Research article

CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT

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

Canadian Institute for Cybersecurity - University of New Brunswick (UNB), Fredericton, New Brunswick, Canada

ARTICLE INFO

ABSTRACT

The Internet of Things (IoT) is increasingly integrated into daily life, particularly in healthcare, through the Internet of Medical Things (IoMT). IoMT devices support services like continuous health monitoring but raise significant cybersecurity concerns due to their vulnerability to various attacks. The complexity and data volume of IoMT network traffic requires advanced methods to enhance security and reliability. Machine Learning (ML) offers techniques to detect, prevent, and mitigate cyberattacks. However, existing benchmark datasets lack essential features for robust IoMT security solutions, such as a reduced number of real devices, a limited variety of attacks, and a lack of extensive profiling. We propose a realistic benchmark dataset for IoMT security solutions development and evaluation to address these gaps. We executed 18 attacks on an IoMT testbed with 40 devices (25 real and 15 simulated), using protocols like Wi-Fi, MQTT, and Bluetooth. Supporting technologies, including dedicated network traffic collectors and a Faraday Cage, ensured data quality. The attacks fall into five categories: DDoS, DoS, Recon, MQTT, and spoofing. We aim to establish a baseline that complements existing datasets, aiding researchers in creating secure healthcare systems using ML. Beyond simulating attacks, we capture the lifecycle of IoMT devices from network entry to exit through profiling, allowing classifiers to identify device anomalies. The resulting CICIoMT2024 dataset, published on the CIC dataset page, demonstrates that various methods can classify IoMT cyberattacks. This effort supports new IoMT security solutions and contributes to the broader field of cybersecurity in healthcare, ensuring more reliable IoMT device deployment.

1. Introduction

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]. 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 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 context, 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. In IoT, devices are diverse and present 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 defenses 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. 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. In the context of IoMT, the primary security concerns comprise Confidentiality, Integrity, and Availability (CIA) of safety–critical applications. In fact, the security aspects of IoMT device integration concern healthcare professionals due to the substantial impacts of malicious activities. This emphasizes the need for advanced solutions to identify complex and underlying patterns beyond traditional methods, paving the way for the use of Machine Learning (ML).

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]. Alongside 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.

Nowadays, acquiring IoMT devices is expensive and requires installation, configuration, and maintenance regularly. This obstacle prevents datasets from monitoring the behavior of various real devices, downscaling the data size and evaluation scenarios. Furthermore, IoMT devices are assembled for different purposes, which represents special constraints for cyberattacks. In this sense, the reduced number of devices affects the cyberattacks that can be launched, including the operation of different protocols and their respective weaknesses (e.g., specialized flooding attacks). Finally, the complexity of understanding IoMT devices' behavior from the networking standpoint is emphasized by the limited device variety. A comprehensive testbed enables the collection of profiles at scale and further enables IoMT security solutions.

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 motivation of this research and the proposed method relies on the limitations of existing datasets and networking data processing pipelines in the context of medical security. The CICIoMT2024 brings a novel processing pipeline that enables data processing for multiple protocols. This effort extends the collection of malicious traffic in home automation scenarios [28] to healthcare settings, adopting new devices, topology, protocols, and malicious behaviors. The main contributions of this research are:

- **Development of a Comprehensive IoMT Security Dataset:** We introduce the CICIoMT2024 dataset as an advanced effort to build a realistic and multi-protocol benchmark for the Internet of Medical Things (IoMT) security. 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 novel 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.
- **Profiling IoMT Device Lifecycle for Enhanced Security Understanding:** This research captures the lifecycle of these devices in different vital phases of a device from the moment they join the network until they leave. As mobility in healthcare organizations is considered a regular practice, profiling the lifecycle while encompassing various operational phases (e.g., 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: Section 3 presents related works and highlights the main aspects of this research. Secondly, Section 2 introduces the main aspects of IoMT applications in healthcare. Section 4 introduces the CICIoMT2024 dataset and explains the phases involved in the data collection. Section 5 depicts 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 describes 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 Fig. 1. These applications include sleep and oxygen monitoring in different areas of patient care, heart rate and cardiovascular monitoring for cardiologic applications, and chronic condition management. Respiratory function evaluation is another important area of application alongside muscle activity, neurological function, and patient safety. Finally, IoMT plays a critical role in medication management, wellness tracking, and alert systems.

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
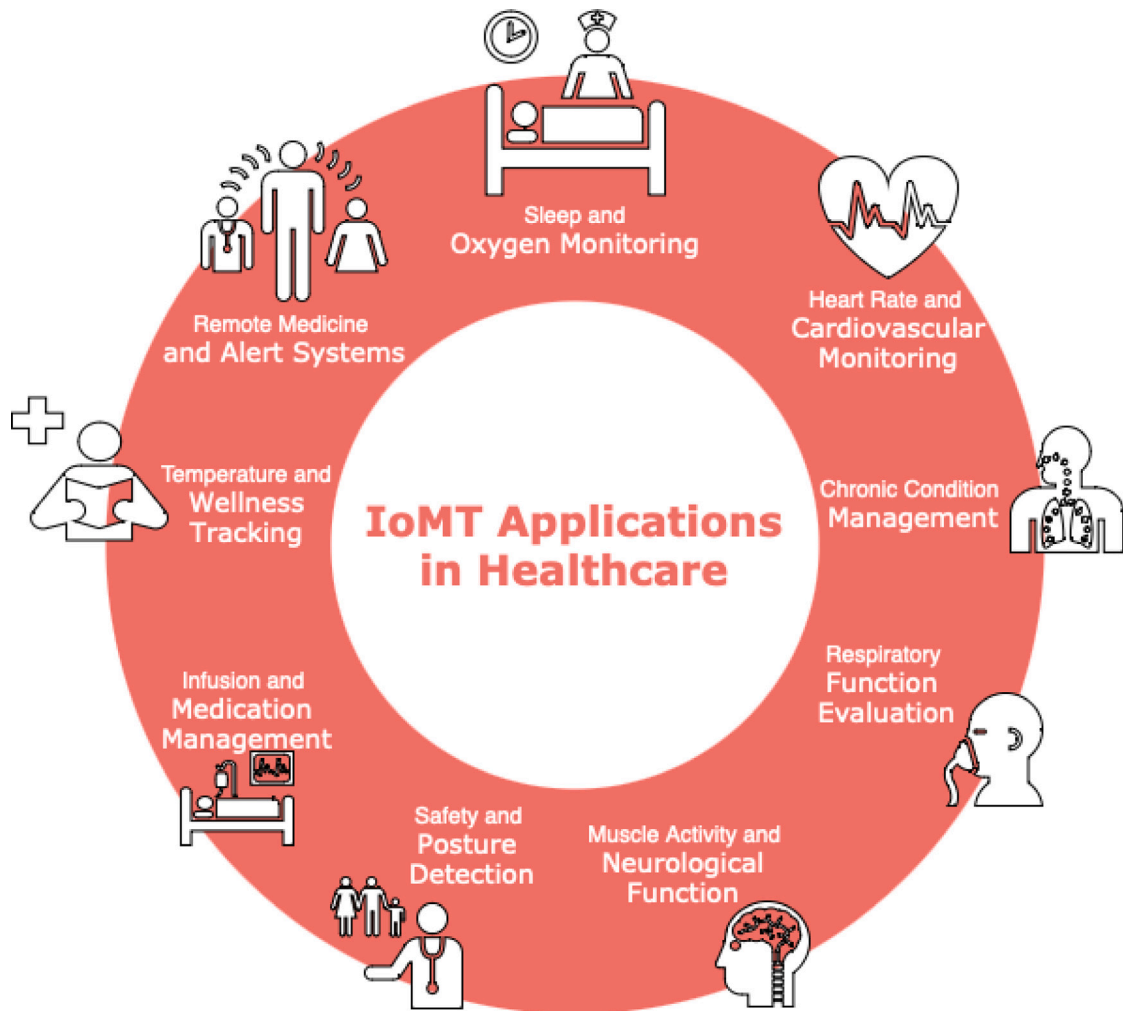
Fig. 1. Applications of IoMT in healthcare.

need support [41,42]. 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]. Furthermore, 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].

