Article

Not peer-reviewed version

CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security

Sajjad Dadkhah * , Euclides Carlos Pinto Neto , Raphael Ferreira , Reginald Chukwuka Molokwu , Somayeh Sadeghi , Ali Ghorbani

Posted Date: 16 February 2024

doi: 10.20944/preprints202402.0898.v1

Keywords: Internet of Medical Things (IoMT); Internet of Things (IoT); Intrusion Detection System (IDS); Security; Dataset; IoT Healthcare

Article

CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security

Sajjad Dadkhah, Euclides Carlos Pinto Neto, Raphael Ferreira, Reginald Chukwuka Molokwu, Somayeh Sadeghi and Ali A. Ghorbani

Canadian Institute for Cybersecurity - University of New Brunswick (UNB), Fredericton, New Brunswick, Canada; e.neto@unb.ca; raphael.ferreira@unb.ca; r.c.molokwu@unb.ca; s.sadeghi@unb.ca; ghorbani@unb.ca

* Correspondence: sdadkhah@unb.ca

Abstract: The Internet of Things (IoT) has a growing presence in society's daily lives. These lightweight devices can be easily deployed and maintained, enabling extensive adoption in different environments. Furthermore, one of the most promising areas for using IoT devices is healthcare, comprising devices referred to as the Internet of Medical Things (IoMT). Several examples of healthcare services are supported by IoMT devices, e.g., continuous health monitoring. Conversely, there is an increasing concern with the cybersecurity aspects of these devices, and several attacks against IoT infrastructures have been launched in the past few years. These cybersecurity concerns also apply to healthcare applications, where the tradeoff between the benefits and security of IoMT devices must be observed. Given the complexity and amount of data IoMT network traffic generates, advanced methods become especially useful in these environments. Although Machine Learning (ML) brings various techniques and solutions to improve cyberattack detection, prevention, and mitigation, essential features are not addressed in the current state-of-the-art benchmark dataset contributions. Thereupon, the main goal of this research is to propose a realistic benchmark dataset to enable the development and evaluation of IoMT security solutions. In order to accomplish this, 18 attacks were executed against an IoMT testbed composed of 40 IoMT devices (25 real devices and 15 simulated devices), considering the plurality of protocols used in healthcare (e.g., Wi-Fi, MQTT, and Bluetooth). These attacks are categorized into five classes: DDoS, DoS, Recon, MQTT, and spoofing. This effort aims to establish a baseline complementary to the state-of-the-art contributions. The outcome supports researchers in investigating and developing new solutions to make healthcare systems more secure using different mechanisms (e.g., machine learning - ML). This research goes beyond merely conducting attacks on IoMT devices. We also attempt to capture the lifecycle of these devices in different vital phases, from the moment they join the network until they leave, which is called profiling. Profiling allows the different classifiers to identify anomalies of each device individually in the healthcare network. The CICIoMT2024 dataset has been published on CIC's dataset page, making it available for other researchers to use.

Keywords: Internet of Medical Things (IoMT); Internet of Things (IoT); Intrusion Detection System (IDS); security; dataset; healthcare

1. Introduction

Nowadays, the Internet of Things (IoT) has a growing presence in society's daily lives. These lightweight devices can be easily deployed and maintained [1,2], enabling extensive adoption in different environments. The development of smart cities also relies on the advances of such technology [3]. Solutions that were once considered futuristic can be achieved by integrating ubiquitous systems with advanced analytics [4–6]. Besides, the current adoption of existing advanced technologies represents an ideal platform for new solutions [7,8]. For example, wearable devices (e.g., smart watches) can support health monitoring applications at scale once they have been widely adopted. This

 doi:10.20944/preprints202402.0898.v1

new paradigm provides multiple services that can be beneficial in a variety of areas, e.g., transportation [9], education [10], and energy [11]. IoT devices play very distinguished roles in each application while observing different levels of constraints (e.g., safety-critical systems). One of the most promising areas for the use of IoT devices is healthcare, referred to as the Internet of Medical Things (IoMT) [12–14].

There are several examples of healthcare services supported by IoMT devices. For example, an important area in patient care is health monitoring [15]. Observing different physiological metrics is vital in multiple treatments and continuous measurements can improve the process results [16]. In this case, IoMT devices can play the role of physiological monitors since they can be set up easily and provide critical information to medical personnel [17]. Also, they provide mobility and simplicity in the hospital environment. Another important area is smart medication delivery, in which the process of medicating patients is automated with the amount prescribed by the doctors [18]. In this case, infusion pumps are becoming more and more popular in healthcare institutions and support treatments with an automated and precise approach. Remote medicine is another concept that has been growing in popularity in the past few years [19]. Allowing patients to be treated and monitored remotely can improve the overall practice by providing more comfort and continuous checks. In this application, IoMT devices can play the role of sensors by collecting important data and actuators by providing some local service (e.g., automated medication delivery).

However, although IoT devices are beneficial in many applications, there is an increasing concern with the cybersecurity aspects of these devices [20]. In the past few years, several attacks against IoT infrastructures have been launched [21,22], and the consequences of such threats depend on the environment considered. IoT devices present a limited pool of computational resources compared to traditional systems (e.g., servers). This is a key factor to observe in terms of the device security, the simpler network profiles these components bring to the network (e.g., limited pool of protocols), and the possible open doors for attackers [23,24]. For instance, IoT devices can be exploited in Advanced Persistent Threats (APT) as key vectors. Furthermore, compared to traditional vulnerability assessment and patching, there is a current lack of standards for IoT devices. For example, the National Institute of Standards and Technology (NIST) maintains a repository for the vulnerability management of several devices called the National Vulnerability Database (NVD) [25]. Vulnerabilities discovered that can affect devices in use are shared in this database to enable the general public to be aware and patch their systems. Regarding IoT, devices are very diverse, with multiple brands, firmware, and purposes. Although there are some initiatives to create standard repositories for IoT [26], this diversity makes it difficult for vulnerabilities to be tracked and patched for all devices. The main issue refers to the increase of IoT as an important asset in many environments as well as a main target for attackers. Knowing the benefits of IoT to businesses motivates companies to invest in this technology, but the fragile security defences of such devices may lead attackers to exploit and disrupt IoT operations [27].

These benefits and cybersecurity concerns also apply to healthcare applications. Although adopting IoT devices can be beneficial in several medical procedures, the tradeoff between usefulness and cybersecurity needs to be observed [28]. Relying on insecure devices can bring risks that may compromise the quality of the treatment provided. Besides, some IoT devices are not widely adopted in specific environments. For example, infusion pumps are devices adopted in healthcare and unavailable in other environments (e.g., transportation). The limited use of this device is another factor in hardening the discovery and patching of potential vulnerabilities. For example, IoT devices have been targeted in many ransomware attacks against healthcare organizations in the past few years. In fact, security solutions need to consider this aspect in different areas of healthcare. Furthermore, there may be several consequences resulting from such attacks. In terms of confidentiality, sensitive information from patients may be disclosed [29]. In terms of integrity, vital readings can be manipulated to compromise the accuracy of the treatments provided. Regarding availability, attacks may disrupt critical services and lead the operations to unsafe states. Finally, considering healthcare as a safety-critical application for IoT, the consequences of attacks can be critical, and solutions to improve the protection of such operations are necessary.

 doi:10.20944/preprints202402.0898.v1

Given the complexity and amount of data generated by IoT and IoMT network traffic, advanced methods have become especially useful in these environments. In this context, Machine Learning (ML) brings various techniques and solutions that can improve the detection, prevention, and mitigation of cyber-attacks [30,31]. By analyzing the networking patterns in a multidimensional space, ML can identify anomalies in the network, abnormal IoMT traffic, and characteristics of attacks that can be launched (e.g., Distributed Denial-of-Service - DDoS) [32,33]. ML can enable the automated detection of potential threats and help healthcare professionals deliver high-quality services with a continuous security monitoring approach. Moreover, the characteristics of IoT network traffic can vary greatly depending on the devices and environments. For example, a temperature sensor can be implemented to send temperature readings once a day. At the same time, an aircraft sensor can be implemented to send structural readings regularly [34]. Besides the temporal differences, IoT services can also rely on multiple protocols (e.g., MQTT), which can include specific patterns in the network traffic. Similarly, IoMT devices can operate differently depending on the application. For example, the traffic generated by an infusion pump is usually less frequent than a continuous physiological monitor. These differences can be learned or captured by ML techniques to identify if abnormal traffic is sent through the network.

Although there are some datasets available for the development of security applications in IoMT, there are important features not addressed in the current state-of-the-art contributions [35]. For example, operational diversity is a critical aspect to consider to mimic a realistic IoMT environment. Hence, there is a need for an extensive testbed composed of several IoMT devices comprising both network traffic for Intrusion Detection Systems (IDS) as well as for IoMT profiling. IoMT features and profiles can drive ML and other advanced analytics methods to improve the security of these systems. For this reason, establishing a realistic and extensive topology with IoMT devices of different subcategories is required. Another key feature to support new solutions is the adoption of multiple protocols. To mimic a healthcare IoMT infrastructure, a topology needs to rely on the use of multiple services that would naturally adopt different protocols (e.g., Wi-Fi, Bluetooth, and MQTT). Finally, special attention needs to be given to defining experiments to represent the data transmission in real topologies, both in terms of attacks and in everyday operations.

Thereupon, the main objective of this research is to propose a realistic benchmark dataset to enable the development and evaluation of IoMT security solutions. In this effort, 18 attacks were executed against an IoMT testbed comprising 40 IoMT devices (25 real devices and 15 simulated devices), considering the plurality of protocols used in healthcare (e.g., Wi-Fi, MQTT, and Bluetooth). These attacks are categorized into five classes: DDoS, DoS, Recon, MQTT, and spoofing. This effort aims to establish a baseline complementary to the state-of-the-art contributions and supports researchers in investigating and developing new solutions to make healthcare systems more secure using different mechanisms (e.g., machine learning - ML). The main contributions of this research are:

- **Development of a Comprehensive IoMT Security Dataset:** This paper introduces the CICIoMT2024 dataset, an advanced effort to construct a realistic and multi-protocol benchmark for the security of the Internet of Medical Things. By executing 18 different cyberattacks against a diverse set of 40 IoMT devices, we contribute to the Healthcare field by providing a comprehensive dataset containing most of the protocols in the devices in this field, namely Wi-Fi, MQTT, and Bluetooth protocols.
- **Innovative Methodology in IoMT Attack Simulation and Data Collection:** A unique aspect of this paper is the systematic approach to simulating and capturing IoMT network traffic under various cyberattack scenarios. Considering the complex network of healthcare organizations, it is essential to consider several attributes, such as understanding the effects of different types of attacks, including DDoS, DoS, Recon, MQTT, and spoofing, using a combination of real and simulated devices. Advanced network monitoring techniques and specialized hardware, such as network taps, ensure the high fidelity of data collection.

 doi:10.20944/preprints202402.0898.v1

- **Profiling IoMT Device Lifecycle for Enhanced Security Understanding:** This research goes beyond merely conducting attacks on IoMT devices. We also attempt to capture the lifecycle of these devices in different vital phases of a device from the moment they join the network until they leave. Mobility in healthcare organizations is considered to be a regular aspect. Thus, profiling the lifecycle of these devices, encompassing various operational phases such as power interaction, idle, active, and interaction states, becomes very important. This study offers an in-depth understanding of the devices' behavioral patterns by meticulously capturing and analyzing the behavior of IoMT devices from the moment they join the network. This profiling is critical in identifying and mitigating potential security vulnerabilities.
- **Multi-dimensional Evaluation:** This research extends beyond dataset creation to evaluate the efficacy of multiple machine learning algorithms in detecting and classifying IoMT cyberattacks. By assessing techniques like Logistic Regression, Adaboost, Random Forest, and Deep Neural Networks, the study not only benchmarks the current state of ML in IoMT security but also opens avenues for future exploration in algorithm optimization and feature engineering.

The paper is structured as follows: Firstly, Section 3 reviews related works and identifies the main aspects of this research. Secondly, Section 2 presents the primary aspects of IoMT applications in healthcare. After that, Section 4 introduces the CICIoMT2024 dataset and explains the phases involved in the data collection. Section 5 presents the method used in this research to evaluate multiple aspects of the data collected and Machine Learning (ML) algorithms. Then, Section 6 describes the feature extraction process and provides a description of the data collected. Finally, Sections 7 and 8 present the ML evaluation in identifying different attacks and the conclusion of this research.

