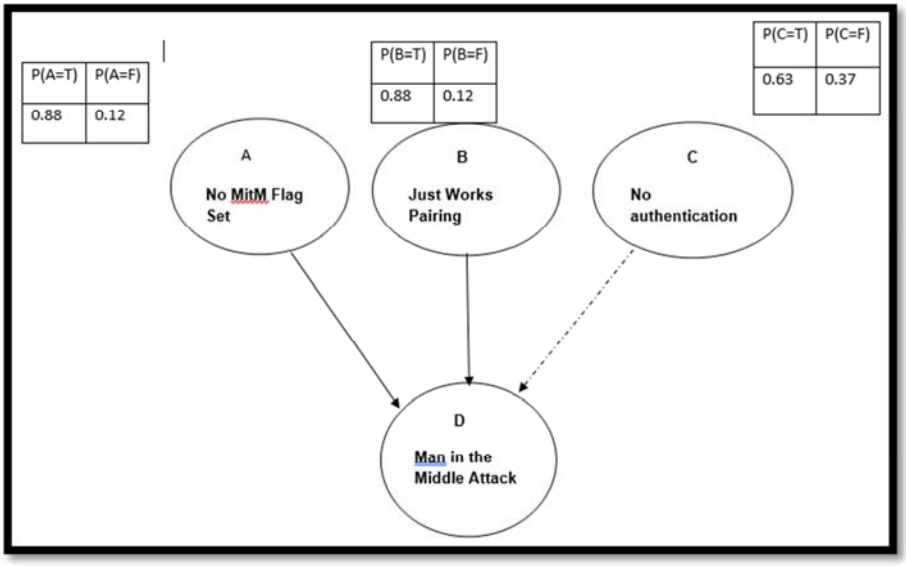

Figure 17. *Model of the Man-in-the-middle attack using Bayesian Network.*

V2, V3, and V4 are the most critical vulnerabilities as they may be exploited to launch a MitM attack which can also lead to other attacks. The Man-in-the-Middle attack was used for the security assessment design for IoMT because of the possible impact such attacks can have on medical devices and its impact on the device users. These may range from user confidentiality and privacy compromise to health data manipulation which can be fatal.

4.2. Model for MitM Attack Success

Figure 17 shows the Bayesian Network Graph of the Causal-Consequence relationship for the implementation or non-implementation of the security features A, B, and C. The CVSS scores for the identified MitM attack vulnerabilities were used for this model. Although the device manufacturer and application developer may implement some additional security features in the device design, the non-implementation of these standard Bluetooth Features was considered, and the uncertainty of other security measures was integrated into the design by applying the NIST CVSS vulnerability scores.

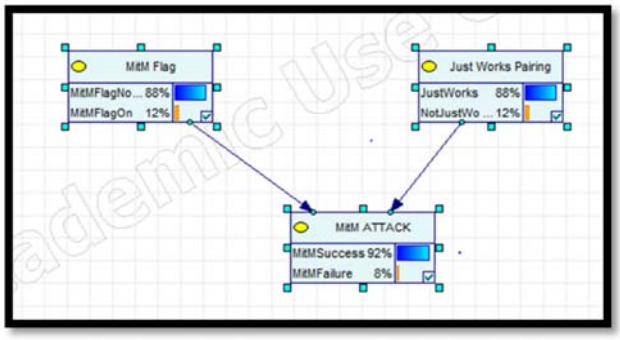

Figure 18. *Probability of MitM attack success using the device before proposed security implementation.*

Figure 18 shows the model when the Just Works Pairing and the Man-in-the-Middle flag are not implemented in the design of the

Bluetooth device. The model shows that the MitM attack success rate is 92%.

Figure 19 shows the impact of implementing Authentication on Man-in-the-Middle attack success. The Model shows a 6% decline (86%) in the Man-in-the-Middle attack success rate as against 92% earlier. Thereby, increasing the security level of the device.