Such technologies can continuously observe chronic conditions, 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 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 datasets 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 evaluation setup comprised 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 behavior 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 Laptop). Concerning the attacks launched, the authors focus on scaling, ARP spoofing, 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).

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 terms of topology, these works rely on real and simulated devices and vary in testbed size. For example, ICU presents more IoMT variety than other datasets. Regarding attacks, most efforts present a limited range of attack types and categories. Although all of them are focused on healthcare

Table 1
Recent healthcare datasets in IoT domain.

	Year	Devices	Attacks	Healthcare	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	✓	✓	✓

and IoT devices, they do not consider IoMT profiling and, in many cases, a reduced set of communication protocols. 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.

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 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 [97,98]

Fig. 2. CIC IoT lab.

introduce the MQTT datasets. The researchers in [99,100], and [28] propose IoT datasets comprising more extensive testbeds and experiments.

Finally, the research gaps highlight the need for a comprehensive effort toward an extensive and realistic IoMT security benchmark dataset. The data supply from various devices will extend existing analytics capabilities including privacy-preserving methods [101]. Besides, the plurality of devices and attacks addresses the incomplete data samples used in modern approaches by including attacks against different protocols [101]. Finally, the lack of profiling samples prevents the evaluation of healthcare-specific networking workflows and behavior [102]. Hence, the CICIoMT2024 builds upon the state-of-the-art efforts by addressing existing shortcomings through adopting an extensive testbed, evaluating multiple protocols used in healthcare applications, and collecting behavioral aspects to generate IoMT profiles.

4. The proposedCICIoMT2024

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. 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.

Fig. 2 illustrated the CIC IoT lab. The photos illustrate several IoMT and supporting devices to enable the execution of attacks and data collection. It includes computers, networking devices, cables, and actual IoMT sensors and actuators. 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 labeled to streamline management and identification.

4.2. IoMT topology

The CICIoMT2024 comprises the use of several devices and multiple purposes. Fig. 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. Also, devices are separated based on the protocol used to enable protocol-specific attacks to be executed and captured.

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.
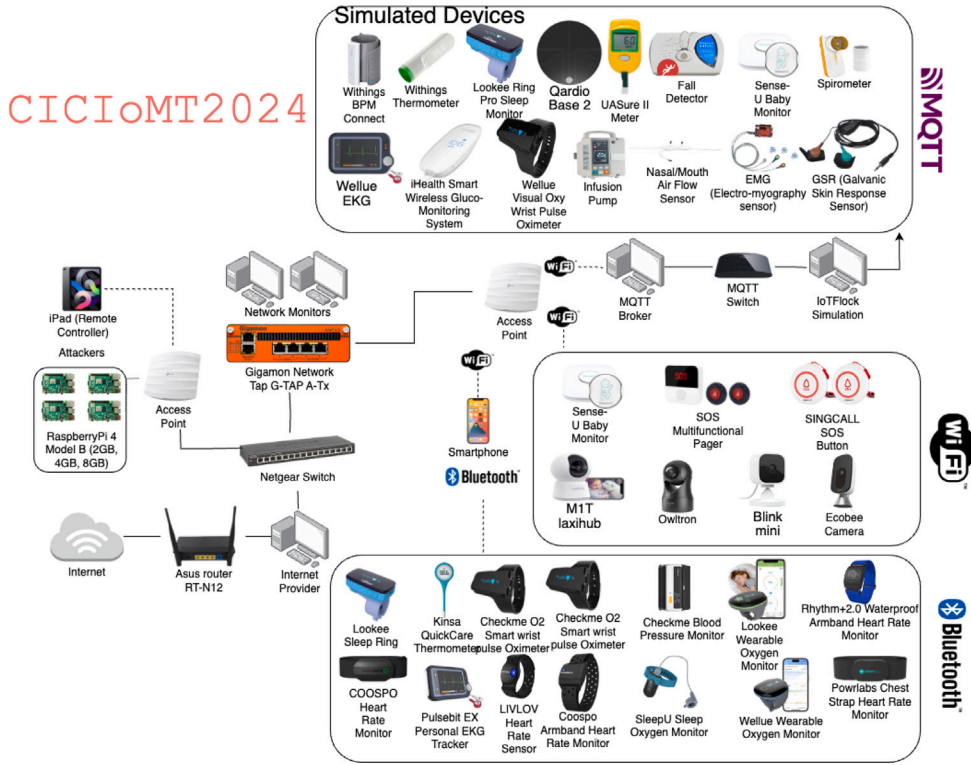
Fig. 3. CICIoMT2024 topology.

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.

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 protocols of critical importance for healthcare applications [35], popular attacks that threaten CIA constraints in IoT operations, and 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.

Multiple attacks were executed against Wi-Fi devices. ARP spoofing was carried out to perform Man-in-the-middle attacks [103]. Concerning Dos and DDoS [104,105], we executed several flooding campaigns, namely ICMP Flood, SYN Flood, TCP Flood, and UDP Flood. Finally, reconnaissance attacks were also conducted [106,107], 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

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

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 focussing on flooding the MQTT broker with various connect request packets to establish new connections [108]. To accomplish this, a custom Python script was developed to conduct Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. Second, MQTT Publish Floods were also conducted based on using publish packets under random topics in DoS and DDoS formats. Finally, the MQTT Malformed Data attack was executed. This attack uses the MQTTSA tool [109] 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 "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 Fig. 4, the Bluetooth experiments were executed inside of a Faraday Cage 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. The assessment of IoMT profiles enhances the capabilities of classifiers to detect anomalies in healthcare operations by defining the expected benign networking behavior. In classification tasks, unseen patterns might indicate malicious activities and zero-day attacks. To enable the development of such methods, we describe how the generation and collection of profiling data were conducted for different experiments.

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

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 min. The device is later powered off, and capture is allowed to continue for another 3 min 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 behaviors were captured when connecting to the smartphone.

4.4.2. Idle experiments

The idle experiments are carried out in a span of two 13-h 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 h. 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 h. 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. Fig. 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.

First, the attacks are conducted and the raw network traffic is stored in PCAP files. Five categories of attack are executed (i.e., DDoS, DoS, Recon, MQTT, and spoofing), selected based on their popularity and level of impact presented in real-world healthcare scenarios. 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. This phase represents the collection of the actual network traffic in an IoMT environment and reveals how each device reacts to malicious activities. Regardless of the analysis researchers aim to conduct, these files store all relevant features in an optimized format.

Second, we divide the collected traffic into two groups: (i) train and (ii) test. The "train" group is intended 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. Based on this separation, researchers develop new defensive solutions and easily compare their results with other initiatives by adopting a unified evaluation configuration.

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 Fig. 6. First, TCPDUMP [110] 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 since serial converters require a long time to execute. Then, for each PCAP chunk, DPKT [111] 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 [112] and available for researchers in a labeled format.