2. Internet of Medical Things (IoMT) in Healthcare

Nowadays, several medical solutions rely on IoMT devices to enhance or accelerate treatment. These devices bring many advantages compared to traditional medical equipment while ensuring the accuracy of the multiple procedures considered. Various areas in the healthcare practice can benefit from adopting IoMT infrastructure, and this Section presents a discussion on how such devices can be useful in this context as illustrated in Figure 1.

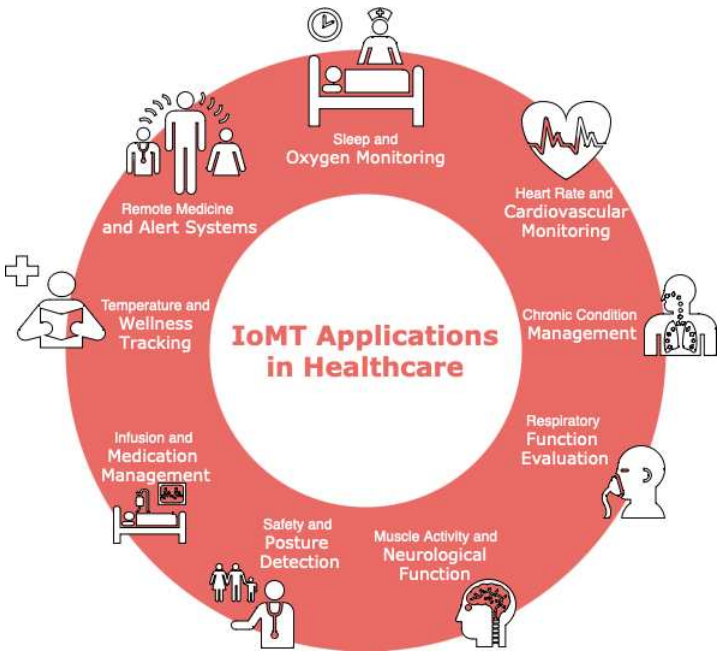


Figure 1. Applications of IoMT in Healthcare.

 doi:10.20944/preprints202402.0898.v1

Remote medicine and alert systems use IoMT to simplify patient care in remote conditions while observing the continuity and readiness of services [36]. This area includes not only teleconsultations but also refers to remote diagnosis and therapy [37,38]. Remote care poses requirements other than the needs of in-person care. To address them and ensure effectiveness, alert systems are vital and vary depending on the patient's condition. In this case, general emergency notification services are responsible for informing medical personnel that medical attention is required [13,39]. Also, critical monitoring informs the medical staff of physiological conditions based on multiple parameters [12,40], while fall detection services inform that patients have fallen and need support [41,42]. Besides, some solutions ensure the medications and treatments are used as medical doctors recommend and are also referred to as medication reminders [43,44]. In all these cases, IoMT offers a simpler approach to remote medicine and alert systems by integrating devices and software platforms [45,46].

Furthermore, another critical area in patient care is the evaluation of sleep patterns and oxygen levels in the blood. This area is called sleep and oxygen assessment and helps medical staff treat sleep and respiratory disorders and improve the overall medical practice by monitoring cardiovascular health [47–49]. These solutions comprise using IoMT devices for sleep analysis, including monitors and actuators [50]. Also, IoMT devices can act as oxygen saturation as part of the continuous monitoring framework alongside integrated systems (e.g., software platforms that can control IoMT devices) [51,51,52]. Another important category of IoMT devices in this context is wearable technology, which offers comfort and simplicity in patient care. Finally, alert systems can also be adopted in this context [53,54].

Monitoring technologies are present in many areas of medical practice, including heart rate and cardiovascular solutions. IoMT devices enable measuring and tracking parameters necessary to cardiovascular health, e.g., pulse rate, blood pressure, and oxygen saturation [55,56,56]. These parameters are critical to ensure patients' well-being, and IoMT helps ensure good condition continuously. For example, heart rate tracking can be achieved using devices such as smartwatches, chest straps, and fitness trackers [57–59]. Similarly, Electrocardiogram (ECG) monitoring devices detect anomalies in the heart beating pace [60,61]. Besides, blood pressure and overall cardiac monitoring and telemetry are areas in which IoMT can enable effective and continuous real-time treatment. Finally, deploying IoMT solutions can also include using software platforms to simplify the data management of information sharing [51].

Patient care also includes wellness. In this case, IoMT can leverage the periodic and continuous measurement and evaluation of wellness indicators [62,63]. Solutions include using smart thermometers capable of sharing essential data with medical applications [64]. Tracking devices are especially important in this area through the use of fitness trackers and wearable devices [65,66]. Besides, chronic conditions can be continuously observed with such technologies, and treatment can be optimized [67]. The same applies to patients recovering from illnesses who can benefit from using IoMT devices. Finally, this area extends beyond illness detection, comprising wellness tracking in preventive efforts.

Chronic condition management comprises managing and treating chronic diseases in different cases, targeting diseases such as diabetes, hypertension, and asthma [68,69]. In this application area, IoMT devices are designed to attend to the particular needs of each patient. For example, continuous monitoring needs to be regarded for specific metrics such as blood pressure (hypertension) and blood glucose levels (diabetes) [56,70]. IoTM is essential in engaging medical staff and patients in chronic condition management because it enables remote care, personalized treatments, and preventive measures.

A particular area of care that IoMT devices can support is the respiratory function evaluation. These solutions monitor and evaluate the health of the respiratory system and are crucial in special conditions (e.g., asthma and sleep apnea) [71,72]. Devices can be used to measure the inhaled and exhaled airflow to ensure an appropriate lung function that can be vital in some treatments and can be

 doi:10.20944/preprints202402.0898.v1

used by smart inhalers [73]. The oxygen saturation level in the blood is another critical indicator for respiratory conditions in remote care practice.

Muscle activity and neurological function represent another medical care area that IoMT devices can improve. It uses advanced solutions to enhance muscular and neurological health conditions [74]. Such solutions act not only in treating diseases but also in the prevention and recovery. For example, Electromyography (EMG) devices can be used alongside neurological monitoring devices to evaluate the health of muscles continuously [75]. Physical rehabilitation is another area of IoMT applications since patients' movement patterns can be closely assessed (e.g., balance) [76]. Finally, solutions for different types of treatment can be developed using IoMT devices to support remote care and patient comfort.

Furthermore, safety and posture detection helps medical personnel improve patients' safety levels considering their postures and movement patterns [77]. These solutions enhance the treatment of different movement-related diseases and can include remote services such as fall detection and real-time posture monitoring [78,79]. Regarding remote care, sensors can be distributed in a smart home environment to ensure the patient's continuous care and comfort [80]. IoMT solutions play a unique role in these applications, with devices deployed to support these functions and the software platforms that manage and share the data collected.

Moreover, medication management is crucial to ensure patients are treated efficiently. Infusion and medication management is an area of medical care that deals with methods to automate medication delivery and improve the patient's treatment [81,82]. IoMT devices can be used in different ways in this context. For example, infusion pumps are widely used in hospitals and can provide several treatment benefits [83]. This extends to environments outside hospitals, where medications can be remotely infused, and data can be shared with the medical staff.

Finally, new applications are being developed using IoMT devices in healthcare [84]. These solutions aim to improve the medical practice by offering comfort, remote care, higher accuracy, and interconnection. Besides, the hardware of such devices is improving, and more robust solutions are expected in the next few years [85,86]. Although IoMT brings many advantages to healthcare, there are challenges to ensuring secure operations. In this sense, resources that enable the development of cybersecurity solutions in this context are vital, e.g., datasets that mimic natural environments with extensive testbed.

3. Healthcare dataset in IoT domain

In [87], the researchers proposed an intrusion detection system for IoT devices in the Healthcare environment. Their proposed method has merged network and biometric metrics to enhance IDS development. Their experimental setup involved a hybrid method, including an Electrocardiogram, PM4100 Six Pe Multi-Sensor Board, a Gateway simulated in the Windows operating system, Blood Oxygen Saturation (SpO2), and a device to measure Blood Oxygen Saturation (SpO2). They conducted attacks such as spoofing and data alteration and investigated scenarios where different vulnerabilities can be exposed.

In [88], the authors present the ECU-IoHT dataset to demonstrate the exploitation of IoT devices in a healthcare environment. An analysis of attack behaviour is conducted to support the development of new security solutions comprising many real devices (MySignals, temp sensor, BP sensor, HR sensor, Bluetooth and wireless adapter,Kali and Windows Laptob). Concerning the attacks launched, the authors focus on scaling, ARP spoon, DoS, Smart, and injection.

The authors in [89] introduce a dataset focused on how attacks are executed against IoMT topologies with a special focus on Bluetooth. An important discussion on the technical aspects of this protocol is presented alongside its applicability to the healthcare context. Multiple devices are used, and several attacks are launched, followed by an in-depth ML analysis considering the evaluation of multiple algorithms (e.g., Support Vector Machine, K-Means, and Deep Neural Networks).

 doi:10.20944/preprints202402.0898.v1

Hussain et al. [90] introduce a data generation method to support the design of IoT security solutions focused on healthcare. This method, named IoTFlock, enables the generation of both normal and malicious network traffic. The dataset proposed adopted many IoMT devices and resulted from the network traffic captured during. Several types of attacks can target the MQTT protocol. These attacks include Distributed Denial of Service (DDoS), brute force, SlowITE, and MQTT publish flood attacks.

The study described in [91] concentrates on a commonly used protocol in industrial healthcare systems, namely IEC 60 870-5-104. The research aims to address the issue of limited resources available for this protocol. Several attacks, such as Man-In-The-Middle and DoS, were executed as part of the research. Furthermore, the study evaluated the effectiveness of machine learning techniques in the analysis process.

Table 1 summarizes the contributions and compares them with the characteristics of this research. In fact, the CICIoMT2024 provides an extensive list of real IoMT devices while executing several attacks. Besides, extensive IoMT profiling is part of the contributions of this research.

Table 1. Recent Healthcare datasets in IoT domain

	Year	Devices	Attacks	Heathcare	IoT	Extensive Profiling
WUSTL EHMS [87]	2020	Windows Laptop, Blood Oxygen Saturation (SpO2), PM4100 Six Pe Board, EKG or ECG	Spoofing and Data alteration	✓	✓	X
ECU-IoHT [88]	2021	Bluetooth Adapter, wireless network adapter, Windows 10 laptop, Heart rate sensor, Blood pressure sensor, Temperature sensor, Kali laptop, Libelium MySignals	Network scan, Script Injection, ARP spoofing Smurf,DoS,	✓	✓	X
BlueTack [89]	2022	SpO2, heart rate, and ECG	DDoS, Bluesmack, MITM, and DoS	✓	✓	X
ICU [90]	2021	response (GSR) Sensor, Galvanic skin, Nasal/Mouth, Barometer, Remote Electrocardiogram, Fire Sensor, (ECG) monitoring, Smoke Sensor Solar Radiation Sensor, Pulsoximeter (SPO2), CO Sensor, Infusion Pump Glucometer, monitor Sensor Blood pressure, AirFlow Sensor, Electromyography (EMG), Body Temperature Sensor Sensor, Air Temperature Sensor Air Humidity Sensor	SlowITE, and brute force, DDoS MQTT, MQTT publish flood	✓	✓	X
IEC [91]	2021	Industrial Healthcare equipment, SDN Switch	MITM, Traffic Sniffing, DoS, Unauthorized Access	✓	✓	X
CICIoMT2024	2024	Sense-U Baby Monitor, SOS Multifunctional Pager, SINGCALL SOS Button, Ecobee Camera, blink mini, M1T laxihub, owltron, TP-Link_CIC (AP2), Raspberry pi 4 (4), iPad, TP-Link_CICIoT_Doctor (AP1), Lookee Sleep ring, Powerlabs HR Monitor Arm band, COOSPO 808s Chest HR Monitor, COOSPO HW807 Armband, Livlov Heart Rate Sensor, Wellue O2 Ring - 3438, Lookee O2 Ring, Checkme BP2A, SleepU Sleep Oxygen Monitor, Rhythm+ 2.0, Wellue Pulsebit EX, Kinsa Thermometer, Checkme O2 Wrist Pulse Oximeter (2), Dell CICM99, Samsung A11. Simulated devices: Withings BPM Connect, Withings Thermometer, Lookee Ring-Pro Sleep Monitor, Qardio Base 2, Wellue EKG, iHealth Smart Wireless Gluco-Monitoring System, Wellue Visual Oxy Wrist Pulse Oximeter, Nasal/Mouth Air Flow Sensor, EMG (Electro-myography Sensor), GSR (Galvanic Skin Response Sensor), Industrial devices, UASure II Meter, Fall Detector, Baby Sleep Position - SenseU Baby, Spirometer	ARP spoofing, Ping Sweep, Recon VulScan, OS Scan, Port Scan, MQTT Malformed Data, MQTT DoS Connect flood, MQTT DoS Publish flood, MQTT DDoS Connect flood, MQTT DDoS Publish flood, DoS TCP, DoS ICMP, DoS SYN, DoS UDP, DDoS TC, DDoS ICMP, DDoS SYN, DDoS UDP	✓	✓	✓

Moreover, other IoT security datasets are not necessarily focused on healthcare applications. "IoT-SH [92] presents data related to twelve attacks, categorized into four classes, that were carried out against eight smart home devices.". Kitsune [93] is a dataset comprising four different classes

 doi:10.20944/preprints202402.0898.v1

of attacks conducted for 9 IoT devices. MedBIoT [94] is built using an IoT network topology with a combination of real and emulated devices. The authors in [95] introduce the IoT-23 dataset as a botnet dataset. IoTIDs (2020) [96] is another IoT security dataset comprising the execution of four attacks against two devices. On the other hand, the authors in [97] and [98]introduce the MQTT datasets. Finally, [99], [100], and [28] propose IoT datasets comprising more extensive testbeds and experiments.

