

Received March 8, 2020, accepted March 28, 2020, date of publication March 31, 2020, date of current version April 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2984726

# SEC-C-U: The Security of Intensive Care Unit Medical Devices and Their Ecosystems

CARMEL ELIASH<sup>1,2</sup>, ISAAC LAZAR<sup>3</sup>, AND NIR NISSIM<sup>1,4</sup>

<sup>1</sup>Malware Lab, Cyber Security Research Center, Ben-Gurion University of the Negev, Beer-Sheva 8410501, Israel

<sup>2</sup>Department of Industrial Engineering, Tel Aviv University, Tel Aviv 6997801, Israel

<sup>3</sup>Division of Pediatrics, Pediatric Intensive Care Unit, Soroka University Medical Center, Beer-Sheva 8410101, Israel, and also with the Faculty of Health Sciences, Ben-Gurion University of the Negev, Beer-Sheva 8410501, Israel

<sup>4</sup>Department of Industrial Engineering and Management, Ben-Gurion University of the Negev, Beer-Sheva 8410501, Israel

Corresponding author: Nir Nissim (nirni@bgu.ac.il)

**ABSTRACT** An intensive care unit (ICU) is dedicated to caring for patients whose medical condition places them at high risk of mortality or serious morbidity. ICU medical devices (ICUMDs) are used to closely monitor, stabilize, and treat ICU patients who are often unconscious and rely almost solely on ICUMDs. ICUMDs have become more autonomous, with a range of components, connectivity to external devices, and functionalities, opening the door to cyber-attacks. We present a taxonomy based on the functionality of 19 widely used ICUMDs, providing an explanation of each device's medical role, properties, interactions, and how they impact each other's security. We provide an extensive survey of 16 possible attacks aimed at ICUMDs and assess each device's vulnerability. We also create an ecosystem graph describing the roles and interactions of the players of each ICU sub-department. For each device type we produce a unique attack flow diagram that presents the most vulnerable vectors and components within the ecosystem. Finally, we survey relevant security mechanisms and map their coverage for the attacks, identifying existing gaps. We show that current security mechanisms generally fail to provide protection, covering just 12.5-56.3% of the attacks against ICUMDs, leaving the devices and the patients vulnerable.

**INDEX TERMS** ICU, medical device, cyber-attack, malware, detection, security, privacy.

## I. INTRODUCTION

In recent years, there has been a growing trend in the use of advanced technologies in medical ecosystems in order to improve patient care. As part of this trend, medical devices incorporating advanced technologies have been used to assist medical teams in providing optimal treatment for patients, expanding physicians' abilities and providing them with more accurate and useful information regarding the patient's current condition. The use of information systems for the retrieval of prior medical data on the patient enables the medical team to provide patients with tailored treatment that meets their personal needs [1]. Figure 1 shows the growth of the global digital health market between 2015 and 2020 [88]. In 2015, the total cost was 79 billion US dollars, and by the end of 2020, it is estimated to reach 206 billion dollars, an increase of 260% in just five years. This segment of the market includes the following fields: Electronic Health

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran<sup>1</sup>.

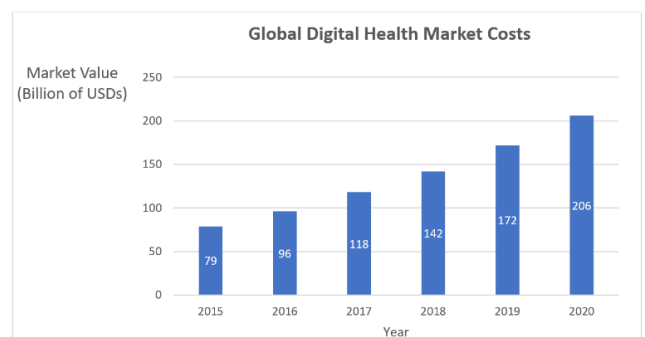


FIGURE 1. The growth of the global digital health market in recent years.

Record, telehealth, mobile health, and wireless health, all of which related to medical devices and systems like those used in the ICU. Such a graph emphasizes the need to enhance the security of medical devices to improve patients' healthcare and enhance their security as well.

In addition to offering medical advantages, the use of IT in the medical sector also has significant financial advantages, for example, the use of electronic health records (EHRs) could lead to a savings of \$81 billion per year [19] by improving the administration of chronic medications and reducing the number of repeated diagnoses that could result from insufficient documentation [20].

However, the use of advanced medical technology creates many challenges, especially in terms of vendors' responsibility and reputation, and patients' privacy. For example, in recent years, EHRs have been targeted by cyber-criminals [80].

The multiplicity of devices, connections between devices, technological uniqueness of each device, as well as the targeted functionality of each device, contribute to a complex combination of potential cyber-security risks, vulnerabilities, and challenges. In addition, unlike the past where medical devices were considered standalone devices, distributed medical systems featuring integration and communication between different information systems and medical devices [21] are very popular these days.