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 [113], Adaboost [114–116], Random Forest [117], and Deep Neural Network [118]. The evaluation is focussed on three tasks: Binary classification (i.e., Benign 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 [119]:

- **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:

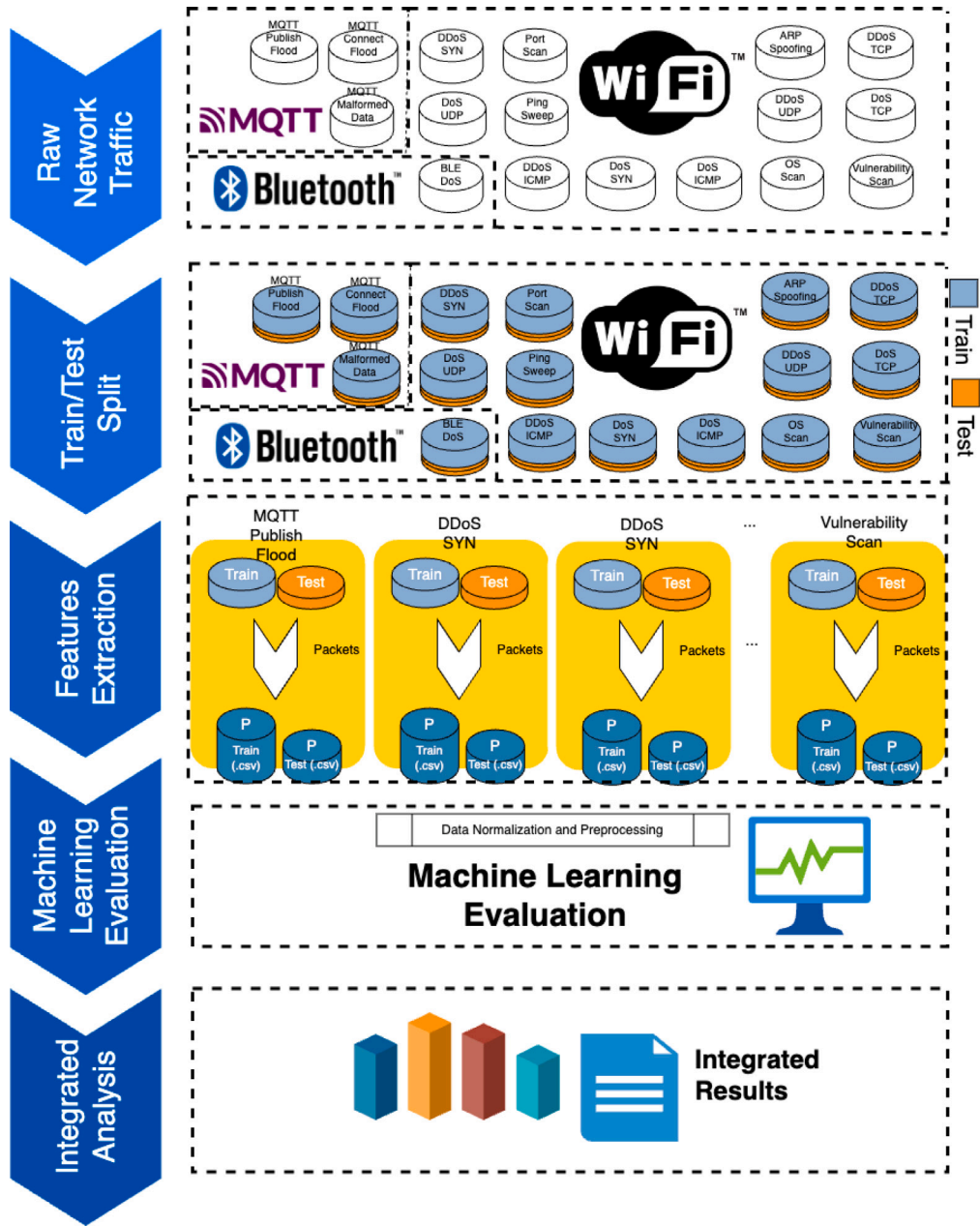$$F1 = 2 \times \frac{Pre \times Rec}{Pre + Rec} \tag{4}$$

Fig. 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.
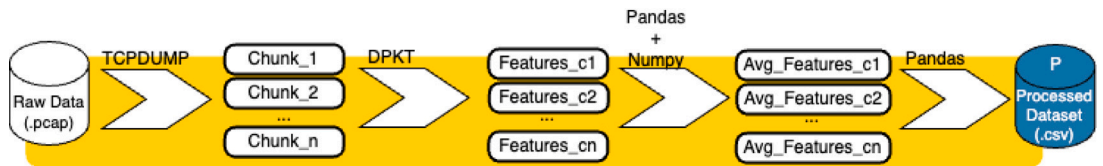

Fig. 6. Process of converting PCAP files to CSV files.

Table 5
Features extracted from PCAP files [28].

#	Feature	Description
1	Header Length	Mean of the Header Lengths of the Transport Layer
2	Time-To-Live	Time-To-Live
3	Rate	Speed of packet transmission within a window packets/s
4	fin flag number	Proportion of packets with FIN flags in the window
5	syn flag number:	Proportion of packets with SYN flags in the window
6	rst flag number	Proportion of packets with RST flags in the window
7	psh flag number	Proportion of packets with PSH flags in the window
8	ack flag number	Proportion of packets with ACK flags in the window
9	ece flag number	Proportion of packets with ECE flags in the window
10	cwr flag number	Proportion of packets with Cwr flags in the window
11	syn count	Count of Syn flag occurrences in packets
12	ack count	Count of Ack flag occurrences in packets
13	fin count	Count of Fin flag occurrences in packets
14	rst count	Count of Rst flag occurrences in packets
15	IGMP	Average no. of IGMP in the window
16	HTTPS	Average no. of HTTPS in the window
17	HTTP	Average no. of HTTP packets in the window
18	Telnet	Average no. of Telnet packets in the window
19	DNS	Average no. of DNS packets in the window
20	SMTP	Average no. of SMTP packets in the window
21	SSH	Average no. of SSH packets in the window
22	IRC	Average no. of IRC packets in the window
23	TCP	Average no. of TCP packets in the window
24	UDP	Average no. of UDP packets in the window
25	DHCP	Average no. of DHCP packets in the window
26	ARP	Average no. of ARP packets in the window
27	ICMP	Average no. of ICMP packets in the window
28	IPv	Average no. of IPv packets in the window
29	LLC	Average no. of LLC packets in the window
30	Tot Sum	Total Packet Length within the aggregated packets (window)
31	Min	Shortest packet length among the aggregated packets (window)
32	Max	Longest packet length among the aggregated packets (window)
33	AVG	Mean of the packet length among the aggregated packets (window)
34	Std	Standard deviation of the packet length from the aggregated packets (window)
35	Tot Size	(Avg.) Length of the packet
36	IAT	Interval mean between the current and previous packet in the window
37	Number	Total number of packets in the window
38	Variance	Variance of the packet lengths in the window
39	Protocol Type	Mode of the protocols found in the window

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 represents a comprehensive list that represents several aspects of the network traffic, this selection can be easily increased by recurring to the original PCAP files.

Nevertheless, Figs. 7 and 8 illustrate 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, Fig. 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 6 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).