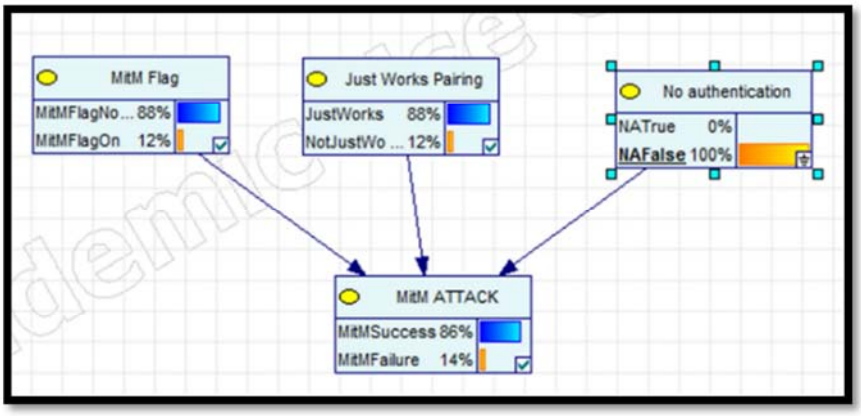

Figure 19. *Bayesian Network Model showing non- implementation of 3 security features.*

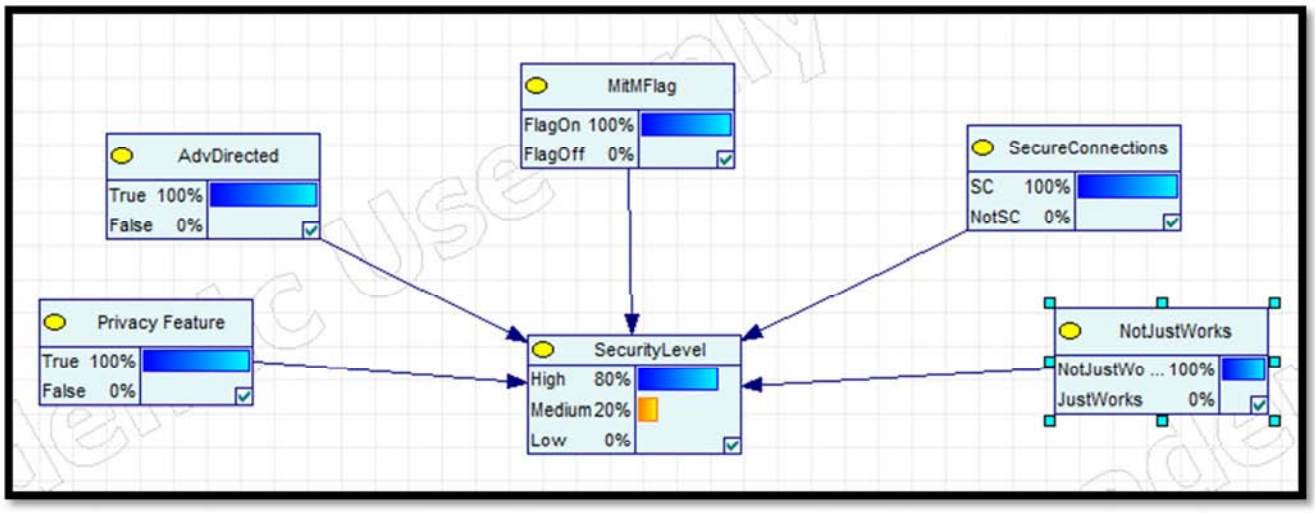

Figure 20. *Security Level Bayesian Model for Implementation of Bluetooth security features.*

4.3. Security Assessment Framework Design for Bluetooth IoMT Devices

Figure 20 is the Security Assessment Framework Model for Bluetooth IoMT devices using Bluetooth Security Features. This model can be used to assess the security levels of the devices based on the implementation or non-implementation of current Bluetooth security features. The model shows that the implementation of all required security measures shows the probability of a High-Security Level of 80% and a Medium Security Level of 20%. Although none of the 3 IoMT devices investigated in this research has all the security features, current research work shows that integration of these features and application-level encryption and authentication will increase the security levels of Bluetooth IoMT devices. Furthermore, the framework can be used to assess and rank the security levels of Bluetooth IoMT devices while implementing other security measures to

increase device security.