4. The Proposed CICIoMT2024

This Section introduces the details of how the CICIoMT2024 dataset was planned, generated, and captured. This discussion includes the facilities where all experiments were conducted, the topology adopted, malicious traffic generation, and aspects of IoMT profiling.

4.1. CIC IoT lab

Establishing an IoT lab with several devices is difficult for many reasons. Such devices require supporting network devices (e.g., routers, access points, and switches) to connect and a team capable of setting up all the configurations needed. Furthermore, purchasing these devices at scale requires planning and financial investments that are not readily available. The Canadian Institute for Cybersecurity (CIC) has invested in establishing a well-equipped IoT lab. This investment comprises the acquisition of tens of IoT devices for multiple purposes (e.g., healthcare devices, home automation devices, and next-generation devices), several supporting network systems (e.g., routers, switches, access points, servers, adapters, sniffers, and networks taps), IoT kits (e.g., Arduino and Raspberry Pi's), and miscellaneous devices. Besides, a technical team is dedicated to maintaining and managing the current IoT devices, network, and inventory while analyzing new IoT devices that can be purchased and included in our topology.

Figure 2 illustrated the CIC IoT lab. Devices are connected across the IoT lab in multiple places as several power plugs are available. There are racks across the room to simplify the organization of devices. Finally, all devices are labelled to streamline management and identification.

Figure 2. CIC IoT Lab.

4.2. IoMT Topology

The CICIoMT2024 comprises the use of several devices and multiple purposes. Figure 3 illustrates the devices used alongside the network segregation. The main goal of this topology is to simplify the process of capturing network traffic from different protocols while mimicking realistic operations. Besides, devices are separated based on the protocol used to enable protocol-specific attacks to be executed and captured.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 February 2024 doi:10.20944/preprints202402.0898.v1

Figure 3. CICIoMT2024 topoly.

An iPad acts as a remote controller for several devices across the network. This iPad and four Raspberry Pi's are connected to an access point. In this case, the Raspberry Pi is a malicious device that launches all attacks. Then, this access point is connected to a Netgear switch, which gives access to the IoMT devices as well as to the Internet provider. This Internet connection is essential since many IoMT devices need to connect to remote servers.

Furthermore, all the traffic between the switch and the IoMT devices is captured using a network tap. This device is a dedicated hardware that enables real-time duplication of packets without affecting the network performance. The traffic is collected and stored by network monitors. Then, this network tap is connected to another access point that acts as a gateway for the IoMT devices.

This access point connects all IoMT devices. First, 15 simulated devices are connected to the network using the MQTT protocol. Table 2 lists all simulated devices and presents their IP addresses, time profiles, categories, and simulated value range. Second, 7 Wi-Fi devices are also connected to the CICIoMT2024 topology. Table 3 lists all devices alongside their MAC addresses. Note that the iPad remote controller and the attacking Raspberry Pi are also presented in the table. Finally, 14 Bluetooth Low-Energy (BLE) devices are connected through a smartphone. These devices are listed in Table 4.

 doi:10.20944/preprints202402.0898.v1

Table 2. Simulated Devices used in the CICIoMT2024.

Device Name	IP Address	Time Profile	Category	Simulated Value Range
Withings BPM Connect	10.0.0.1	Periodic-30sec	Blood Pressure Withings	DIA (40- 130 mmHg) / SYS (60-230 mmHg)
Withings Thermometer	10.0.0.2	Periodic-4sec	Temperature Withings	35C - 43C
Lookee Ring-Pro Sleep Monitor	10.0.0.7	Periodic-1sec	Sleep Monitor Lookee	30-250 bpm
Qardio Base 2	10.0.0.8	Periodic-5sec	Weighing Scale	5-180kg
Wellue EKG	10.0.0.4	Periodic-30sec	Pulse	30-250bpm
iHealth Smart Wireless Gluco-Monitoring System	10.0.0.9	Periodic-5sec	Glucometer	20-600mg/dL
Wellue Visual Oxy Wrist Pulse Oximeter	10.0.0.12	Periodic-1sec	Pulse Oximeter	70-100%
Infusion Pump	10.0.0.13	Periodic-4 mins	Infusion Pump	10-100mL
Nasal/Mouth Air Flow Sensor	10.0.0.3	periodic-1sec	Breathing	0–60 ppm peaks/min
EMG (Electro-myography Sensor)	10.0.0.10	Periodic-1min	Biomedical Sensor	0-60 cpm (contractions / min)
GSR (Galvanic Skin Response Sensor)	10.0.0.11	Periodic-2mins	Biomedical Sensor	0-20 uS (micro Semens)
UASure II Meter	10.0.0.6	Periodic-10sec	Blood Uric Acid	3-20 mg/dL
Fall Detector	10.0.0.5	periodic-3mins	Fall	Fall Detected
Baby Sleep Position - SenseU Baby	10.0.0.15	Periodic-4mins	Sleep Position	Sleep Position
Spirometer	10.0.0.14	Periodic-3secs	Spirometry	100-900L/min

Table 3. Wi-Fi Devices used in the CICIoMT2024.

Device Name	MAC Address
Sense-U Baby Monitor	34:94:54:F0:DB:F0
SOS Multifunctional Pager	FC:67:1F:E1:9E:58
SINGCALL SOS Button	1C:90:FF:E6:E2:4B
Ecobee Camera	44:61:32:E8:88:2F
blink mini	90:11:95:16:40:3B
M1T laxihub	F4:B1:9C:C9:79:FF
Owltron	FC:67:1F:F7:CB:07
Raspberry pi 4 (1)	DC:A6:32:DC:27:D5
Raspberry pi 4 (4)	DC:A6:32:C9:E5:A4
Raspberry pi 4 (9)	DC:A6:32:C9:E4:D5
Raspberry pi 4 (7)	DC:A6:32:C9:E4:AB
iPad	E6:AA:E4:09:FC:8A

Table 4. Bluetooth Devices used in the CICIoMT2024.

Device Name	BT MAC Address	Device Name	BT MAC Address
Lookee Sleep ring 5569	c2:52:be:33:2f:20	Checkme BP2A (BPMonitor)	d0:7f:54:a5:f2:51
Powerlabs HR Monitor Arm band (WRIST)	D3:36:04:BD:77:36	SleepU Sleep Oxygen Monitor	c2:20:57:14:11:78
COOSPO 808s Chest HR Monitor	dd:77:40:54:1f:98	Rhythm+ 2.0 (Scosche)	f2:8d:2e:ec:c5:56
COOSPO HW807 Armband	ce:3e:10:2c:68:8a	Wellue Pulsebit EX	55:55:0a:05:a7:2e
Livlov Heart Rate Sensor	e7:ae:80:89:a8:b2	Kinsa Thermometer	c6:c6:df:f6:4d:19
Wellue O2 Ring	e3:28:42:de:34:58	Checkme O2 Wrist Pulse Oximeter	e3:4e:ec:2f:9e:42
Lookee O2 Ring	c8:1a:2a:27:ea:01	CheckmeO2 Wrist Pulse Oximeter	f2:4e:56:88:a4:4b

 doi:10.20944/preprints202402.0898.v1

4.3. Generation of Malicious Traffic

To enable the development of cybersecurity solutions, a benchmark dataset needs to mimic aspects of real IoMT deployments and operations. To accomplish this, we consider aspects of different protocols as well as the characteristics of individual devices.

4.3.1. Wi-Fi

The devices contained in the Wi-Fi topology involve 4 Raspberry Pi's attackers, and a remote controller (iPad) connected to one Access point. The healthcare devices are connected to the other access point on the other side of the network tap. These devices comprise 3 healthcare devices and 4 cameras.

Several attacks were executed against Wi-Fi devices. ARP spoofing was carried out to perform Man-in-the-middle attacks [101]. Regarding Dos and DDoS [102,103], we executed ICMP Flood, SYN Flood, TCP Flood, and UDP Flood. Finally, reconnaissance attacks were conducted [104,105], including Port Scan, OS Scan, Ping Sweep, and vulnerability scan.

4.3.2. MQTT

To simulate IoMT devices operating on the MQTT protocol, we used IoTFlock [90]. This simulation platform generates network traffic and is developed for IoMT applications. The simulator was run using a VMware image (Ubuntu OS running on version 18.04.6 LTS) containing an executable IoTFlock GUI C++, allowing the creation of executable environments using XML. Once an XML has been created, IoTFlock parses it, and runs the simulation. In fact, all simulated MQTT devices that publish numerical values do not include units of measurement. Also, the MQTT topology contains a local connection between a PC that hosts the IoTFlock virtual machine and a Ubuntu laptop running an MQTT broker.

A MQTT switch establishes this connection. The IoTFlock PC shares network interfaces with the Virtual Machine (VM). Furthermore, the iPad acts as a remote controller and also as an MQTT subscriber.

Moreover, three different attacks were executed against MQTT devices. First, the MQTT Connect Flood was executed. This attack floods the MQTT broker with several connect packets to establish a connection [106]. To accomplish this, a custom Python script was developed to conduct both Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. Second, MQTT Publish Floods were also conducted. This threat uses publish packets under random topics and was executed in a DoS and DDoS format. Finally, the MQTT Malformed Data attack was executed. This attack uses the MQTTSA tool [107] and tries to sniff the broker by sending specific packets to understand its behavior. In this process, the attacker collects the names of topics that have been published to it and attempts to send malformed data. To accomplish this, we modified the tool to send each topic collected some malformed data.

4.3.3. Bluetooth Low Energy (BLE)

Given the criticality of the data BLE devices generate in the IoMT context, it is paramount that they are secured against potential attacks. However, BLE requires a particular approach to both execute attacks and capture the network traffic. To accomplish this, we used a smartphone connected to the BLE devices. Then, an attacker PC conducts the malicious activities.

In this case, the Bleak library is adopted as a tool for Bluetooth operations in Python and scanned nearby BLE devices in a discovery approach. The script attempts to establish a connection and fetch all the services and characteristics to determine the data format. This effort empowers attackers to potentially disrupt the device's operations.

The script then iterates through each characteristic, attempting to write data packets of varying sizes, ranging from 20 bytes to 810 bytes in increments of 10 bytes. The data packets consisted of repeating numeric sequences, e.g., an arbitrary data packet would follow a trend as

 doi:10.20944/preprints202402.0898.v1

"0123456789012345...". All successful writing was logged, noting the characteristics' Universally Unique Identifier (UUID) and the data format that succeeded.

After identifying the successful UUIDs and their corresponding data formats, the script entered a continuous loop, constantly writing data to these UUIDs. This continuous writing aimed to potentially overload the device or disrupt its regular operations, thereby executing a DoS attack.

To gather comprehensive data, we not only examined benign logs (Bluetooth snoop log on the Android device where the IoT device is supposed to communicate with using Android SDK) but also utilized the Ubertooth One sniffer to capture attack logs right from the PC where the Attack script originated. This dual-log approach ensured we had a holistic understanding of the device's behavior under both normal and attack conditions.