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., including all classes available). Fig. 9 illustrates the experiments' results regarding accuracy, recall, precision, and F1-score.
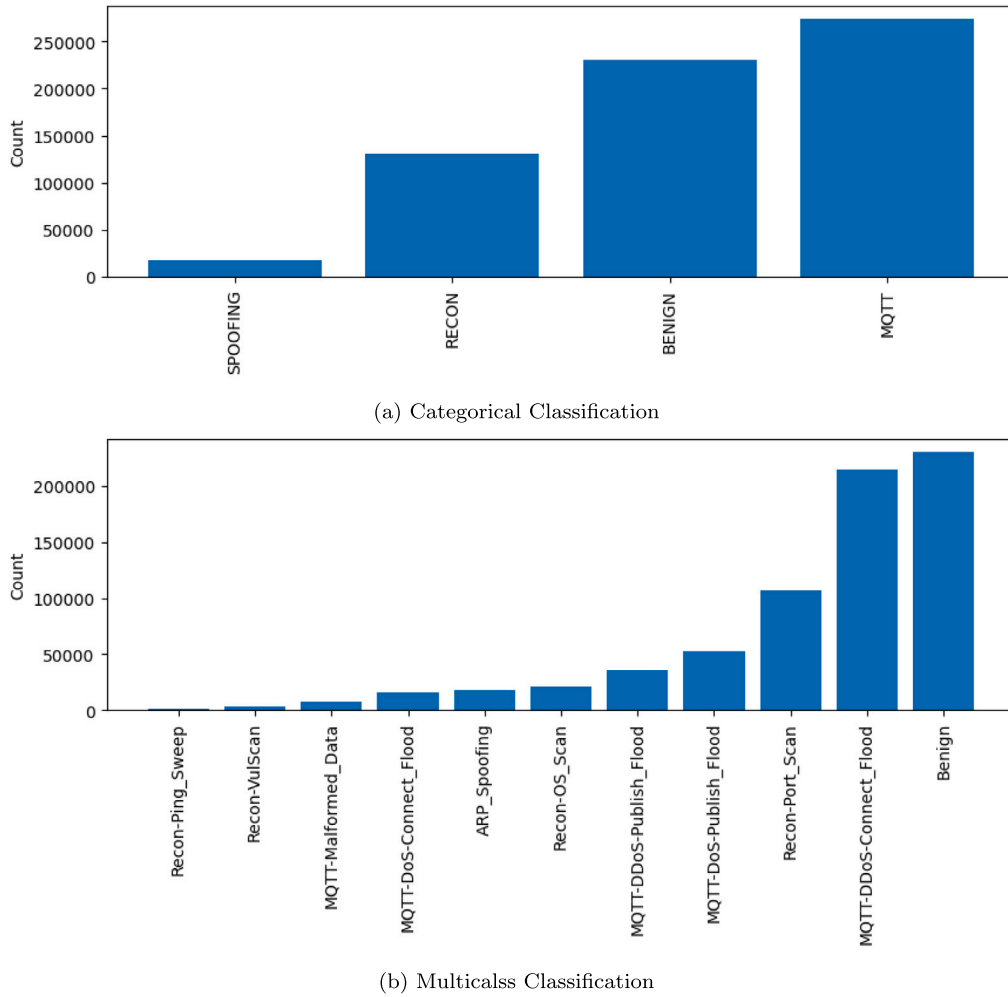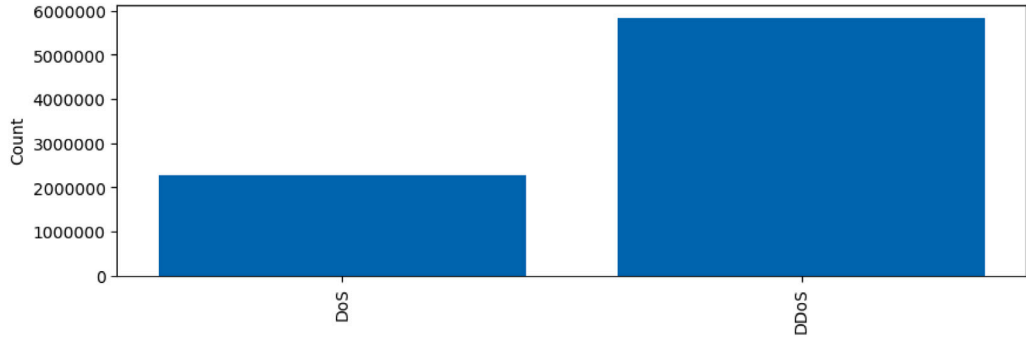
(a) Categorical Classification

(b) Multicalss Classification

Fig. 7. Class distribution in (a) Categorical, and (b) Multiclass classification.

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 close to 1. 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 0.72 and 0.73, respectively.
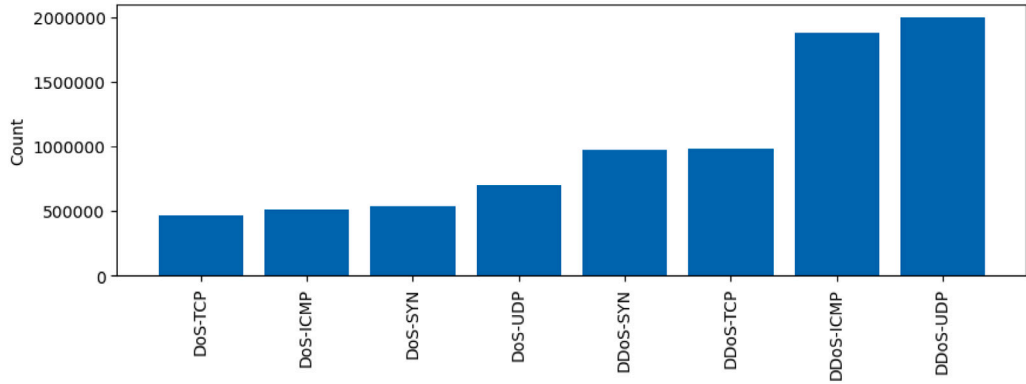
To understand the results presented, Table 8 lists the parameters adopted by each ML technique. Also, Table 7 presents the numerical results obtained in each experiment. Although the overall outcomes are similar across the four techniques, RF outperformed all other models in most cases. Conversely, all models struggle to classify specific attacks rather than their general category. This highlights the need for future investigations in the development of advanced models to improve classification performance.

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. 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.

These experiments demonstrate that the CICIoMT2024 dataset enables ML algorithms to detect attacks against IoMT operations. Conversely, the evaluation presented in this research is limited to applying standard and lightweight models, enabling researchers to design complex architectures specialized in IoMT to improve the overall performance. Also, organizations are constantly producing

(a) Categorical Classification

(b) Multicalss Classification

Fig. 8. Class distribution in (a) Categorical, and (b) Multiclass classification for DoS and DDoS.

Table 6
Number of instances in each class of the CICIoMT2024 dataset.

Class	Category	Attack	Count
BENIGN	–	–	230 339
ATTACK	SPOOFING	ARP spoofing	17 791
	RECON	Ping sweep	926
		Recon VulScan	3207
		OS scan	20 666
		Port scan	106 603
	MQTT	Malformed data	6877
		DoS connect flood	15 904
		DDoS publish flood	36 039
		DoS publish flood	52 881
		DDoS connect flood	214 952
	DoS	DoS TCP	462 480
		DoS ICMP	514 724
		DoS SYN	540 498
		DoS UDP	704 503
	DDoS	DDoS SYN	974 359
		DDoS TCP	987 063
		DDoS ICMP	1 887 175
		DDoS UDP	1 998 026

Table 7

Numerical results obtained by each ML technique.

		LogisticRegression	AdaBoost	DeepNeuralNetwork	RandomForest
2 classes	Accuracy	0.995	**0.996**	**0.996**	**0.996**
	Recall	0.94	**0.961**	0.948	0.951
	Precision	0.952	0.959	0.956	**0.971**
	F1-Score	0.946	0.959	0.952	**0.961**
6 classes	Accuracy	0.729	0.437	0.734	**0.735**
	Recall	0.712	0.506	0.693	**0.713**
	Precision	**0.748**	0.587	0.725	0.735
	F1-Score	**0.694**	0.501	0.665	0.676
19 classes	Accuracy	0.727	0.422	0.729	**0.733**
	Recall	0.471	0.238	0.553	**0.577**
	Precision	0.547	0.144	0.649	**0.691**
	F1-Score	0.432	0.141	0.522	**0.551**

Table 8

Parameters adopted by ML techniques.

Model	Parameters
Random Forest (RF)	n_estimators=100, criterion='gini', min_samples_split=2, min_samples_leaf=1, min_weight_fraction_leaf=0.0, max_features='sqrt', min_impurity_decrease=0.0, bootstrap=True, oob_score=False, warm_start=False, ccp_alpha=0.0
AdaBoost (AB)	estimator=DecisionTreeClassifier, n_estimators=50, learning_rate=1.0, algorithm='SAMME.R'
Logistic Regression (LR)	penalty='l2', dual=False, tol=0.0001, C=1.0, fit_intercept=True, intercept_scaling=1, solver='lbfgs', max_iter=100, warm_start=False
Deep Neural Network (DNN)	hidden_layer_sizes=(32,32,32), solver='adam', alpha=0.0001, batch_size='auto', learning_rate='constant', learning_rate_init=0.001, power_t=0.5, max_iter=200, shuffle=True, tol=0.0001, warm_start=False, momentum=0.9, nesterovs_momentum=True, early_stopping=False, validation_fraction=0.1, beta_1=0.9, beta_2=0.999, epsilon=1e−08, n_iter_no_change=10, max_fun=15000

new medical devices and the CICIoMT2024 dataset only adopts devices currently in use, i.e., future works can include the analysis of devices not currently available on the market.