4.4. Evaluation of the Proposed Security Assessment Framework

The evaluation of the security assessment framework developed was completed using Devices A, B, and C which was investigated in section 3.1. The security levels of the devices are determined, and device ranking was also completed using the framework. Furthermore, a Pareto chart shows the comparison of the 3 devices using this framework.

Device A Security Level

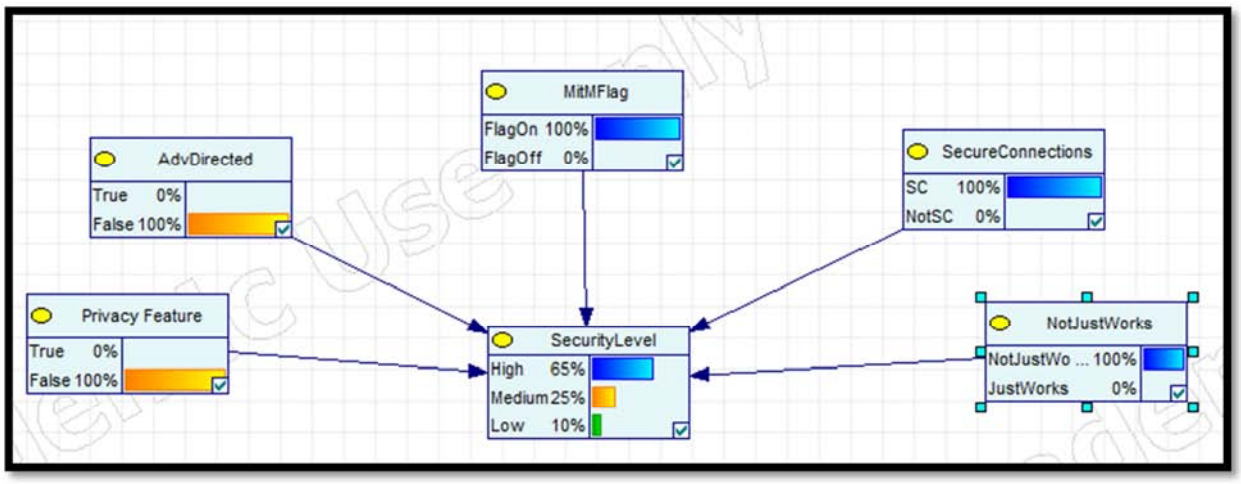

Figure 21. *Device A showing security level possible in Device A with the implemented security features.*

Figure 21 shows that device A's privacy feature was not set and ADV_DIRECT_IND was not set. On the other hand, the security features MitM flag was set, Secure Connections was set, and the association model of Passkey implemented for this device. Given that the critical security features of MitM flag, Secure Connections, and use of the Passkey Association Model were implemented for device A, the outcome of the security assessment for device A was high with security probability level of 65% (High). Although to achieve a higher security level, all the security features are recommended with additional implementations at the application level and device design discussed in section 4.