Furthermore, this methodology was replicated for each healthcare device and the outcome provided valuable insights into the resilience and vulnerabilities of these devices in the face of BLE-based attacks:

- **Lookee Sleep Ring:** showcased resilience against the attack, operating without any noticeable disruptions.
- **Powerlabs HR Monitor Arm Band:** Similarly, this armband maintained its standard functionality during the attack.
- **COOSPO HW807 Armband:** In stark contrast, our attack had a significant impact on this device. It became overwhelmed and subsequently turned off.
- **Livlov Heart Rate Sensor:** This heart rate sensor managed to resist our attack, operating without any observed disruptions.
- **Wellue O2 Ring:** This device remained unaffected and continued to operate normally.
- **Lookee O2 Ring:** This device was vulnerable to our attack. Upon execution, the device became overwhelmed and turned off.
- **Checkme BP2A:** This device displayed a unique behavior. While it stored data during the attack, it only transmitted this data once a Bluetooth connection was re-established.
- **SleepU Sleep Oxygen Monitor:** This monitor resisted our attack, showcasing its resilience by maintaining standard functionality.
- **Rhythm+ 2.0 (Scosche):** significantly affected by our attack, this device became overwhelmed and subsequently shut down.
- **Wellue Pulsebit EX:** This device withstood the attack and continued to operate without disruptions.
- **Checkme O2 Smart Wrist Pulse Oximeter:** It resisted our attack, continuing its standard operations.
- **Kinsa Thermometer:** Our attack impacted this device uniquely. While under attack, it was not possible to reset the connection by turning off the thermometer. The only methods to terminate the connection were to either let the battery deplete or to halt the attack. The device behaved as it remained connected throughout the attack.

Finally, as illustrated in Figure 4, the Bluetooth experiments were executed inside of a Faraday Cage to block external signals that may interfere with the network traffic collected.

 doi:10.20944/preprints202402.0898.v1

Figure 4. CIC's Faraday Cage used in Bluetooth experiments to block external signals that may interfere with the network traffic collected.

4.4. IoMT Profiling

Understanding the behavioral aspects of IoMT operations is vital to enhancing these systems' security. To enable the development of such methods, we describe how the generation and collection of profiling data were conducted for different experiments.

4.4.1. Power Experiments

The power experiments for Wi-Fi enabled devices are carried out by disconnecting all the devices from the network. In these experiments, the MQTT network is not considered as a simulated network. Hence, we are only interested in the 7 Wi-Fi devices. Furthermore, all Raspberry Pi's from the previous sections were disconnected. The iPad is the only device connected to the network to control and monitor devices.

The captures were done similarly to CICIoT2022 [100], wherein all devices are disconnected from the network. The device we are interested in is powered on, and its behavior is captured by filtering the MAC address for about 2 minutes. The device is later powered off, and capture is allowed to continue for another 3 minutes for leftover packets or until no packets are transmitted from the device. However, some devices did not have physical power buttons, and adjustments needed to be made to perform the experiments:

1. **Singcall Sensor:** This device does not explicitly have a power button instead it has a reset button. The device is disconnected from the network when reset and connects back to it when we reconnect the device to the app.
2. **SOS Multifunctional Pager:** This device includes the button and its base station. In these experiments, since the button depended on the base station, the base station was powered on and off.
3. **Sense U Baby:** This device includes an MQTT base station (publisher) and a sensor that collects data and sends it to the base station. The data collected during this experiment is that of the base station. The sensor was excluded since it does not take part in communicating with the cloud service and only repeatedly collects data and transmits it to the base station for publishing. This behavior is later analyzed in idle/active experiments.

Similarly, the same procedure was conducted for 10 applicable Bluetooth Low Energy (BLE) enabled devices wherein their power behaviours were captured when connecting to the smartphone.

 doi:10.20944/preprints202402.0898.v1

4.4.2. Idle Experiments

The idle experiments are carried out in a span of two 13-hour captures. The captures were performed on two nights between the hours of 6:00 pm, and 7:00 am to ensure no interaction with devices would happen. Among our Wi-Fi devices, only the Singcall SOS Button did not produce any traffic. Another similar device, the Multifunctional Pager (SOS button paired with base station) had some form of external communication with services.

In these experiments, the Sense-U Baby Monitor was disconnected from its base station since the sensor does not have any idle state. The base station, however, continuously measured the temperature and humidity of the environment.

The MQTT broker was connected to this capture, and the iPad was subscribed to it. The iPad (subscriber) was running for the full 26 hours. In fact, no simulated MQTT traffic was published during these experiments. It was expected that the broker would remain idle during the capture, and the only traffic produced was when the subscriber pinged the broker at different times to ensure it was awake and when the broker made DNS queries.

4.4.3. Active Experiments

The experiments were done in batches to accumulate a total of 26 hours. The devices were left to interact with one another as people actively (e.g., triggering SOS buttons, wearing baby sleep sensors, interacting with apps) or passively (e.g., motion detection from cameras) interacted with the devices. MQTT simulation was also included in these captures. Finally, It was observed during these captures that the M1T Laxihub camera sends unencrypted image frames to its cloud.

4.4.4. Interaction Experiments

The interaction experiments were carried out by capturing the interaction with devices either physically or through their companion apps. 3 types of interactions were considered where applicable:

1. **Physical:** carried out where devices could be interacted with using physical buttons. These experiments were combined with LAN and WAN experiments where applicable, i.e., the apps were either connected to the same network as the IoMT devices or connected to another network.
2. **LAN:** These experiments were carried out by making use of the device's companion apps, and interacting with them while being on the same network as the IoMT devices.
3. **WAN:** These experiments were carried out by making use of the device's companion apps, and interacting with them while being on another network as the IoMT devices.

5. Methodology

Once the experiments have been conducted and the network traffic has been stored in PCAP format, the data needs to be organized to simplify access. Figure 5 illustrates the process of storing network traffic in PCAP format, converting this traffic into CSV files, conducting Machine Learning (ML) evaluation, and reporting integrated results.

 doi:10.20944/preprints202402.0898.v1

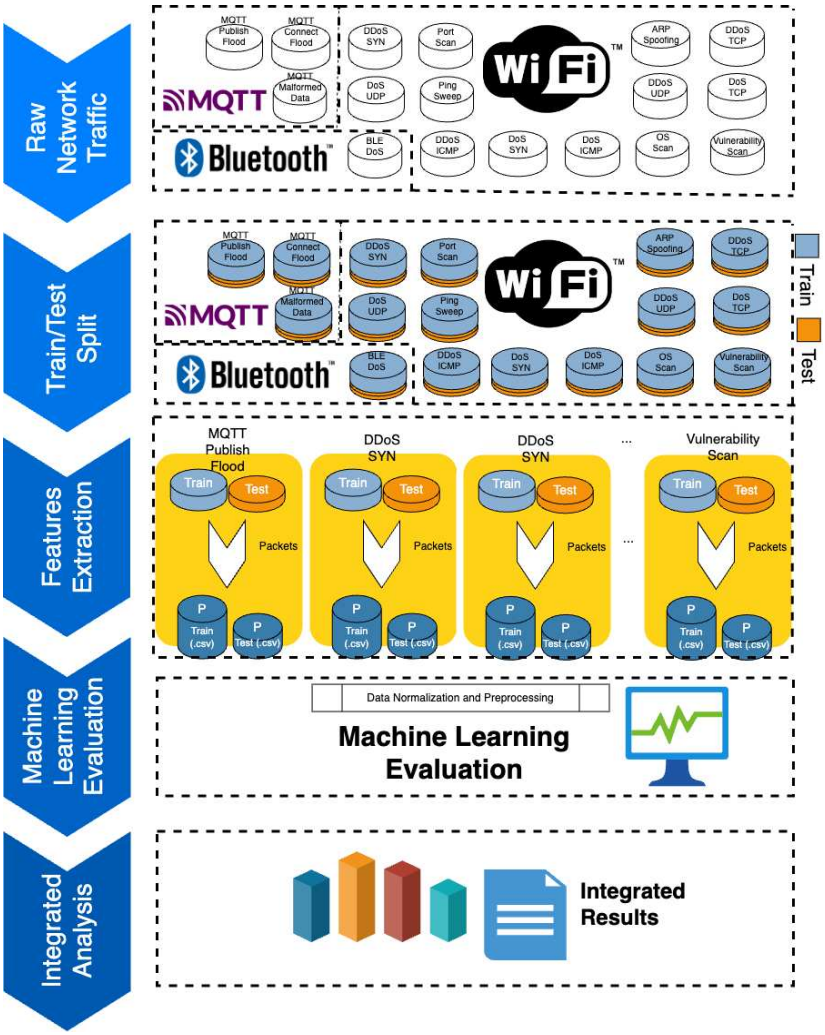


Figure 5. Methodology adopted to produce the CICIoMT2024 dataset: storing network traffic in PCAP format, converting this traffic into CSV files, conducting Machine Learning (ML) evaluation, and reporting integrated results.

First, the raw network traffic is stored in PCAP files. These are the original traffic data that can be used in future research directions to secure IoMT operations. These files are separated into MQTT, Bluetooth (BLE), and Wi-FI. Finally, profiling experiments are also stored in PCAP format.

Second, we divide the collected traffic into two groups: (i) train and (ii) test. The “train" group is intended to be used to develop new solutions (e.g., ML training), while the “test" group is designed to evaluate such solutions in unseen data. This division relies on defining a group of PCAP files comprising 80% (“train") and 20% (“test") of all PCAP files available.

After that, a process of converting PCAP files to CSV files is conducted for each attack. In this case, we target Wi-Fi and MQTT attacks due to the nature of their features. To accomplish this, a set of supporting tools needs to be used and are illustrated in Figure 6. First, TCPDUMP [108] is used to split a big PCAP file into a group of smaller PCAP files. This is done to enable the parallel execution of the conversion script. Then, for each PCAP chunk, DPKT [109] is used in parallel to extract features and save them into CSV format. As the traffic generated is extensive, we average packets with varying window sizes of 10 (i.e., ping sweep, vulnerability scan, Bluetooth benign, Bluetooth DoS, OS scan, MQTT malformed data, ARP spoofing, port scan, and benign) and 100 (e.g., MQTT DoS connect flood, MQTT DDoS connect flood, MQTT DoS publish flood, MQTT DDoS publish flood, DoS TCP, DoS ICMP, DoS SYN, DoS UDP, DDoS SYN, DDoS TCP, DDoS ICMP, DDoS UDP) packets. Finally, these resulting CSV files are combined into a single CSV file using Pandas [110].

 doi:10.20944/preprints202402.0898.v1

Furthermore, different ML techniques are evaluated to assess their performance in detecting and classifying these attacks. In this research, we evaluate the performance of five widely used ML techniques, namely Logistic Regression [111], Adaboost [112–114], Random Forest [115], and Deep Neural Network [116]. The evaluation is focussed on three tasks: Binary classification (i.e., Begnign and Attack), Categorical Classification (i.e., benign, spoofing, DDoS, DoS, recon, and MQTT), and multiclass classification (i.e., including all classes available).

Finally, the integrated results are presented using multiple metrics. Considering *TP* True Positives, *TN* True Negatives, *FP* False Positive, and *FN* False Negatives, the metrics used in this research are [117]:

- **Accuracy:** evaluates the classification models by calculating the proportion of correct predictions in a dataset using the following expression:

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

- **Recall:** ratio classes identified to the total number of occurrences of this particular class:

$$Rec = \frac{TP}{TP + FN} \tag{2}$$

- **Precision:** ratio of correctly classified labels to the total number of positive classifications:

$$Pre = \frac{TP}{TP + FP} \tag{3}$$

- **F1-Score:** geometric average of precision and recall:

$$F1 = 2 \times \frac{Pre \times Rec}{Pre + Rec} \tag{4}$$

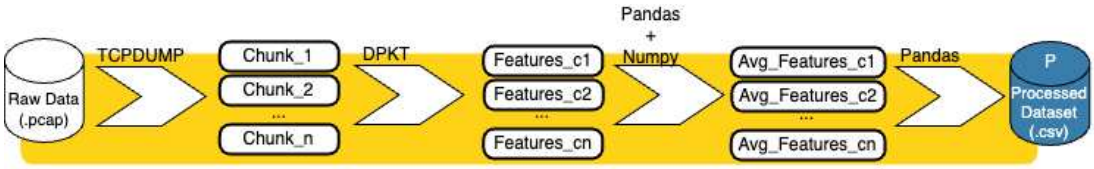


Figure 6. Process of converting PCAP files to CSV files.

6. Feature Extraction and Data Description

The process of extracting features from PCAP files to CSV aims to simplify threat detection. Several features can be extracted and engineered to represent multiple traffic characteristics (e.g., protocols and temporal aspects) in this context. Table 5 lists the features extracted and used in the ML evaluation process. Although this is a comprehensive list that represents several aspects of the network traffic, this selection can be easily increased by recurring to the original PCAP files. Table 6 describes the data for the CICIoMT2024 dataset by presenting the mean, standard deviation (std), minimum (min), 25% percentile (25%), 50% percentile (50%), 75% percentile (75%), and maximum (max) values for each feature.

 doi:10.20944/preprints202402.0898.v1

Table 5. Features Extracted from PCAP files [28].