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. Three protocols were targeted considering the characteristics of healthcare operations (i.e., Wi-Fi, MQTT, and Bluetooth). The primary 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.

From the theoretical standpoint, this research empowers new IDS concepts and supports the specialization of traditional detection pipelines for IoMT operations. On the practical side, the implications of this investigation shed light on how healthcare providers can deploy security countermeasures to ensure confidentiality, integrity, and availability of medical service. This paper introduced a comprehensive IoMT security dataset and a novel method for attack simulation and data collection while observing profiling experiments. A detailed 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.

The CICIoMT2024 addresses important issues of state-of-the-art approaches in many ways. First, the plurality and diversity of IoMT devices adopted is unique and the data collected are more extensive than existing efforts. Besides, the attacks executed comprise a comprehensive list of popular threats, including attacks not covered by other efforts. Finally, IoMT profiling is a pillar among the contributions of this research and is not provided by similar datasets. This research builds upon state-of-the-art efforts by addressing existing shortcomings through adopting an extensive testbed, evaluating multiple protocols used in healthcare applications, and collecting behavioral aspects to generate IoMT profiles.
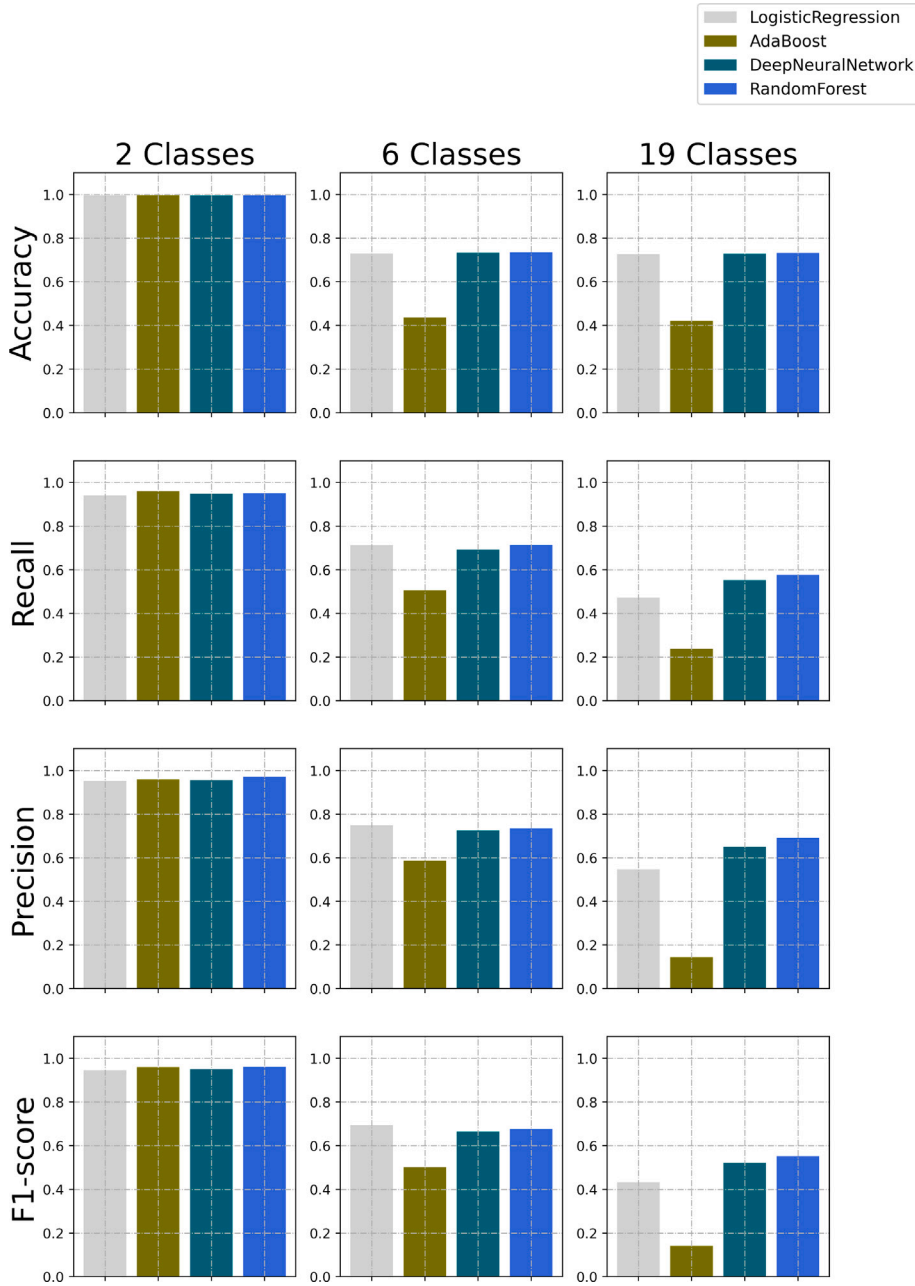
Fig. 9. Results obtained in the experiments regarding accuracy, recall, precision, and F1-score. These experiments comprise the classification of IoMT attacks in multiple scenarios (2, 6, and 19 classes).

Conversely, this proposal presents limitations that can be addressed in future works. For example, the evaluation process is limited to applying standard and lightweight models, while researchers can further design complex architectures to enhance the overall performance. The devices adopted herein refer to up-to-date technologies, which are likely to change in the next decade.

There are several possible future directions for future works. Major areas of investigation include the combination of domain features and cybersecurity features. Although network anomalies can reveal the presence of malicious activities, integrating domain features in the detection process can further improve the performance of ML models and establish a better understanding of security principles in healthcare. Also, another major obstacle for future proposals relies on deployability. The CICIoMT2024 dataset enables a realistic evaluation of detection mechanisms. However, there are aspects beyond the context of this research to consider for real-world deployments, e.g., real-time evaluation, efficiency, and zero-day attacks. The hyperparameter optimization of ML models represents a third direction, 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). Our proposal contributes to the research community and unveils immediate research directions in the context of IoMT security.

CRediT authorship contribution statement

Sajjad Dadkhah: Writing – review & editing, Writing – original draft, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Euclides Carlos Pinto Neto:** Writing – original draft, Visualization, Resources, Formal analysis, Data curation. **Raphael Ferreira:** Validation, Investigation, Data curation, Conceptualization. **Reginald Chukwuka Molokwu:** Validation, Methodology, Formal analysis, Data curation. **Ali A. Ghorbani:** Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The dataset is available on the CIC dataset page https://www.unb.ca/cic/datasets/iomt-dataset-2024.html.