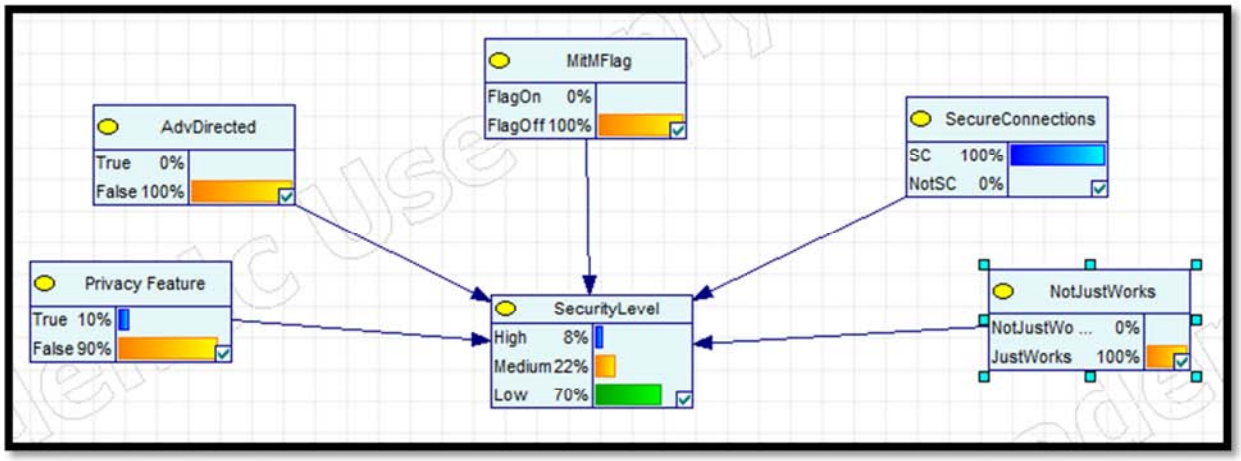

Figure 22. *Figure showing the security Level in Device B with the security implementation.*

Device B Security Level

The privacy feature for device B was not implemented fully, although the sniffed packet showed the BD_ADDR as random, randomisation was not implemented. Also, ADV_DIRECT_IND was not set on, MitM flag was not set, secure connections' feature was implemented whereas the Just Works association model was used for pairing. Although pairing for this device required application-level authentication, the experiment shows that the non-implementation of either passkey, OOB, or Numeric Key resulted in the success of the MitM attack launched against this device. The security level assessment for this device using the framework is low with a low security level probability of 70%. In the same vein, the security level for device B can be increased with the implementation of all identified security features, and other application-level security mechanisms.

Device C Security Level

Figure 23 shows that the privacy feature for device C is not set, ADV_DIRECT_IND is not set, MitM flag was not

set, secure connections was implemented, and the Just Works association model was used for pairing. The security level of device C is low given that the security probability score from the security assessment framework is 72% low. Conversely, to achieve a higher security level, further security features and mechanisms can be implemented.