#	Feature	Description
1	Header Length	Length of the packet header
2	Duration	Lifetime of the packet in transit
3	Rate	Speed of packet transmission within a flow
4	Srate	Transmission speed of outgoing packets in a flow
5	fin flag number	Value of the Fin flag in TCP/IP
6	syn flag number	Value of the Syn flag in TCP/IP
7	rst flag number	Value of the Rst flag in TCP/IP
8	psh flag numbe	Value of the Psh flag in TCP/IP
9	ack flag number	Value of the Ack flag in TCP/IP
10	ece flag numbe	Value of the Ece flag in TCP/IP
11	cwr flag number	Value of the Cwr flag in TCP/IP
12	syn count	Tally of Syn flag occurrences in a flow
13	ack count	Tally of Ack flag occurrences in a flow
14	fin count	Tally of Fin flag occurrences in a flow
15	rst count	Tally of Rst flag occurrences in a flow
16	IGMP	Denotes the use of IGMP in application layer protocols
17	HTTPS	Denotes the use of HTTPS in application layer protocols
18	HTTP	Denotes the use of HTTP in application layer protocols
19	Telnet	Denotes the use of Telnet in application layer protocols
20	DNS	Denotes the use of DNS in application layer protocols
21	SMTP	Denotes the use of SMTP in application layer protocols
22	SSH	Denotes the use of SSH in application layer protocols
23	IRC	Denotes the use of IRC in application layer protocols
24	TCP	Usage of TCP in the transport layer protocol
25	UDP	Usage of UDP in the transport layer protocol
26	DHCP	Presence of DHCP in the application layer protocol
27	ARP	Usage of ARP in the link layer protocol
28	ICMP	Usage of ICMP in the network layer protocol
29	IPv	Usage of IP in the network layer protocol
30	LLC	Usage of LLC in the link layer protocol
31	Tot sum	Total packet length within a flow
32	Min	Shortest packet length in a flow
33	Max	Longest packet length in a flow
34	AVG	Mean packet length in a flow
35	Std	Variability in packet length within a flow
36	Tot size	Length of the packet
37	IAT	Interval between the current and previous packet
38	Number	Total number of packets in the flow
39	Radius	Root mean square of the variances of incoming and outgoing packet lengths in the flow
40	Magnitude	Root mean square of the averages of incoming and outgoing packet lengths in the flow
41	Variance	Ratio of the variances of incoming to outgoing packet lengths in the flow
42	Covariance	Covariance between the lengths of incoming and outgoing packets
43	Weight	Product of the number of incoming and outgoing packets
44	Protocol Type	Type of protocol used (IP, UDP, TCP, etc.) expressed in integer values

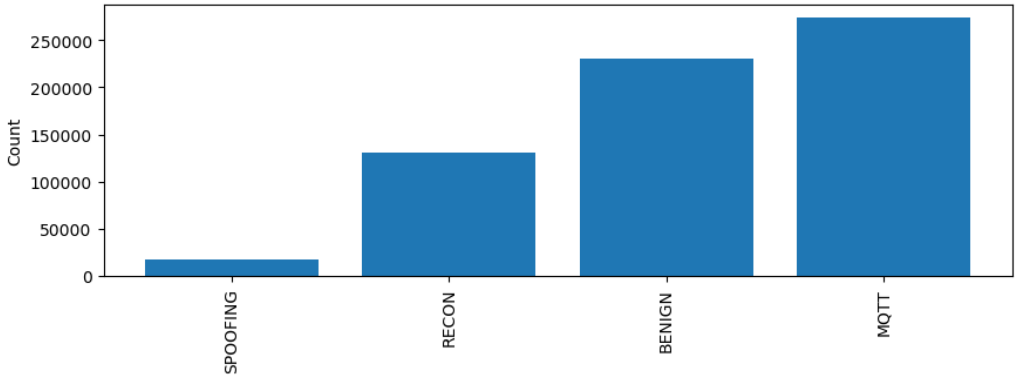
 doi:10.20944/preprints202402.0898.v1

Table 6. Data Description for the CICIoMT2024.

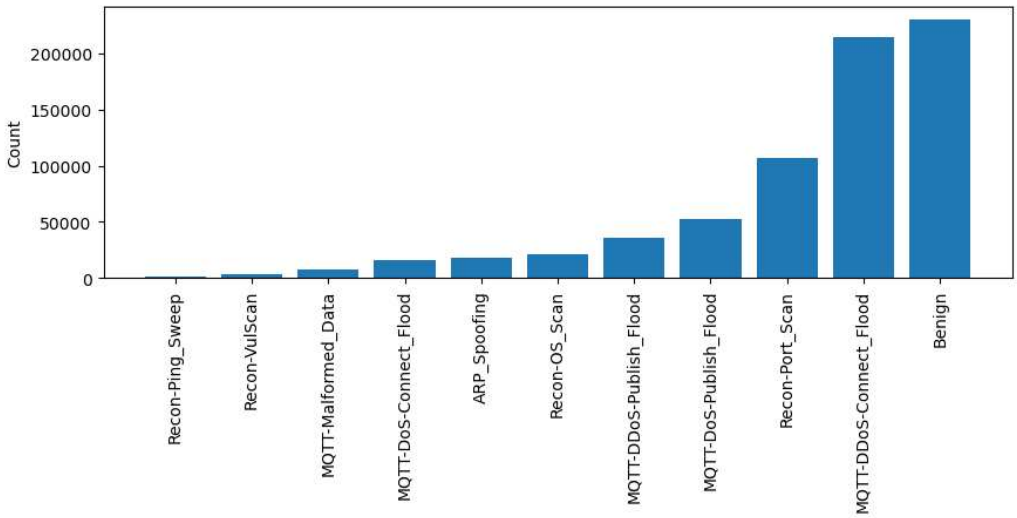
	mean	std	min	25%	50%	75%	max
Header_Length	29962.4717	282363.394	0	2.17	108	19421	9896704
Protocol Type	8.04720327	6.30483218	0	1.05	6	17	17
Duration	64.6369088	7.85306556	0	64	64	64	255
Rate	15744.4895	40008.5463	0	6.42273084	133.141869	19759.2022	2097152
Srate	15744.4895	40008.5463	0	6.42273084	133.141869	19759.2022	2097152
fin_flag_number	0.0051233	0.03415862	0	0	0	0	1
syn_flag_number	0.15721153	0.33687886	0	0	0	0	1
rst_flag_number	0.03951838	0.13929947	0	0	0	0	1
psh_flag_number	0.02217887	0.0965354	0	0	0	0	1
ack_flag_number	0.09566387	0.25214153	0	0	0	0	1
ece_flag_number	2.91E-06	0.0005036	0	0	0	0	0.2
cwr_flag_number	1.92E-06	0.00037966	0	0	0	0	0.2
ack_count	0.02797713	0.17825565	0	0	0	0	11.2
syn_count	0.2938792	0.60364144	0	0	0	0	10.7
fin_count	0.08557531	0.56123908	0	0	0	0	151.74
rst_count	65.8712672	498.281211	0	0	0	0	9576.5
HTTP	0.00086767	0.0284215	0	0	0	0	1
HTTPS	0.00559028	0.06034021	0	0	0	0	1
DNS	0.00015156	0.0052478	0	0	0	0	1
Telnet	1.25E-05	0.00089169	0	0	0	0	0.1
SMTP	1.25E-05	0.00089171	0	0	0	0	0.1
SSH	2.61E-05	0.00271903	0	0	0	0	1
IRC	1.25E-05	0.00089234	0	0	0	0	0.11111111
TCP	0.41487102	0.48990278	0	0	0	1	1
UDP	0.31084898	0.45956644	0	0	0	1	1
DHCP	3.26E-06	0.00098659	0	0	0	0	0.6
ARP	0.00076075	0.01928389	0	0	0	0	1
ICMP	0.27351348	0.44404871	0	0	0	0.99	1
IGMP	4.47E-06	0.0012065	0	0	0	0	0.7
IPv	0.99923925	0.01928389	0	1	1	1	1
LLC	0.99923925	0.01928389	0	1	1	1	1
Tot sum	636.01138	991.6091	42	441	525	567	23467
Min	55.1201614	69.0993765	42	42	50	54	1514
Max	72.3325073	133.609047	42	43.77	50	54	1514
AVG	60.5865132	88.0720219	42	42.0933304	50	54	1514
Std	6.06053694	38.0578569	0	0	0	0	721.15087
Tot size	60.5890934	87.8768798	42	42.24	50	54	1514
IAT	84683677.9	17819169.6	-1.2820613	84679174	84696417	84696902.6	169470846
Number	9.49908609	0.84157738	1	9.5	9.5	9.5	15
Magnitue	10.4382451	3.15807323	9.16515139	9.17497736	10	10.3923048	55.027266
Radius	8.56000977	53.8045034	0	0	0	0	1020.23203
Covariance	2370.54475	19758.8155	0	0	0	0	520437.887
Variance	0.09074362	0.2329791	0	0	0	0	1
Weight	141.527342	21.6618865	1	141.55	141.55	141.55	244.6

Nevertheless, Figures 7 and 8 illustrates the data distribution for each class present in the dataset. In fact, the amount of data generated by DDoS and DoS attacks is much larger than in any other experiment. These graphs show that the dataset presents a much larger proportion of attacks than benign traffic. It results from the number of attacks executed against the proposed topology. The categorial classification graph shows that most of the traffic collected stems from MQTT and benign traffic. The multiclass classification graph shows that benign and MQTT connect floods represent the majority of the traffic generated, while some attacks present reduced traffic due to the challenges of large-scale data generation (e.g., ping sweep). Nevertheless, Figure 8 depicts the traffic generated by DoS and DDoS. These two classes present a substantial number of instances, and the majority of the specific attacks executed refer to UDP and ICMP floods. Table 7 presents the number of instances for each attack, presenting the total count (i.e., attack and benign), the categorical count (i.e., spoofing, recon, MQTT, DoS, and DDoS), and the individual count (i.e., considering all individual attacks).

 doi:10.20944/preprints202402.0898.v1



(a) Categorical Classification

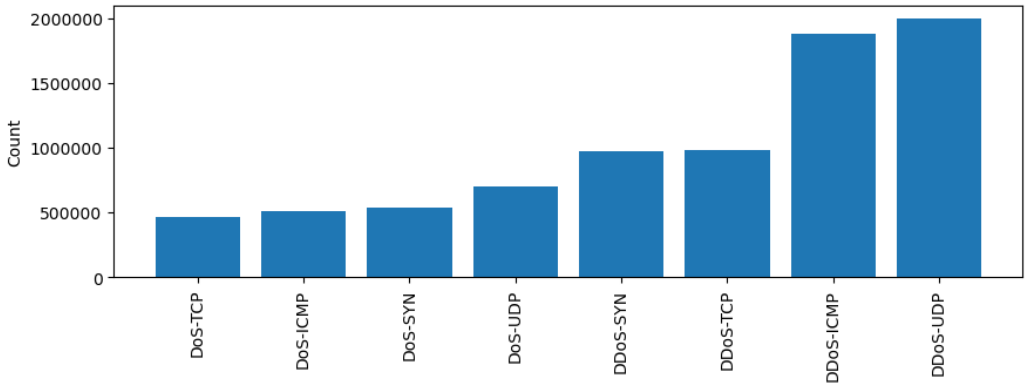


(b) Multicalss Classification

Figure 7. Class Distribution in (a) Categorical, and (c) Multiclass classification.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 February 2024 doi:10.20944/preprints202402.0898.v1

(a) Categorical Classification



(b) Multicalss Classification

Figure 8. Class Distribution in (a) Caterical, and (b) Multiclass classification for DoS and DDoS.

Table 7. Number of Instances in each class of the CICIoMT2024 dataset.