References

[1] S. Madakam, V. Lake, V. Lake, V. Lake, et al., Internet of things (IoT): A literature review, J. Comput. Commun. 3 (05) (2015) 164.
[2] M.U. Farooq, M. Waseem, S. Mazhar, A. Khairi, T. Kamal, A review on internet of things (IoT), Int. J. Comput. Appl. 113 (1) (2015) 1–7.
[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[4] A. Mukherjee, A. Pal, P. Misra, Data analytics in ubiquitous sensor-based health information systems, in: 2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies, IEEE, 2012, pp. 193–198.
[5] B. Yuan, J. Herbert, A cloud-based mobile data analytics framework: case study of activity recognition using smartphone, in: 2014 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, IEEE, 2014, pp. 220–227.
[6] S.W. Loke, Supporting ubiquitous sensor-cloudlets and context-cloudlets: Programming compositions of context-aware systems for mobile users, Future Gener. Comput. Syst. 28 (4) (2012) 619–632.
[7] C.-W. Hsu, C.-C. Yeh, Understanding the factors affecting the adoption of the internet of things, Technol. Anal. Strateg. Manage. 29 (9) (2017) 1089–1102.
[8] F.J. Riggins, S.F. Wamba, Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics, in: 2015 48th Hawaii International Conference on System Sciences, IEEE, 2015, pp. 1531–1540.
[9] T.M. Bojan, U.R. Kumar, V.M. Bojan, An internet of things based intelligent transportation system, in: 2014 IEEE International Conference on Vehicular Electronics and Safety, IEEE, 2014, pp. 174–179.
[10] M. Kassab, J. DeFranco, P. Laplante, A systematic literature review on internet of things in education: Benefits and challenges, J. Comput. Assist. Learn. 36 (2) (2020) 115–127.
[11] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, B. Zakeri, Internet of things (IoT) and the energy sector, Energies 13 (2) (2020) 494.
[12] S. Vishnu, S.J. Ramson, R. Jegan, Internet of medical things (IoMT)-an overview, in: 2020 5th International Conference on Devices, Circuits and Systems, ICDCS, IEEE, 2020, pp. 101–104.
[13] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, Recent advances in the internet-of-medical-things (IoMT) systems security, IEEE Internet Things J. 8 (11) (2020) 8707–8718.
[14] F. Al-Turjman, M.H. Nawaz, U.D. Ulusar, Intelligence in the internet of medical things era: A systematic review of current and future trends, Comput. Commun. 150 (2020) 644–660.
[15] K. Wei, L. Zhang, Y. Guo, X. Jiang, Health monitoring based on internet of medical things: architecture, enabling technologies, and applications, IEEE Access 8 (2020) 27468–27478.
[16] Q. Wu, P. Tang, M. Yang, Data processing platform design and algorithm research of wearable sports physiological parameters detection based on medical internet of things, Measurement 165 (2020) 108172.
[17] N. Yadav, F. Keshtkar, C. Schweikert, G. Crocetti, Cradle: An IOMT psychophysiological analytics platform, in: 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] N. Kumar, R.K. Kaushal, S.N. Panda, IoT based smart and portable system for remote patient monitoring and drug delivery, in: Journal of Physics: Conference Series, Vol. 1950, IOP Publishing, 2021, 012017.
[19] H.T. Yew, M.F. Ng, S.Z. Ping, S.K. Chung, A. Chekima, J.A. Dargham, Iot based real-time remote patient monitoring system, in: 2020 16th IEEE International Colloquium on Signal Processing & Its Applications, CSPA, IEEE, 2020, pp. 176–179.
[20] Y. Lu, L. Da Xu, Internet of things (IoT) cybersecurity research: A review of current research topics, IEEE Internet Things J. 6 (2) (2018) 2103–2115.
[21] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, J. Lopez, A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3453–3495.
[22] B. Kaur, S. Dadkhah, F. Shoeleh, E.C.P. Neto, P. Xiong, S. Iqbal, P. Lamontagne, S. Ray, A.A. Ghorbani, Internet of things (IoT) security dataset evolution: Challenges and future directions, Internet Things (2023) 100780.
[23] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2702–2733.
[24] I. Butun, P. Österberg, H. Song, Security of the internet of things: Vulnerabilities, attacks, and countermeasures, IEEE Commun. Surv. Tutor. 22 (1) (2019) 616–644.
[25] H. Booth, D. Rike, G.A. Witte, The national vulnerability database (nvd): Overview, 2013.

[26] P.K. Danso, S. Dadkhah, E.C.P. Neto, A. Zohourian, H. Molyneaux, R. Lu, A.A. Ghorbani, Transferability of machine learning algorithm for IoT device profiling and identification, IEEE Internet Things J. (2023).

[27] W.H. Hassan, et al., Current research on internet of things (IoT) security: A survey, Comput. Netw. 148 (2019) 283–294.

[28] E.C.P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, A.A. Ghorbani, CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment, 2023.

[29] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, C. Douligeris, Security in IoMT communications: A survey, Sensors 20 (17) (2020) 4828.

[30] A. Sivanathan, H.H. Gharakheili, V. Sivaraman, Managing IoT cyber-security using programmable telemetry and machine learning, IEEE Trans. Netw. Serv. Manag. 17 (1) (2020) 60–74.

[31] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for internet of things (IoT) security, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1646–1685.

[32] M. Suresh, R. Anitha, Evaluating machine learning algorithms for detecting ddos attacks, in: Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011 4, Springer, 2011, pp. 441–452.

[33] M. Zekri, S. El Kafhali, N. Aboutabit, Y. Saadi, DDoS attack detection using machine learning techniques in cloud computing environments, in: 2017 3rd International Conference of Cloud Computing Technologies and Applications, CloudTech, IEEE, 2017, pp. 1–7.

[34] M. Tavana, M. Ozger, A. Baltaci, B. Schleicher, D. Schupke, C. Cavdar, Wireless power transfer for aircraft IoT applications: System design and measurements, IEEE Internet Things J. 8 (15) (2021) 11834–11846.

[35] E.C.P. Neto, S. Dadkhah, S. Sadeghi, H. Molyneaux, A.A. Ghorbani, A review of machine learning (ML)-based IoT security in healthcare: A dataset perspective, Comput. Commun. (2023).

[36] R. Dwivedi, D. Mehrotra, S. Chandra, Potential of internet of medical things (IoMT) applications in building a smart healthcare system: A systematic review, J. Oral Biol. Craniofac. Res. 12 (2) (2022) 302–318.

[37] S.M. Mbengue, O. Diallo, M.N. El Hadji, J.J. Rodrigues, A. Neto, J. Al-Muhtadi, Internet of medical things: Remote diagnosis and monitoring application for diabetics, in: 2020 International Wireless Communications and Mobile Computing, IWCMC, IEEE, 2020, pp. 583–588.

[38] E.V.D. Subramaniam, K. Srinivasan, S.M. Qaisar, P. Pławiak, Interoperable IoMT approach for remote diagnosis with privacy-preservation perspective in edge systems, Sensors 23 (17) (2023) 7474.

[39] S. Joshi, S. Joshi, A sensor based secured health monitoring and alert technique using iomt, in: 2019 2nd International Conference on Intelligent Communication and Computational Techniques, ICCT, IEEE, 2019, pp. 152–156.

[40] M.A. Khan, F. Algarni, A healthcare monitoring system for the diagnosis of heart disease in the IoMT cloud environment using MSSO-ANFIS, IEEE Access 8 (2020) 122259–122269.

[41] L. Rachakonda, S.P. Mohanty, E. Kougianos, cStick: a calm stick for fall prediction, detection and control in the IoMT framework, in: IFIP International Internet of Things Conference, Springer, 2021, pp. 129–145.

[42] A. Gupta, R. Srivastava, H. Gupta, B. Kumar, IoT based fall detection monitoring and alarm system for elderly, in: 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering, UPCON, IEEE, 2020, pp. 1–5.

[43] S. Arora, IoMT (Internet of Medical Things): Reducing cost while improving patient care, IEEE Pulse 11 (5) (2020) 24–27.

[44] D. Karagiannis, K. Mitsis, K.S. Nikita, Development of a low-power IoMT portable pillbox for medication adherence improvement and remote treatment adjustment, Sensors 22 (15) (2022) 5818.

[45] I. Villanueva-Miranda, H. Nazeran, R. Martinek, A semantic interoperability approach to heterogeneous internet of medical things (IoMT) platforms, in: 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services, HealthCom, IEEE, 2018, pp. 1–5.

[46] D. Kavitha, C. Subramaniam, Security threat management by software obfuscation for privacy in internet of medical thing (IoMT) application, J. Comput. Theor. Nanosci. 14 (7) (2017) 3100–3114.

[47] M.-E. Piché, A. Tchernof, J.-P. Després, Obesity phenotypes, diabetes, and cardiovascular diseases, Circ. Res. 126 (11) (2020) 1477–1500.

[48] S.L. Halson, Sleep monitoring in athletes: motivation, methods, miscalculations and why it matters, Sports Med. 49 (10) (2019) 1487–1497.

[49] J. Wang, M. Chen, Q. Chen, H. Wang, Medical oxygen sensor based on acoustic resonance frequency tracking using FPGA, IEEE Sens. J. 22 (21) (2022) 21281–21286.