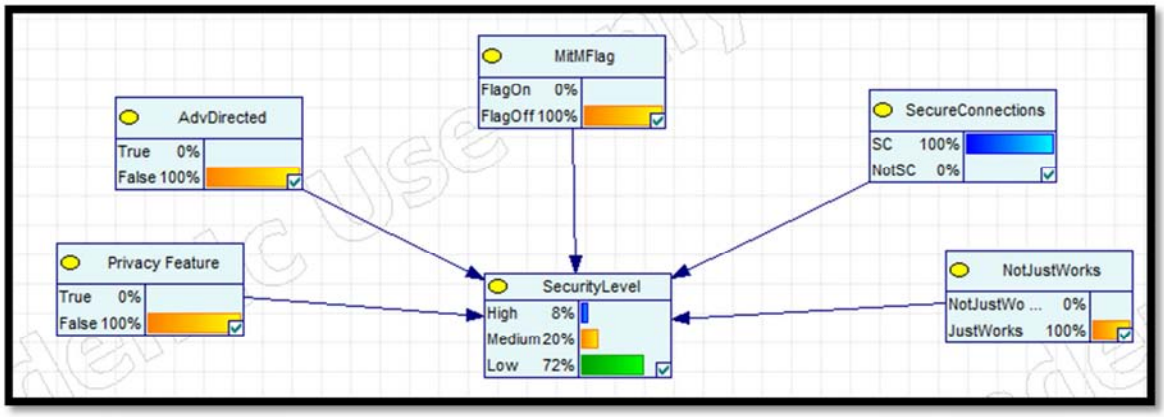

Figure 23. *Showing the security Level of device C with the security level.*

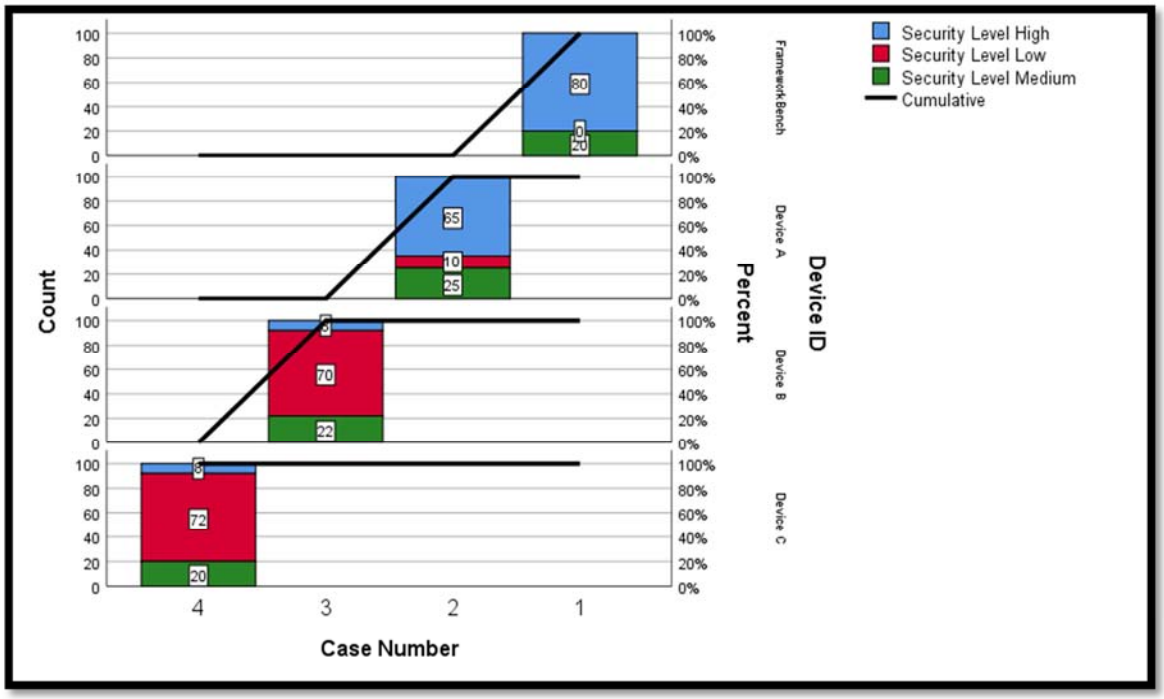

Figure 24. *Pareto Chart showing Device A and C ranks.*

MitM Rag	MitMRagNotOn				MitMRagOn			
Just Works Pairing	JustWorks		NotJustWorks		JustWorks		NotJustWorks	
No authentication	NATrue	NAFalse	NATrue	NAFalse	NATrue	NAFalse	NATrue	NAFalse
MitMSuccess	1	1	0.7	0.5	0.6	0.3	0.3	0.1
MitMFailure	0	0	0.3	0.5	0.4	0.7	0.7	0.9

Figure 25. *CPT Table for the Active Eavesdropping Attack/MITM attack simulation model.*

Privacy Feature		False															
AdvDirected		True								False							
MitMFlag		FlagOn				FlagOff				FlagOn				FlagOff			
SecureConnect...	SC	SC		NotSC		SC		NotSC		SC		NotSC		SC		NotSC	
NotJustWorks	JustWorks	NotJustWorks	JustWorks	NotJustWorks	JustWorks	NotJustWorks	JustWorks	NotJustWorks	JustWorks	NotJustWorks	JustWorks	NotJustWorks	JustWorks	NotJustWorks	JustWorks	NotJustWorks	JustWorks
High	0.05	0.7	0.2	0.2	0.1	0.2	0.1	0.15	0.05	0.65	0.2	0.2	0.15	0.15	0.08	0.15	0
Medium	0.15	0.25	0.3	0.3	0.25	0.35	0.25	0.2	0.25	0.25	0.3	0.3	0.25	0.3	0.2	0.25	0.25
Low	0.8	0.05	0.5	0.5	0.65	0.45	0.65	0.65	0.7	0.1	0.5	0.5	0.6	0.55	0.72	0.6	0.75