Class	Category	Attack	Count
BENIGN	-	-	230339
ATTACK	SPOOFING	ARP Spoofing	17791
	RECON	Ping Sweep	926
		Recon VulScan	3207
		OS Scan	20666
		Port Scan	106603
	MQTT	Malformed Data	6877
		DoS Connect Flood	15904
		DDoS Publish Flood	36039
		DoS Publish Flood	52881
		DDoS Connect Flood	214952
	DoS	DoS TCP	462480
		DoS ICMP	514724
		DoS SYN	540498
		DoS UDP	704503
	DDoS	DDoS SYN	974359
		DDoS TCP	987063
		DDoS ICMP	1887175
		DDoS UDP	1998026

7. Machine Learning (ML) Evaluation

The experiments conducted in this research evaluated the performance of four ML techniques: Logistic Regression (LR), Random Forest (RF), Adaboost (AD), and Deep Neural Network (DNN). Three classification problems were considered: Binary classification (i.e., benign and attack), categorical classification (i.e., benign, spoofing, recon, MQTT, DoS, and DDoS), and multiclass classification (i.e.,

 doi:10.20944/preprints202402.0898.v1

including all classes available). Figure 9 illustrates the experiments' results regarding accuracy, recall, precision, and F1-score. Also, Table 8 lists the numerical results obtained in each scenario.

The overall results show that all ML techniques performed well in several scenarios. However, this graph also shows that some techniques presented a decrease in performance in some cases. Considering the binary classification, all methods could distinguish benign and attacks successfully. In this scenario, the rate of mislabeled instances is low as accuracy, and the F1-score reaches values above 0.98. In the categorical classification scenario, there is a clear impact on the performance of some algorithms. While RF can maintain high performance, LR significantly reduces the resulting values. The most challenging scenario refers to the multiclass classification. In this 19-class challenge, the overall performance is decreased for all metrics as detecting internal patterns for each attack becomes more difficult. Conversely, RF and DNN could still present accuracy results of 0.76 and 0.99, respectively. In terms of the F1-score, RF presents 0.907.

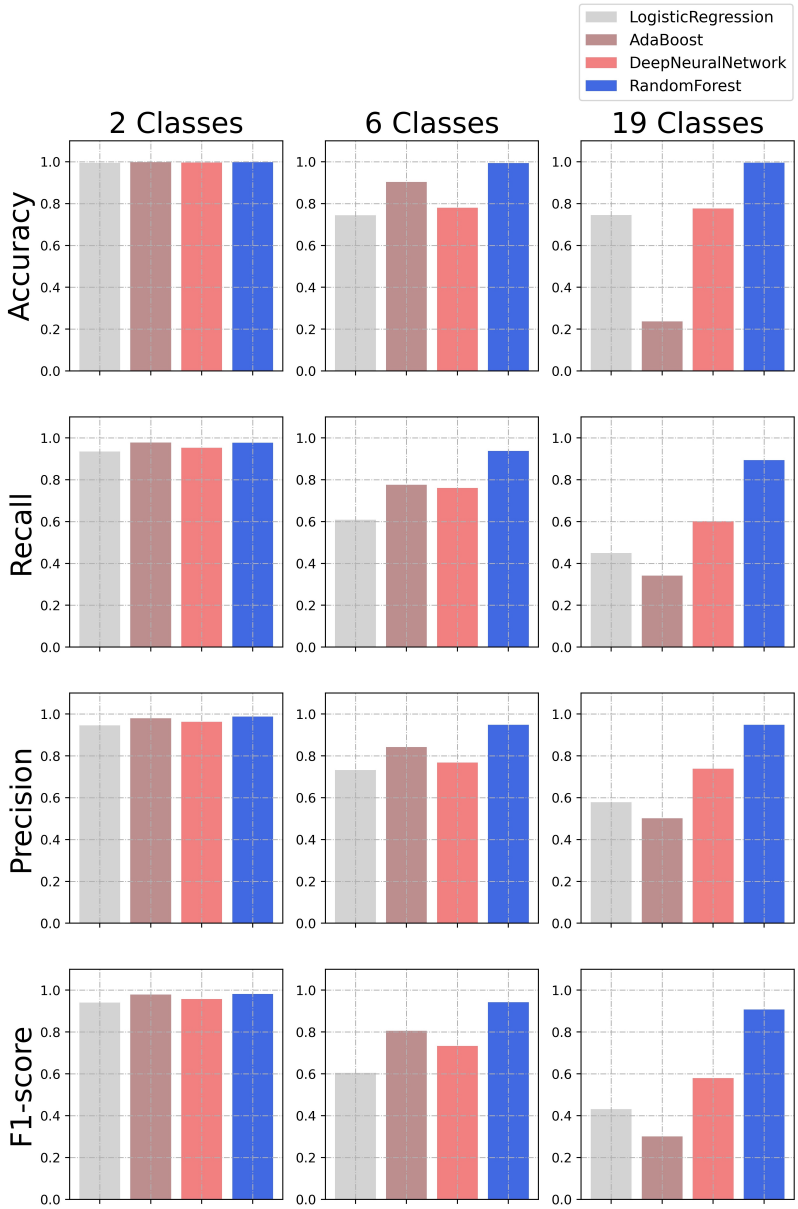


Figure 9. Results obtained in the experiments conducted regarding accuracy, recall, precision, and F1-score. These experiments comprise the classification of IoMT attacks in multiple scenarios (2, 6, and 19 classes).

 doi:10.20944/preprints202402.0898.v1

Table 8. Results obtained in the experiments conducted regarding accuracy, recall, precision, and F1-score. These experiments comprise the classification of IoMT attacks in multiple scenarios (2, 6, and 19 classes).

		LR	AB	DNN	RF
Binary (2 classes)	**Accuracy**	0.99464682	0.99807704	0.99617391	**0.99837193**
	Recall	0.93505479	**0.97788699**	0.95233191	0.97640269
	Precision	0.94600144	0.9797801	0.96276398	**0.98754544**
	F1-Score	0.94045653	0.97883158	0.95748541	**0.98190642**
Categorical (6 classes)	**Accuracy**	0.74399479	0.90303572	0.78052413	**0.99388111**
	Recall	0.60901055	0.77537141	0.76020495	**0.9379039**
	Precision	0.73229673	0.8417807	0.76809269	**0.94855819**
	F1-Score	0.60443814	0.80562143	0.73354862	**0.94221191**
Multiclass (19 classes)	**Accuracy**	0.74562534	0.23653652	0.77656609	**0.99553086**
	Recall	0.4495978	0.34171028	0.60194873	**0.89345693**
	Precision	0.57814073	0.50168939	0.73835033	**0.94831885**
	F1-Score	0.43098172	0.30109723	0.57906237	**0.90736136**

To understand the results presented, the confusion matrix highlights the challenges a given model faces for each class. Since RF outperformed the other techniques, Tables 9, 10, and 11 present the confusion matrix of RF for binary, categorical, and multiclass classification, respectively. Most instances for all classes are correctly classified for binary and categorical classification. However, distinguishing recon and spoofing attacks from benign traffic is challenging. Also, separating MQTT and TCP-IP DoS attacks is a complex task. Furthermore, the results obtained for multiclass are similar in terms of the issues faced. For example, there is a misclassification between MQTT DoS and DDoS attacks. Besides, internal recon classes are also difficult to distinguish in some cases due to the traffic similarity (e.g., OS, Port, and Vulnerability scan). Finally, although some mistakes can be found among classes of the same category (e.g., UDP DDoS and SYN DDoS), RF is capable of correctly classy instances in most cases.

Table 9. Results obtained by the Random Forest (RF) model for the binary classification problem (2 classes).

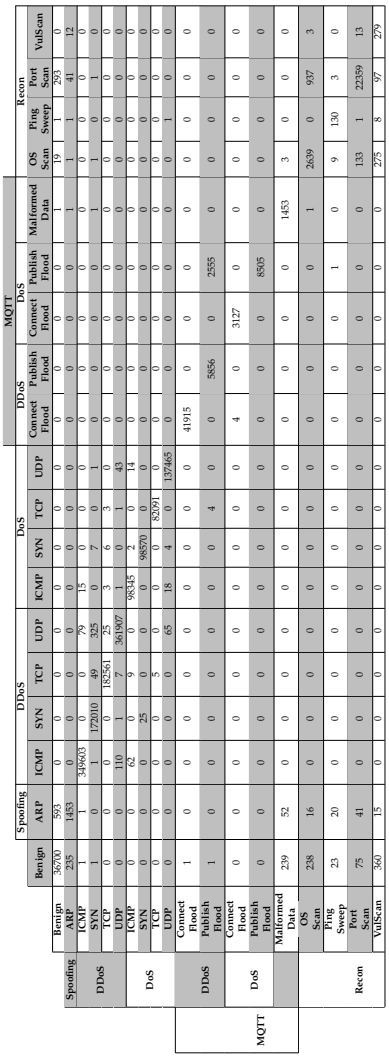
	BENIGN	ATTACK
BENIGN	35853	1754
ATTACK	874	1575701

Table 10. Results obtained by the Random Forest (RF) model for the categorical classification problem (6 classes).

	BENIGN	DDoS	DoS	MQTT	RECON	SPOOFING
BENIGN	36620	0	1	0	666	320
DDoS	2	1066695	67	0	0	0
DoS	0	170	425010	0	1	0
MQTT	234	0	7372	47548	4	52
RECON	597	0	0	5	27007	67
SPOOFING	219	0	0	1	99	1425

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 February 2024 doi:10.20944/preprints202402.0898.v1

Table 11. Results obtained by the Random Forest (RF) model for the multiclass classification problem (19 classes).



		Benign	ARP	ICMP	SYN	TCP	UDP	ICMP	SYN	TCP	UDP	Connect Flood	Publish Flood	Connect Flood	Publish Flood	Malformed Data	OS Scan	Ping Sweep	Port Scan	VulScan
		Benign	36700	593	0	0	0	0	0	0	0	1	0	0	0	1	19	1	243	0
Spoofing		ARP	235	1483	0	0	0	0	0	0	0	0	0	0	0	0	1	0	41	12
DDoS		ICMP	1	1	349633	0	0	79	15	0	0	0	0	0	0	0	0	0	0	0
		SYN	1	0	1	172010	49	325	0	7	0	0	0	0	0	0	1	0	1	0
		TCP	0	0	0	0	182561	25	3	6	3	0	0	0	0	0	0	0	0	0
		UDP	0	0	0	110	7	361907	1	0	1	43	0	0	0	0	0	0	0	0
DoS		ICMP	0	0	0	62	9	0	98345	2	0	14	0	0	0	0	0	0	0	0
		SYN	0	0	0	25	0	0	0	98570	0	0	0	0	0	0	0	0	0	0
		TCP	0	0	0	0	3	0	0	0	82091	0	0	0	0	0	0	0	0	0
		UDP	0	0	0	0	0	65	18	4	0	137465	0	41915	0	0	0	0	0	0
MQTT	DDoS	Connect Flood	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		Publish Flood	1	0	0	0	0	0	0	0	4	0	5856	0	0	0	0	0	0	0
	DoS	Connect Flood	0	0	0	0	0	0	0	0	0	0	0	3127	0	0	0	0	0	0
		Publish Flood	0	0	0	0	0	0	0	0	0	0	0	0	8505	0	0	0	0	0
		Malformed Data	239	52	0	0	0	0	0	0	0	0	0	0	0	1453	3	0	0	0
Recon		OS Scan	238	16	0	0	0	0	0	0	0	0	0	0	0	1	2639	0	937	3
		Ping Sweep	23	20	0	0	0	0	0	0	0	0	0	0	1	0	9	130	3	0
		Port Scan	75	41	0	0	0	0	0	0	0	0	0	0	0	0	133	1	22359	13
		VulScan	360	15	0	0	0	0	0	0	0	0	0	0	0	0	275	8	97	279

8. Conclusion

This research focuses on developing a multi-protocol dataset for assessing IoMT device security named CICIoMT2024. To accomplish this, 18 different attacks were against an IoMT topology comprising 40 IoMT devices. Besides, three protocols were targeted considering the characteristics of healthcare operations (i.e., Wi-Fi, MQTT, and Bluetooth). The main goal is to contribute to the existing state-of-the-art by defining a complementary baseline that supports researchers in investigating and developing new solutions for cybersecurity in healthcare and IoMT operations.

A comprehensive explanation of how the dataset was collected, processed, and stored was conducted alongside evaluating different ML algorithms. Besides, we conducted a discussion on how each attack was conducted, as well as feature extraction and data description. The dataset is available in PCAP and CSV formats and comprises the network traffic collected throughout the experiments. The www.unb.ca/cic/datasets/iomt-dataset dataset has been published on CIC's dataset page, making it available for other researchers to use.

Finally, there are several possible future directions for future work. For example, the hyperparameter optimization of ML models, the analysis and engineering of new features that can be extracted from the PCAP files, and the integration of this dataset with other healthcare resources (e.g., datasets and simulation platforms).

 doi:10.20944/preprints202402.0898.v1

Acknowledgments: The authors would like to thank the Canadian Institute for Cybersecurity (CIC) for financial and educational support.