[50] C. Kotronis, I. Routis, E. Politi, M. Nikolaidou, G. Dimitrakopoulos, D. Anagnostopoulos, A. Amira, F. Bensaali, H. Djelouat, Evaluating internet of medical things (IoMT)-based systems from a human-centric perspective, Internet Things 8 (2019) 100125.

[51] S. Razdan, S. Sharma, Internet of medical things (IoMT): Overview, emerging technologies, and case studies, IETE Tech. Rev. 39 (4) (2022) 775–788.

[52] W. Zhong, Z. Ji, C. Sun, A review of monitoring methods for cerebral blood oxygen saturation, in: Healthcare, Vol. 9, MDPI, 2021, p. 1104.

[53] F.P. Wilson, M. Martin, Y. Yamamoto, C. Partridge, E. Moreira, T. Arora, A. Biswas, H. Feldman, A.X. Garg, J.H. Greenberg, et al., Electronic health record alerts for acute kidney injury: multicenter, randomized clinical trial, BMJ 372 (2021).

[54] R. Hu, B. Michel, D. Russo, N. Mora, G. Matrella, P. Ciampolini, F. Cocchi, E. Montanari, S. Nunziata, T. Brunschwiler, An unsupervised behavioral modeling and alerting system based on passive sensing for elderly care, Future Internet 13 (1) (2021) 6.

[55] M.M. Khan, S. Mehnaz, A. Shaha, M. Nayem, S. Bourouis, et al., IoT-based smart health monitoring system for COVID-19 patients, Comput. Math. Methods Med. 2021 (2021).

[56] N. Hashim, N. Norddin, F. Idris, S. Yusoff, M. Zahari, IoT blood pressure monitoring system, Indones. J. Electr. Eng. Comput. Sci. 19 (3) (2020) 1384–1390.

[57] T. Chalmers, B.A. Hickey, P. Newton, C.-T. Lin, D. Sibbritt, C.S. McLachlan, R. Clifton-Bligh, J. Morley, S. Lal, Stress watch: The use of heart rate and heart rate variability to detect stress: A pilot study using smart watch wearables, Sensors 22 (1) (2021) 151.

[58] C. Romano, E. Schena, D. Formica, C. Massaroni, Comparison between chest-worn accelerometer and gyroscope performance for heart rate and respiratory rate monitoring, Biosensors 12 (10) (2022) 834.

[59] F.J. Dian, R. Vahidnia, A. Rahmati, Wearables and the internet of things (IoT), applications, opportunities, and challenges: A survey, IEEE Access 8 (2020) 69200–69211.

[60] K. Arquilla, A.K. Webb, A.P. Anderson, Textile electrocardiogram (ECG) electrodes for wearable health monitoring, Sensors 20 (4) (2020) 1013.

[61] M.A. Serhani, H. T. El Kassabi, H. Ismail, A. Nujum Navaz, ECG monitoring systems: Review, architecture, processes, and key challenges, Sensors 20 (6) (2020) 1796.

[62] J.H. Brice, J.M. Cyr, A.T. Hnat, T.L. Wei, S. Principe, S.E. Thead, T.R. Delbridge, J.E. Winslow, J.R. Studnek, A.R. Fernandez, et al., Assessment of key health and wellness indicators among north carolina emergency medical service providers, Prehospital Emerg. Care 23 (2) (2019) 179–186.

[63] M.F. Khan, T.M. Ghazal, R.A. Said, A. Fatima, S. Abbas, M. Khan, G.F. Issa, M. Ahmad, M.A. Khan, et al., An iomt-enabled smart healthcare model to monitor elderly people using machine learning technique, Comput. Intell. Neurosci. 2021 (2021).

[64] S.D. Chamberlain, I. Singh, C. Ariza, A. Daitch, P. Philips, B.D. Dalziel, Real-time detection of COVID-19 epicenters within the United States using a network of smart thermometers, 2020, MedRxiv 2020-2004.

[65] R. Chandrasekaran, V. Katthula, E. Moustakas, Patterns of use and key predictors for the use of wearable health care devices by US adults: insights from a national survey, J. Med. Internet Res. 22 (10) (2020) e22443.

[66] M. Wu, J. Luo, Wearable technology applications in healthcare: a literature review, Online J. Nurs. Inform. 23 (3) (2019).

[67] R.C. Walker, A. Tong, K. Howard, S.C. Palmer, Patient expectations and experiences of remote monitoring for chronic diseases: systematic review and thematic synthesis of qualitative studies, Int. J. Med. Inform. 124 (2019) 78–85.