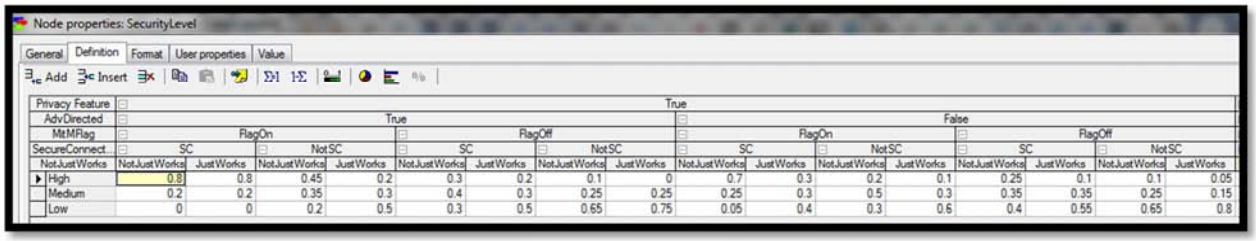

Figure 26. *CPT Table for the Security Level Assessment simulation model.*

Figure 24 shows the possible security levels for all the 3 IoMT devices that were investigated in this research. To analyse the Pareto chart, a framework benchmark device model was included as a fourth device to aid comparison. This framework device model has all the security features implemented to simulate outcomes if the device implements all security features. Furthermore, the Pareto chart shows that the most secure of all the 3 devices is Device A, while Devices B and C has about the same security level with device B slightly higher than Device C security level. In the same vein, the experiment analysis of Table 1 also attests to this deduction.

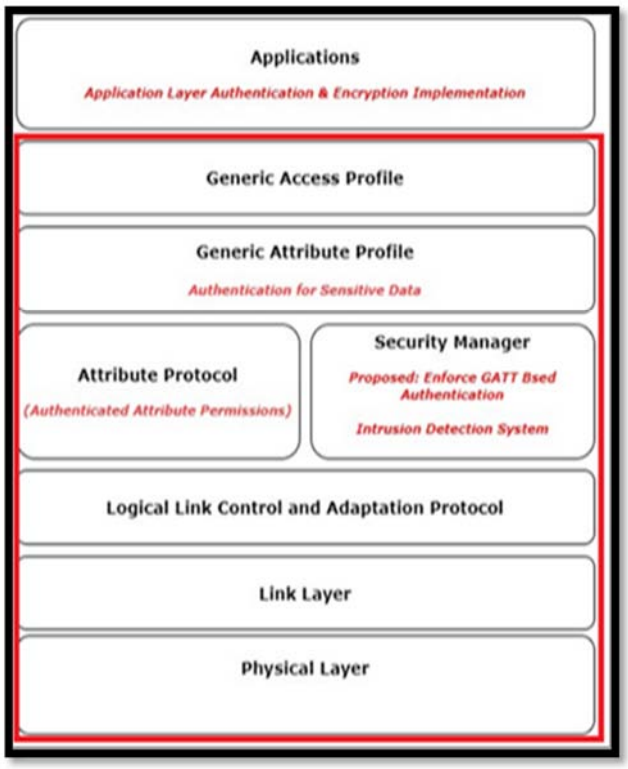

Figure 27. *Showing the BLE protocol stack with the proposed security implementations.*

Figures 25, 26 and 27 show the CPT tables for the Bayesian Network Model simulation of the developed Security Assessment Framework.

4.5. Security Features in Bluetooth Technology and Its Implementation in Wearable Bluetooth IoMT

There are Bluetooth security features recommended to mitigate Confidentiality threat, which is the Privacy feature (Private BD_ADDR). It randomises the MAC address and used to mitigate identity tracking. Also, the Bluetooth LE Secure Connections is more secure than the earlier Bluetooth LE legacy. Bluetooth Secure Connection uses authenticated connection and pairing with encryption. It also uses the Elliptic Curve Diffie Hellman Cryptography for the key generation. The Passkey pairing association model protects against the MitM attack by displaying a 6-digit passkey on one of the devices which should be input on the second Bluetooth device. The OOB process also protects against MitM by using other transmission means such as NFC, for authentication.

The Numeric Comparison provides some protection against MitM attacks by displaying 6 digits on the 2 devices and requiring the user to confirm if both numbers are the same. This is done by clicking a yes or no on the device screen. Just Works is the least secure of all the pairing models. It does not require the user to authenticate.