References

1. Madakam, S.; Lake, V.; Lake, V.; Lake, V.; et al. Internet of Things (IoT): A literature review. *Journal of Computer and Communications* **2015**, *3*, 164.
2. Farooq, M.U.; Waseem, M.; Mazhar, S.; Khairi, A.; Kamal, T. A review on internet of things (IoT). *International journal of computer applications* **2015**, *113*, 1–7.
3. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet of Things journal* **2014**, *1*, 22–32.
4. Mukherjee, A.; Pal, A.; Misra, P. Data analytics in ubiquitous sensor-based health information systems. In Proceedings of the 2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies. IEEE, 2012, pp. 193–198.
5. Yuan, B.; Herbert, J. A cloud-based mobile data analytics framework: case study of activity recognition using smartphone. In Proceedings of the 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. IEEE, 2014, pp. 220–227.
6. Loke, S.W. Supporting ubiquitous sensor-cloudlets and context-cloudlets: Programming compositions of context-aware systems for mobile users. *Future Generation Computer Systems* **2012**, *28*, 619–632.
7. Hsu, C.W.; Yeh, C.C. Understanding the factors affecting the adoption of the Internet of Things. *Technology Analysis & Strategic Management* **2017**, *29*, 1089–1102.
8. Riggins, F.J.; Wamba, S.F. Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. In Proceedings of the 2015 48th Hawaii international conference on system sciences. IEEE, 2015, pp. 1531–1540.
9. Bojan, T.M.; Kumar, U.R.; Bojan, V.M. An internet of things based intelligent transportation system. In Proceedings of the 2014 IEEE international conference on vehicular electronics and safety. IEEE, 2014, pp. 174–179.
10. Kassab, M.; DeFranco, J.; Laplante, P. A systematic literature review on internet of things in education: Benefits and challenges. *Journal of computer Assisted learning* **2020**, *36*, 115–127.
11. Hossein Motlagh, N.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the energy sector. *Energies* **2020**, *13*, 494.
12. Vishnu, S.; Ramson, S.J.; Jegan, R. Internet of medical things (IoMT)-An overview. In Proceedings of the 2020 5th international conference on devices, circuits and systems (ICDCS). IEEE, 2020, pp. 101–104.
13. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet of Things Journal* **2020**, *8*, 8707–8718.
14. Al-Turjman, F.; Nawaz, M.H.; Ulusar, U.D. Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. *Computer Communications* **2020**, *150*, 644–660.
15. Wei, K.; Zhang, L.; Guo, Y.; Jiang, X. Health monitoring based on internet of medical things: architecture, enabling technologies, and applications. *IEEE Access* **2020**, *8*, 27468–27478.
16. Wu, Q.; Tang, P.; Yang, M. Data processing platform design and algorithm research of wearable sports physiological parameters detection based on medical internet of things. *Measurement* **2020**, *165*, 108172.
17. Yadav, N.; Keshtkar, F.; Schweikert, C.; Crocetti, G. Cradle: An IOMT psychophysiological analytics platform. In Proceedings of the Proceedings of the Workshop on Human-Habitat for Health (H3): Human-Habitat Multimodal Interaction for Promoting Health and Well-Being in the Internet of Things Era, 2018, pp. 1–7.
18. Kumar, N.; Kaushal, R.K.; Panda, S.N. IoT based smart and portable system for remote patient monitoring and drug delivery. In Proceedings of the Journal of Physics: Conference Series. IOP Publishing, 2021, Vol. 1950, p. 012017.
19. Yew, H.T.; Ng, M.F.; Ping, S.Z.; Chung, S.K.; Chekima, A.; Dargham, J.A. Iot based real-time remote patient monitoring system. In Proceedings of the 2020 16th IEEE international colloquium on signal processing & its applications (CSPA). IEEE, 2020, pp. 176–179.
20. Lu, Y.; Da Xu, L. Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal* **2018**, *6*, 2103–2115.

 doi:10.20944/preprints202402.0898.v1

21. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Communications Surveys & Tutorials* **2018**, *20*, 3453–3495.
22. Kaur, B.; Dadkhah, S.; Shoeleh, F.; Neto, E.C.P.; Xiong, P.; Iqbal, S.; Lamontagne, P.; Ray, S.; Ghorbani, A.A. Internet of Things (IoT) security dataset evolution: Challenges and future directions. *Internet of Things* **2023**, p. 100780.
23. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials* **2019**, *21*, 2702–2733.
24. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials* **2019**, *22*, 616–644.
25. Booth, H.; Rike, D.; Witte, G.A. The national vulnerability database (nvd): Overview **2013**.
26. Danso, P.K.; Dadkhah, S.; Neto, E.C.P.; Zohourian, A.; Molyneaux, H.; Lu, R.; Ghorbani, A.A. Transferability of Machine Learning Algorithm for IoT Device Profiling and Identification. *IEEE Internet of Things Journal* **2023**.
27. Hassan, W.H.; et al. Current research on Internet of Things (IoT) security: A survey. *Computer networks* **2019**, *148*, 283–294.
28. Neto, E.C.P.; Dadkhah, S.; Ferreira, R.; Zohourian, A.; Lu, R.; Ghorbani, A.A. CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment **2023**.
29. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT communications: A survey. *Sensors* **2020**, *20*, 4828.
30. Sivanathan, A.; Gharakheili, H.H.; Sivaraman, V. Managing IoT cyber-security using programmable telemetry and machine learning. *IEEE Transactions on Network and Service Management* **2020**, *17*, 60–74.
31. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials* **2020**, *22*, 1646–1685.
32. Suresh, M.; Anitha, R. Evaluating machine learning algorithms for detecting DDoS attacks. In Proceedings of the Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011 4. Springer, 2011, pp. 441–452.
33. Zekri, M.; El Kafhali, S.; Aboutabit, N.; Saadi, Y. DDoS attack detection using machine learning techniques in cloud computing environments. In Proceedings of the 2017 3rd international conference of cloud computing technologies and applications (CloudTech). IEEE, 2017, pp. 1–7.
34. Tavana, M.; Ozger, M.; Baltaci, A.; Schleicher, B.; Schupke, D.; Cavdar, C. Wireless power transfer for aircraft IoT applications: System design and measurements. *IEEE Internet of Things Journal* **2021**, *8*, 11834–11846.
35. Neto, E.C.P.; Dadkhah, S.; Sadeghi, S.; Molyneaux, H.; Ghorbani, A.A. A review of Machine Learning (ML)-based IoT security in healthcare: A dataset perspective. *Computer Communications* **2023**.
36. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *Journal of oral biology and craniofacial research* **2022**, *12*, 302–318.
37. Mbengue, S.M.; Diallo, O.; El Hadji, M.N.; Rodrigues, J.J.; Neto, A.; Al-Muhtadi, J. Internet of medical things: Remote diagnosis and monitoring application for diabetics. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2020, pp. 583–588.
38. Subramaniam, E.V.D.; Srinivasan, K.; Qaisar, S.M.; Pławiak, P. Interoperable IoMT Approach for Remote Diagnosis with Privacy-Preservation Perspective in Edge Systems. *Sensors* **2023**, *23*, 7474.
39. Joshi, S.; Joshi, S. A sensor based secured health monitoring and alert technique using iomt. In Proceedings of the 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT). IEEE, 2019, pp. 152–156.
40. Khan, M.A.; Algarni, F. A healthcare monitoring system for the diagnosis of heart disease in the IoMT cloud environment using MSSO-ANFIS. *IEEE Access* **2020**, *8*, 122259–122269.
41. Rachakonda, L.; Mohanty, S.P.; Kougianos, E. cStick: a calm stick for fall prediction, detection and control in the IoMT framework. In Proceedings of the IFIP International Internet of Things Conference. Springer, 2021, pp. 129–145.

 doi:10.20944/preprints202402.0898.v1

42. Gupta, A.; Srivastava, R.; Gupta, H.; Kumar, B. IoT based fall detection monitoring and alarm system for elderly. In Proceedings of the 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON). IEEE, 2020, pp. 1–5.
43. Arora, S. IoMT (Internet of Medical Things): Reducing cost while improving patient care. *IEEE pulse* **2020**, *11*, 24–27.
44. Karagiannis, D.; Mitsis, K.; Nikita, K.S. Development of a Low-Power IoMT Portable Pillbox for Medication Adherence Improvement and Remote Treatment Adjustment. *Sensors* **2022**, *22*, 5818.
45. Villanueva-Miranda, I.; Nazeran, H.; Martinek, R. A semantic interoperability approach to heterogeneous internet of medical things (IoMT) platforms. In Proceedings of the 2018 IEEE 20th international conference on e-Health networking, applications and services (HealthCom). IEEE, 2018, pp. 1–5.
46. Kavitha, D.; Subramaniam, C. Security threat management by software obfuscation for privacy in internet of medical thing (IoMT) application. *Journal of Computational and Theoretical Nanoscience* **2017**, *14*, 3100–3114.
47. Piché, M.E.; Tchernof, A.; Després, J.P. Obesity phenotypes, diabetes, and cardiovascular diseases. *Circulation research* **2020**, *126*, 1477–1500.
48. Halson, S.L. Sleep monitoring in athletes: motivation, methods, miscalculations and why it matters. *Sports medicine* **2019**, *49*, 1487–1497.
49. Wang, J.; Chen, M.; Chen, Q.; Wang, H. Medical Oxygen Sensor Based on Acoustic Resonance Frequency Tracking Using FPGA. *IEEE Sensors Journal* **2022**, *22*, 21281–21286.
50. Kotronis, C.; Routis, I.; Politi, E.; Nikolaidou, M.; Dimitrakopoulos, G.; Anagnostopoulos, D.; Amira, A.; Bensaali, F.; Djelouat, H. Evaluating Internet of Medical Things (IoMT)-based systems from a human-centric perspective. *Internet of Things* **2019**, *8*, 100125.
51. Razdan, S.; Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE technical review* **2022**, *39*, 775–788.
52. Zhong, W.; Ji, Z.; Sun, C. A review of monitoring methods for cerebral blood oxygen saturation. In Proceedings of the Healthcare. MDPI, 2021, Vol. 9, p. 1104.
53. Wilson, F.P.; Martin, M.; Yamamoto, Y.; Partridge, C.; Moreira, E.; Arora, T.; Biswas, A.; Feldman, H.; Garg, A.X.; Greenberg, J.H.; et al. Electronic health record alerts for acute kidney injury: multicenter, randomized clinical trial. *Bmj* **2021**, *372*.
54. Hu, R.; Michel, B.; Russo, D.; Mora, N.; Matrella, G.; Ciampolini, P.; Cocchi, F.; Montanari, E.; Nunziata, S.; Brunschwiler, T. An unsupervised behavioral modeling and alerting system based on passive sensing for elderly care. *Future Internet* **2021**, *13*, 6.
55. Khan, M.M.; Mehnaz, S.; Shaha, A.; Nayem, M.; Bourouis, S.; et al. IoT-based smart health monitoring system for COVID-19 patients. *Computational and Mathematical Methods in Medicine* **2021**, *2021*.
56. Hashim, N.; Norddin, N.; Idris, F.; Yusoff, S.; Zahari, M. IoT blood pressure monitoring system. *Indonesian Journal of Electrical Engineering and Computer Science* **2020**, *19*, 1384–1390.
57. Chalmers, T.; Hickey, B.A.; Newton, P.; Lin, C.T.; Sibbritt, D.; McLachlan, C.S.; Clifton-Bligh, R.; Morley, J.; Lal, S. Stress watch: The use of heart rate and heart rate variability to detect stress: A pilot study using smart watch wearables. *Sensors* **2021**, *22*, 151.
58. Romano, C.; Schena, E.; Formica, D.; Massaroni, C. Comparison between chest-worn accelerometer and gyroscope performance for heart rate and respiratory rate monitoring. *Biosensors* **2022**, *12*, 834.
59. Dian, F.J.; Vahidnia, R.; Rahmati, A. Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey. *IEEE access* **2020**, *8*, 69200–69211.
60. Arquilla, K.; Webb, A.K.; Anderson, A.P. Textile electrocardiogram (ECG) electrodes for wearable health monitoring. *Sensors* **2020**, *20*, 1013.
61. Serhani, M.A.; T. El Kassabi, H.; Ismail, H.; Nujum Navaz, A. ECG monitoring systems: Review, architecture, processes, and key challenges. *Sensors* **2020**, *20*, 1796.
62. Brice, J.H.; Cyr, J.M.; Hnat, A.T.; Wei, T.L.; Principe, S.; Thead, S.E.; Delbridge, T.R.; Winslow, J.E.; Studnek, J.R.; Fernandez, A.R.; et al. Assessment of key health and wellness indicators among North Carolina emergency medical service providers. *Prehospital Emergency Care* **2019**, *23*, 179–186.
63. Khan, M.F.; Ghazal, T.M.; Said, R.A.; Fatima, A.; Abbas, S.; Khan, M.; Issa, G.F.; Ahmad, M.; Khan, M.A.; et al. An iomt-enabled smart healthcare model to monitor elderly people using machine learning technique. *Computational Intelligence and Neuroscience* **2021**, *2021*.