[68] M. Fang, D. Wang, J. Coresh, E. Selvin, Trends in diabetes treatment and control in US adults, 1999–2018, New Engl. J. Med. 384 (23) (2021) 2219–2228.
[69] F. Lamonaca, D.L. Carnì, V. Spagnuolo, G. Grimaldi, F. Bonavolontà, A. Liccardo, R.S.L. Moriello, A. Colaprico, A new measurement system to boost the IoMT for the blood pressure monitoring, in: 2019 IEEE International Symposium on Measurements & Networking, M&N, IEEE, 2019, pp. 1–6.
[70] A. Alarcón-Paredes, V. Francisco-García, I.P. Guzmán-Guzmán, J. Cantillo-Negrete, R.E. Cuevas-Valencia, G.A. Alonso-Silverio, An IoT-based non-invasive glucose level monitoring system using raspberry pi, Appl. Sci. 9 (15) (2019) 3046.
[71] Y. Yang, M. Yang, C. Shen, F. Wang, J. Yuan, J. Li, M. Zhang, Z. Wang, L. Xing, J. Wei, et al., Evaluating the accuracy of different respiratory specimens in the laboratory diagnosis and monitoring the viral shedding of 2019-nCoV infections, 2020, MedRxiv 2020-2002.
[72] A. Nicolò, C. Massaroni, E. Schena, M. Sacchetti, The importance of respiratory rate monitoring: From healthcare to sport and exercise, Sensors 20 (21) (2020) 6396.
[73] A. Reshiwaran, L. Jegatheswaran, I.J. Sakira, N.A. Abd Rahman, A review on IoMT device vulnerabilities and countermeasures, in: Journal of Physics: Conference Series, Vol. 1712, IOP Publishing, 2020, 012020.
[74] S.X. Sui, L.J. Williams, K.L. Holloway-Kew, N.K. Hyde, J.A. Pasco, Skeletal muscle health and cognitive function: a narrative review, Int. J. Mol. Sci. 22 (1) (2020) 255.
[75] M.G.R. Alam, S.F. Abedin, S.I. Moon, A. Talukder, C.S. Hong, Healthcare IoT-based affective state mining using a deep convolutional neural network, IEEE Access 7 (2019) 75189–75202.
[76] E. Warmerdam, J.M. Hausdorff, A. Atrsaei, Y. Zhou, A. Mirelman, K. Aminian, A.J. Espay, C. Hansen, L.J. Evers, A. Keller, et al., Long-term unsupervised mobility assessment in movement disorders, Lancet Neurol. 19 (5) (2020) 462–470.
[77] Z. Hong, M. Hong, N. Wang, Y. Ma, X. Zhou, W. Wang, A wearable-based posture recognition system with AI-assisted approach for healthcare IoT, Future Gener. Comput. Syst. 127 (2022) 286–296.
[78] N. Mozaffari, J. Rezazadeh, R. Farahbakhsh, S. Yazdani, K. Sandrasegaran, Practical fall detection based on IoT technologies: A survey, Internet Things 8 (2019) 100124.
[79] A.R. Anwary, D. Cetinkaya, M. Vassallo, H. Bouchachia, et al., Smart-cover: A real time sitting posture monitoring system, Sensors Actuators A 317 (2021) 112451.
[80] M. Talal, A. Zaidan, B. Zaidan, A.S. Albahri, A.H. Alamoodi, O.S. Albahri, M. Alsalem, C.K. Lim, K.L. Tan, W. Shir, 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, J. Med. Syst. 43 (2019) 1–34.
[81] I.A. Kretchy, M. Asiedu-Danso, J.-P. Kretchy, Medication management and adherence during the COVID-19 pandemic: perspectives and experiences from low-and middle-income countries, Res. Soc. Admin. Pharm. 17 (1) (2021) 2023–2026.
[82] M.A. Taylor, R. Jones, Risk of medication errors with infusion pumps: a study of 1,004 events from 132 hospitals across Pennsylvania, Patient Saf. 1 (2) (2019) 60–69.
[83] R. Sharma, D. Singh, P. Gaur, D. Joshi, Intelligent automated drug administration and therapy: Future of healthcare, Drug Deliv. Transl. Res. (2021) 1–25.
[84] M.N. Bhuiyan, M.M. Rahman, M.M. Billah, D. Saha, Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities, IEEE Internet Things J. 8 (13) (2021) 10474–10498.
[85] D. Singh, A. Sandhu, A. Thakur, N. Priyank, An overview of IoT hardware development platforms, Int. J. Emerg. Technol. 11 (2020) 155–163.
[86] M. Capra, R. Peloso, G. Masera, M. Ruo Roch, M. Martina, Edge computing: A survey on the hardware requirements in the internet of things world, Future Internet 11 (4) (2019) 100.
[87] A.A. Hady, A. Ghubaish, T. Salman, D. Unal, R. Jain, Intrusion detection system for healthcare systems using medical and network data: A comparison study, IEEE Access 8 (2020) 106576–106584.
[88] M. Ahmed, S. Byreddy, A. Nutakki, L.F. Sikos, P. Haskell-Dowland, ECU-IoHT: A dataset for analyzing cyberattacks in internet of health things, Ad Hoc Netw. 122 (2021) 102621.
[89] M. Zubair, A. Ghubaish, D. Unal, A. Al-Ali, T. Reimann, G. Alinier, M. Hammoudeh, J. Qadir, Secure bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system, Sensors 22 (21) (2022) 8280.
[90] F. Hussain, S.G. Abbas, G.A. Shah, I.M. Pires, U.U. Fayyaz, F. Shahzad, N.M. Garcia, E. Zdravevski, A framework for malicious traffic detection in IoT healthcare environment, Sensors 21 (9) (2021) 3025.
[91] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos, S. Wan, Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach, IEEE Trans. Ind. Inform. 18 (3) (2021) 2041–2052.
[92] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, P. Burnap, A supervised intrusion detection system for smart home IoT devices, IEEE Internet Things J. 6 (5) (2019) 9042–9053.
[93] Y. Mirsky, T. Doitshman, Y. Elovici, A. Shabtai, Kitsune: an ensemble of autoencoders for online network intrusion detection, 2018, arXiv preprint arXiv:1802.09089.
[94] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, S. Nõmm, MedBIoT: Generation of an IoT botnet dataset in a medium-sized IoT network, in: ICISSP, 2020, pp. 207–218.
[95] A. Parmisano, S. Garcia, M. Erquiaga, A Labeled Dataset with Malicious and Benign IoT Network Traffic, Stratosphere Laboratory, Praha, Czech Republic, 2020.
[96] I. Ullah, Q.H. Mahmoud, A scheme for generating a dataset for anomalous activity detection in IoT networks, in: Canadian Conference on Artificial Intelligence, 2020, pp. 508–520.
[97] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, E. Cambiaso, MQTTset, a new dataset for machine learning techniques on MQTT, Sensors 20 (22) (2020) 6578.
[98] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, X. Bellekens, Machine learning based IoT intrusion detection system: An MQTT case study, 2020, arXiv preprint arXiv:2006.15340.
[99] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, A. Anwar, TON_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven intrusion detection systems, IEEE Access 8 (2020) 165130–165150.
[100] S. Dadkhah, H. Mahdikhani, P.K. Danso, A. Zohourian, K.A. Truong, A.A. Ghorbani, Towards the development of a realistic multidimensional IoT profiling dataset, in: 2022 19th Annual International Conference on Privacy, Security & Trust, PST, IEEE, 2022, pp. 1–11.
[101] M.A. Mohammed, A. Lakhan, D.A. Zebari, M.K. Abd Ghani, H.A. Marhoon, K.H. Abdulkareem, J. Nedoma, R. Martinek, Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology, Eng. Appl. Artif. Intell. 129 (2024) 107612.
[102] A. Lakhan, M.A. Mohammed, K.H. Abdulkareem, M. khanapi Abd Ghani, H.A. Marhoon, J. Nedoma, R. Martinek, B. Garcia-Zapirain, Secure blockchain assisted internet of medical things architecture for data fusion enabled cancer workflow, Internet Things 24 (2023) 100928.
[103] M. Conti, N. Dragoni, V. Lesyk, A survey of man in the middle attacks, IEEE Commun. Surv. Tutorials 18 (3) (2016) 2027–2051.
[104] B. Alhijawi, S. Almajali, H. Elgala, H.B. Salameh, M. Ayyash, A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets, Comput. Electr. Eng. 99 (2022) 107706.
[105] R. Vishwakarma, A.K. Jain, A survey of DDoS attacking techniques and defence mechanisms in the IoT network, Telecommun. Syst. 73 (1) (2020) 3–25.

[106] M. Uma, G. Padmavathi, A survey on various cyber attacks and their classification, Int. J. Netw. Secur. 15 (5) (2013) 390–396.

[107] W. Mazurczyk, L. Caviglione, Cyber reconnaissance techniques, Commun. ACM 64 (3) (2021) 86–95.

[108] A. Alatram, L.F. Sikos, M. Johnstone, P. Szewczyk, J.J. Kang, DoS/DDoS-MQTT-IoT: A dataset for evaluating intrusions in IoT networks using the MQTT protocol, Comput. Netw. 231 (2023) 109809.

[109] I. Vaccari, M. Aiello, E. Cambiaso, SlowITe, a novel denial of service attack affecting MQTT, Sensors 20 (10) (2020) 2932.

[110] TCPDUMP, Tcpdump(1) man page, 2023, https://www.tcpdump.org/manpages/tcpdump.1.html.

[111] DPKT, Dpkt documentation, 2023, https://dpkt.readthedocs.io/en/latest/.

[112] PANDAS, pandas-dev/pandas: Pandas, 2020, http://dx.doi.org/10.5281/zenodo.3509134.

[113] R. Bapat, A. Mandya, X. Liu, B. Abraham, D.E. Brown, H. Kang, M. Veeraraghavan, Identifying malicious botnet traffic using logistic regression, in: 2018 Systems and Information Engineering Design Symposium, SIEDS, IEEE, 2018, pp. 266–271.

[114] B.M.M. AlShahrani, et al., Classification of cyber-attack using adaboost regression classifier and securing the network, Turk J Comput Math Educ (TURCOMAT) 12 (10) (2021) 1215–1223.

[115] A. Rehman Javed, Z. Jalil, S. Atif Moqurrab, S. Abbas, X. Liu, Ensemble adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles, Trans. Emerg. Telecommun. Technol. 33 (10) (2022) e4088.

[116] F. Khan, J. Ahamed, S. Kadry, L.K. Ramasamy, Detecting malicious URLs using binary classification through ada boost algorithm, Int J Electr Comput Eng (2088-8708) 10 (1) (2020).

[117] M. Choubisa, R. Doshi, N. Khatri, K.K. Hiran, A simple and robust approach of random forest for intrusion detection system in cyber security, in: 2022 International Conference on IoT and Blockchain Technology, ICIBT, IEEE, 2022, pp. 1–5.

[118] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, C. Wang, Machine learning and deep learning methods for cybersecurity, IEEE Access 6 (2018) 35365–35381.

[119] P.K. Danso, E.C.P. Neto, S. Dadkhah, H. Molyneaux, A.A. Ghorbani, Ensemble-based intrusion detection for internet of things devices, in: 2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life using ICT, IoT and AI, HONET, IEEE, 2022, pp. 034–039.