Other proposed security implementations to mitigate MitM attack are shown in the highlighted part of Figure 27. GATT-Based ATT attribute authentication is recommended on IoMT devices. Furthermore, Bluetooth anomaly-based detection intrusion detection system is another proposed security implementation for Bluetooth IoMT devices.

Furthermore, Section 3.1 above detailed other proposed security measures that may increase the security of Bluetooth IoMT devices.

It may be argued that integrating additional security implementations on these devices may require additional processing and computational power, however achieving high-security levels is critical to the continual adoption of the internet of things in healthcare. Moreover, recent technological advancements have seen the advent of miniature devices with high computing power. Therefore, a high-security level implementation by design can be adopted for IoMT devices.

5. Result and Discussion

The experiment outcome, and the security assessment framework evaluation show that Device A was the most secure of all the devices. Other relevant observations show that the Bluetooth privacy feature for Device A was not implemented and the passkey used for pairing was 4 digits long instead of the recommended 6 digits. Furthermore, Passive Eavesdropping attack was possible on this device as the MAC address, device information, services, and

characteristics, and some data were captured, however, the personal identifiable user's data was not revealed like it was observed with device C. Hence, this shows that the implementation of privacy feature, use of six-digit passkey and additional security can be used to increase the security level of the device A.

Conversely, device C is a Bluetooth wearable blood pressure Monitor on which experiments and security assessment tests were done. The researcher's name was captured in clear text while the blood pressure and heart rate was displayed in Hexadecimal. The Hex value was converted to decimal to reveal the user's health data. Also, it was observed that most of the Bluetooth security recommended features such as privacy feature, MitM flag on, pairing with authentication were not implemented on this device. Although, device B has the same security limitations as Device C but device B's privacy feature was set as "on" in the experiment. Although, it was discovered that the privacy feature was not fully implemented. Hence, devices B and C have the same security level asides that the user's name was not seen in clear text in Device B.

Melamed discussed Bluetooth technologies and simulated MitM attack. Although, some Bluetooth vulnerabilities were considered, countermeasures and assessment framework for Bluetooth was not discussed [9]. Our paper however, simulated MitM attack and further developed security assessment framework for Bluetooth IoMT devices. Similarly, Yaseen also simulated a MiTM attack and developed an approach for detecting and analysing MiTM attacks (MARC) [8] but is different from our work which also focuses on the development of a security assessment framework to measure the security levels of Bluetooth devices.

6. Conclusion, Recommendation and Future Work

6.1. Conclusion

This study shows the effects of implementing Bluetooth security features on the security levels of Bluetooth IoMT devices. Bayesian Network model was used to implement the security assessment framework to assess the security levels of the IoMT devices in the study. It was observed that the devices that had more security features implemented on them had higher security levels compared to devices that had less security features implemented.

6.2. Recommendation

The following are recommended based on the outcome of this study:

The attribute permissions for devices that transmit sensitive data such as IoMT should be set to encryption required, authorisation required, and authentication required. Although this may have a significant impact on the user experience as there is usually a trade-off between security and user experience. Hence, it behoves on the device manufacturers and developers to ensure adequate security is integrated into wearable Bluetooth IoMT. Consequently, this will ensure that the read and notification requests for sensitive data such as healthcare data are authenticated.

Implementation of Application-Level Authentication and Encryption. This is meant to mitigate MitM attacks and prevent unauthorised access to sensitive data.

Use of Received Signal Strength Indicator (RSSI) to differentiate between a cloned device and legitimate BLE nodes as it is expected that the attacker's distance to the legitimate device user and devices will be more.

Use of Bluetooth Anomaly-Based Intrusion Detection System to detect abnormal operations in IoMT Bluetooth connections and to advise users to respond accordingly.

Biometric authentication may be integrated to the IoMT device chip to enhance the authentication and authorisation process.

Stakeholders in healthcare such as doctors, patients, and healthcare institutions should be aware of the security recommendations of the medical devices to mitigate attacks that can be fatal depending on the motivation of the attacker.