 doi:10.20944/preprints202402.0898.v1

64. Chamberlain, S.D.; Singh, I.; Ariza, C.; Daitch, A.; Philips, P.; Dalziel, B.D. Real-time detection of COVID-19 epicenters within the United States using a network of smart thermometers. *MedRxiv* **2020**, pp. 2020–04.
65. Chandrasekaran, R.; Katthula, V.; Moustakas, E. Patterns of use and key predictors for the use of wearable health care devices by US adults: insights from a national survey. *Journal of medical Internet research* **2020**, *22*, e22443.
66. Wu, M.; Luo, J. Wearable technology applications in healthcare: a literature review. *Online J. Nurs. Inform* **2019**, *23*.
67. Walker, R.C.; Tong, A.; Howard, K.; Palmer, S.C. Patient expectations and experiences of remote monitoring for chronic diseases: systematic review and thematic synthesis of qualitative studies. *International journal of medical informatics* **2019**, *124*, 78–85.
68. Fang, M.; Wang, D.; Coresh, J.; Selvin, E. Trends in diabetes treatment and control in US adults, 1999–2018. *New England Journal of Medicine* **2021**, *384*, 2219–2228.
69. Lamonaca, F.; Carnì, D.L.; Spagnuolo, V.; Grimaldi, G.; Bonavolontà, F.; Liccardo, A.; Moriello, R.S.L.; Colaprico, A. A new measurement system to boost the IoMT for the blood pressure monitoring. In Proceedings of the 2019 IEEE International Symposium on Measurements & Networking (M&N). IEEE, 2019, pp. 1–6.
70. Alarcón-Paredes, A.; Francisco-García, V.; Guzmán-Guzmán, I.P.; Cantillo-Negrete, J.; Cuevas-Valencia, R.E.; Alonso-Silverio, G.A. An IoT-based non-invasive glucose level monitoring system using raspberry pi. *Applied Sciences* **2019**, *9*, 3046.
71. Yang, Y.; Yang, M.; Shen, C.; Wang, F.; Yuan, J.; Li, J.; Zhang, M.; Wang, Z.; Xing, L.; Wei, J.; et al. Evaluating the accuracy of different respiratory specimens in the laboratory diagnosis and monitoring the viral shedding of 2019-nCoV infections. *MedRxiv* **2020**, pp. 2020–02.
72. Nicolò, A.; Massaroni, C.; Schena, E.; Sacchetti, M. The importance of respiratory rate monitoring: From healthcare to sport and exercise. *Sensors* **2020**, *20*, 6396.
73. Reshiwaran, A.; Jegatheswaran, L.; Sakira, I.J.; Abd Rahman, N.A. A Review on IoMT device Vulnerabilities and Countermeasures. In Proceedings of the Journal of Physics: Conference Series. IOP Publishing, 2020, Vol. 1712, p. 012020.
74. Sui, S.X.; Williams, L.J.; Holloway-Kew, K.L.; Hyde, N.K.; Pasco, J.A. Skeletal muscle health and cognitive function: a narrative review. *International journal of molecular sciences* **2020**, *22*, 255.
75. Alam, M.G.R.; Abedin, S.F.; Moon, S.I.; Talukder, A.; Hong, C.S. Healthcare IoT-based affective state mining using a deep convolutional neural network. *IEEE Access* **2019**, *7*, 75189–75202.
76. Warmerdam, E.; Hausdorff, J.M.; Atrsaei, A.; Zhou, Y.; Mirelman, A.; Aminian, K.; Espay, A.J.; Hansen, C.; Evers, L.J.; Keller, A.; et al. Long-term unsupervised mobility assessment in movement disorders. *The Lancet Neurology* **2020**, *19*, 462–470.
77. Hong, Z.; Hong, M.; Wang, N.; Ma, Y.; Zhou, X.; Wang, W. A wearable-based posture recognition system with AI-assisted approach for healthcare IoT. *Future Generation Computer Systems* **2022**, *127*, 286–296.
78. Mozaffari, N.; Rezazadeh, J.; Farahbakhsh, R.; Yazdani, S.; Sandrasegaran, K. Practical fall detection based on IoT technologies: A survey. *Internet of things* **2019**, *8*, 100124.
79. Anwary, A.R.; Cetinkaya, D.; Vassallo, M.; Bouchachia, H.; et al. Smart-Cover: A real time sitting posture monitoring system. *Sensors and Actuators A: Physical* **2021**, *317*, 112451.
80. Talal, M.; Zaidan, A.; Zaidan, B.; Albahri, A.S.; Alamoodi, A.H.; Albahri, O.S.; Alsalem, M.; Lim, C.K.; Tan, K.L.; Shir, W.; et al. Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of medical systems* **2019**, *43*, 1–34.
81. Kretchy, I.A.; Asiedu-Danso, M.; Kretchy, J.P. Medication management and adherence during the COVID-19 pandemic: perspectives and experiences from low-and middle-income countries. *Research in social and administrative pharmacy* **2021**, *17*, 2023–2026.
82. Taylor, M.A.; Jones, R. Risk of medication errors with infusion pumps: a study of 1,004 events from 132 hospitals across pennsylvania. *Patient Safety* **2019**, *1*, 60–69.
83. Sharma, R.; Singh, D.; Gaur, P.; Joshi, D. Intelligent automated drug administration and therapy: Future of healthcare. *Drug Delivery and Translational Research* **2021**, pp. 1–25.
84. Bhuiyan, M.N.; Rahman, M.M.; Billah, M.M.; Saha, D. Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal* **2021**, *8*, 10474–10498.

85. Singh, D.; Sandhu, A.; Thakur, A.; Priyank, N. An overview of IoT hardware development platforms. *Int. J. Emerg. Technol* **2020**, *11*, 155–163.
86. Capra, M.; Peloso, R.; Masera, G.; Ruo Roch, M.; Martina, M. Edge computing: A survey on the hardware requirements in the internet of things world. *Future Internet* **2019**, *11*, 100.
87. Hady, A.A.; Ghubaish, A.; Salman, T.; Unal, D.; Jain, R. Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access* **2020**, *8*, 106576–106584.
88. Ahmed, M.; Byreddy, S.; Nutakki, A.; Sikos, L.F.; Haskell-Dowland, P. ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things. *Ad Hoc Networks* **2021**, *122*, 102621.
89. Zubair, M.; Ghubaish, A.; Unal, D.; Al-Ali, A.; Reimann, T.; Alinier, G.; Hammoudeh, M.; Qadir, J. Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System. *Sensors* **2022**, *22*, 8280.
90. Hussain, F.; Abbas, S.G.; Shah, G.A.; Pires, I.M.; Fayyaz, U.U.; Shahzad, F.; Garcia, N.M.; Zdravevski, E. A framework for malicious traffic detection in IoT healthcare environment. *Sensors* **2021**, *21*, 3025.
91. Radoglou-Grammatikis, P.; Rompolos, K.; Sarigiannidis, P.; Argyriou, V.; Lagkas, T.; Sarigiannidis, A.; Goudos, S.; Wan, S. Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach. *IEEE Transactions on Industrial Informatics* **2021**, *18*, 2041–2052.
92. Anthi, E.; Williams, L.; Słowińska, M.; Theodorakopoulos, G.; Burnap, P. A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal* **2019**, *6*, 9042–9053.
93. Mirsky, Y.; Doitshman, T.; Elovici, Y.; Shabtai, A. Kitsune: an ensemble of autoencoders for online network intrusion detection. *arXiv preprint arXiv:1802.09089* **2018**.
94. Guerra-Manzanares, A.; Medina-Galindo, J.; Bahsi, H.; Nõmm, S. MedBIoT: Generation of an IoT Botnet Dataset in a Medium-sized IoT Network. In Proceedings of the ICISSP, 2020, pp. 207–218.
95. Parmisano, A.; Garcia, S.; Erquiaga, M. A Labeled Dataset with Malicious and Benign IoT Network Traffic. *Stratosphere Laboratory: Praha, Czech Republic* **2020**.
96. Ullah, I.; Mahmoud, Q.H. A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In Proceedings of the Canadian Conference on Artificial Intelligence, 2020, pp. 508–520.
97. Vaccari, I.; Chiola, G.; Aiello, M.; Mongelli, M.; Cambiaso, E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT. *Sensors* **2020**, *20*, 6578.
98. Hindy, H.; Bayne, E.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Bellekens, X. Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study. *arXiv preprint arXiv:2006.15340* **2020**.
99. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven Intrusion Detection Systems. *IEEE Access* **2020**, *8*, 165130–165150.
100. Dadkhah, S.; Mahdikhani, H.; Danso, P.K.; Zohourian, A.; Truong, K.A.; Ghorbani, A.A. Towards the development of a realistic multidimensional IoT profiling dataset. In Proceedings of the 2022 19th Annual International Conference on Privacy, Security & Trust (PST). IEEE, 2022, pp. 1–11.
101. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE communications surveys & tutorials* **2016**, *18*, 2027–2051.
102. Alhijawi, B.; Almajali, S.; Elgala, H.; Salameh, H.B.; Ayyash, M. A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. *Computers and Electrical Engineering* **2022**, *99*, 107706.
103. Vishwakarma, R.; Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems* **2020**, *73*, 3–25.
104. Uma, M.; Padmavathi, G. A survey on various cyber attacks and their classification. *Int. J. Netw. Secur.* **2013**, *15*, 390–396.
105. Mazurczyk, W.; Caviglione, L. Cyber reconnaissance techniques. *Communications of the ACM* **2021**, *64*, 86–95.
106. Alatram, A.; Sikos, L.F.; Johnstone, M.; Szewczyk, P.; Kang, J.J. DoS/DDoS-MQTT-IoT: A dataset for evaluating intrusions in IoT networks using the MQTT protocol. *Computer Networks* **2023**, *231*, 109809.
107. Vaccari, I.; Aiello, M.; Cambiaso, E. SlowITe, a novel denial of service attack affecting MQTT. *Sensors* **2020**, *20*, 2932.
108. TCPDUMP. Tcpdump(1) man page. *https://www.tcpdump.org/manpages/tcpdump.1.html* **2023**.
109. DPKT. Dpkt documentation. *https://dpkt.readthedocs.io/en/latest/* **2023**.
110. PANDAS. pandas-dev/pandas: Pandas **2020**. https://doi.org/10.5281/zenodo.3509134.

111. Bapat, R.; Mandya, A.; Liu, X.; Abraham, B.; Brown, D.E.; Kang, H.; Veeraraghavan, M. Identifying malicious botnet traffic using logistic regression. In Proceedings of the 2018 systems and information engineering design symposium (SIEDS). IEEE, 2018, pp. 266–271.
112. AlShahrani, B.M.M.; et al. Classification of cyber-attack using Adaboost regression classifier and securing the network. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* **2021**, *12*, 1215–1223.
113. Rehman Javed, A.; Jalil, Z.; Atif Moqurrab, S.; Abbas, S.; Liu, X. Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles. *Transactions on Emerging Telecommunications Technologies* **2022**, *33*, e4088.
114. Khan, F.; Ahamed, J.; Kadry, S.; Ramasamy, L.K. Detecting malicious URLs using binary classification through ada boost algorithm. *International Journal of Electrical & Computer Engineering (2088-8708)* **2020**, *10*.
115. Choubisa, M.; Doshi, R.; Khatri, N.; Hiran, K.K. A simple and robust approach of random forest for intrusion detection system in cyber security. In Proceedings of the 2022 International Conference on IoT and Blockchain Technology (ICIBT). IEEE, 2022, pp. 1–5.
116. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. *Ieee access* **2018**, *6*, 35365–35381.
117. Danso, P.K.; Neto, E.C.P.; Dadkhah, S.; Zohourian, A.; Molyneaux, H.; Ghorbani, A.A. Ensemble-based Intrusion Detection for Internet of Things Devices. In Proceedings of the 2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET). IEEE, 2022, pp. 034–039.