6.3. Future Work

This research work focuses on the security of Bluetooth IoMT devices. Future work will be to analyse the security of the IoMT applications installed on smart devices and cloud applications. In the same vein, future work will be on the extension and implementation of the security assessment framework to other network technologies relevant to IoMT such as wireless, Zigbee, and ANT+. Furthermore, the proposed countermeasures discussed in this research can be implemented on simulated open-source platforms and their performance assessed. Other areas of future work can explore the simulation of other attacks.

Acknowledgements

Genie License

The models described in this paper were created using the GeNIe Modeler, available free of charge for academic research and teaching use from BayesFusion, LLC, https://www.bayesfusion.com/

References

[1] Casselman, J., Onopa, N. and Khansa, L., 2017. Wearable healthcare: Lessons from the past and a peek into the future. Telematics and Informatics, 34 (7), pp. 1011-1023.

[2] Alsubaei, F., Abuhussein, A. and Shiva, S., 2019a. Ontology-Based Security Recommendation for the Internet of Medical Things. IEEE Access, 7, pp. 48948-48960.

[3] Muck, J. E., Ünal, B., Butt, H. and Yetisen, A. K., 2019. Market and patent analyses of wearables in medicine. Trends in biotechnology, 37 (6), pp. 563-566.

[4] Shokeen, R., Shanmugam, B., Kannoorpatti, K., Azam, S., Jonkman, M., and Alazab, M. (2019). Vulnerabilities Analysis and Security Assessment Framework for the Internet of Things. 2019 Cybersecurity and Cyberforensics Conference (CCC), 22-29.

[5] Alasmari, S. and Anwar, M., 2016, December. Security & privacy challenges in IoT-based health cloud. In 2016 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 198-201). IEEE.

[6] Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J. and Hayajneh, T., 2018. Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks, 7 (3), p. 28.

[7] Hale, M. L., Lotfy, K., Gamble, R. F., Walter, C. and Lin, J., 2019. Developing a platform to evaluate and assess the security of wearable devices. Digital Communications and Networks, 5 (3), pp. 147-159.

[8] Yaseen, M., Iqbal, W., Rashid, I., Abbas, H., Mohsin, M., Saleem, K. and Bangash, Y. A., 2019. MARC: A Novel Framework for Detecting MITM Attacks in eHealthcare BLE Systems. Journal of Medical Systems, 43 (11), p. 324.

[9] Melamed, T., 2018. An active man-in-the-middle attack on bluetooth smart devices. Safety and Security Studies (2018), 15.

[10] Darwish, S., Nouretdinov, I. and Wolthusen, S. D., 2017. Towards composable threat assessment for medical IoT (MIoT). Procedia computer science, 113, pp. 627-632.

[11] Pathinarupothi, R. K., 2019. Clinically Aware Data Summarization at the Edge for Internet of Medical Things. 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 437–438.

[12] Alsubaei, F., Abuhussein, A., Shandilya, V., and Shiva, S., 2019b. IoMT-SAF: Internet of medical things security assessment framework. Internet of Things, 100-123.

[13] Zhang Y., Weng J., Dey R., Fu X. (2019) Bluetooth Low Energy (BLE) Security and Privacy. Encyclopedia of Wireless Networks. Springer, Cham. pp. 1-12.

[14] Zuo, C., Wen, H., Lin, Z. and Zhang, Y., 2019, November. Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps. In Proceedings of the 2019

[15] Qu, Y. and Chan, P., 2016, April. Assessing vulnerabilities in Bluetooth low energy (BLE) wireless network based IoT systems. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 42-48). IEEE.

[16] Padgette, J., Scarfone, K. and Chen, L., 2017. NIST Special Publication 800-121 Revision 2, Guide to Bluetooth Security. National Institute of Standards and Technology (NIST).

[17] Kammouh, O., Gardoni, P. and Cimellaro, G. P., 2020. Probabilistic framework to evaluate the resilience of engineering systems using Bayesian and dynamic Bayesian networks. Reliability Engineering & System Safety, 198, p. 106813.