The domain of securing medical ecosystems (information systems, devices, and the communication modalities operating between them) has gained momentum in recent years, as awareness of the potential attacks and risks, and their dangers increases [75]<sup>1,2</sup>. Recently, various cyber-attacks have demonstrated their potential harm in medical ecosystems.<sup>3</sup> It is estimated that around 94% of healthcare organizations have already suffered from a cyber-attack [38]. Such attacks include the WannaCry ransomware malware that struck over 150 different countries in May 2017 and 48 hospitals in the United Kingdom [17] alone. Healthcare providers were prevented from accessing patients' medical information, and medical records were encrypted by the ransomware; such encryption also affected other medical information systems at the hospitals, including appointment scheduling, disrupting the delivery of medical services in the country for several days.

The FDA reported over 1.2 million cases of irregularities in various medical devices between 2006 and 2011 (e.g., computer related failures) [2]. The technological complexity of medical devices is only increasing, as is the complex and varied communication between different devices, making it even more difficult to manage the risks, identify the vulnerabilities, anticipate attacks, and devise a means of securing this emerging technology [32].

In addition to attacks that could result in physical harm, intensive care unit medical devices (ICUMDs) also expose patients to information theft, as data regarding the patient's health and medical treatment may be stolen. The breach of a patient's medical confidentiality is a cyber-attack vector

which on one hand can violate patient privacy, while on the other hand can cause medical device vendors to lose a large amount of money and harm their reputations, mainly in light of the new General Data Protection Regulation (GDPR) [51] which results in significant fines to vendors whose customers suffer from privacy violations.

One of the main difficulties in detecting cyber-attacks aimed at medical devices is differentiating between the occurrence of an unusual phenomenon that stems from the patient's medical condition or a technical bug associated with a medical device and a situation that originates from a cyber-attack interfering with the device's normal activity. Between 2009 and 2011, over 142 cases in which malware attacked medical devices were documented, affecting around 156 different medical organizations, including laboratories, medical research institutions, pharmacies, etc. [22]. In 2019, FDA experts warned that medical devices are very vulnerable to hacking and emphasized the difficulty that healthcare providers have in identifying the risks and sharing knowledge about them.<sup>4</sup>

Patients with severe and life-threatening illnesses and injuries are treated in intensive care units (ICUs), an essential unit of all major hospitals. For example, in 2014, there were 5,686 hospitals in the US, each of which had at least one ICU.<sup>5</sup> In 2005, ICU beds represented 15% of the hospital beds in the US. The total costs of critical care medicine constituted 13.4% of hospitals' costs and 4.1% of national health expenditures in the US [43], and the average number of ICUMDs per patient is 2.9-5.5 (based on three observations).<sup>6</sup> These devices (reviewed in detail below) include mechanical ventilators, multi-parametric monitoring systems, drug delivery devices (syringes and infusion pumps), feeding devices, point of care imaging devices, and laboratory devices, all of which are vital for patient care in the ICU. Such devices are very expensive, for example, the price of a single ventilator system can exceed \$100,000.

In terms of security, the ICU differs from other hospital departments in two main respects: 1) the patient's medical condition, along with the treatment they receive from the ICU medical team; and 2) the properties of the ICUMDs themselves. Regarding the former, most ICU patients are partially conscious or even unconscious, preventing them from communicating with the medical team and providing important input regarding their condition or asking for help when needed. Therefore, ICUMDs play a critical role in the ICU, providing immediate and ongoing feedback about the patient's state of health. The ICU medical team depends heavily on the data, measurements, and output of ICUMDs, relying almost solely on these devices when making medical decisions.

<sup>1</sup>[http://www.pmlive.com/blogs/digital\\_intelligence/archive/2016/january/threat\\_of\\_medical\\_device\\_hacking\\_is\\_growing\\_concern\\_913853](http://www.pmlive.com/blogs/digital_intelligence/archive/2016/january/threat_of_medical_device_hacking_is_growing_concern_913853)

<sup>2</sup><https://www.fda.gov/medical-devices/digital-health/cybersecurity>

<sup>3</sup><https://compliancenavigator.bsigroup.com/en/medicaldeviceblog/medical-devices-and-cyber-security/>

<sup>4</sup><https://www.medscape.com/viewarticle/918232>

<sup>5</sup><http://www.sccm.org/Communications/Critical-Care-Statistics>

<sup>6</sup>[https://www.researchgate.net/publication/285474310\\_Vital\\_Medical\\_Devices\\_in\\_Intensive\\_Care\\_Unit](https://www.researchgate.net/publication/285474310_Vital_Medical_Devices_in_Intensive_Care_Unit)

In addition, the medical condition of ICU patients is often unstable and can change quickly and unexpectedly, requiring a quick response from the medical team who must adjust treatment in response to changes in the patient's condition almost immediately. In order to ensure the best support for the medical team, ICUMDs are required to provide continuous availability and full functionality at all times. The shortage of ICU manpower compounds the situation and increases the medical team's dependence on ICUMDs. Increasingly, these devices are semiautonomous machines which serve as reliable alarm systems, issuing alerts when specific parameters are breached.

Regarding security differences associated with the ICUMDs themselves, first, the various ICUMDs provide many different measurements, information, and data, upon which the medical team must draw a comprehensive and accurate picture of the patient's medical status. These measurements may contradict each other, as they may have different meanings in relation to other values. Because of this, the accuracy of the measurements and data, and the reliability of the ICUMDs play a critical role in the ICU patient's health-care. Furthermore, the instability of ICU patients means that minor medical errors that stem from delays in measurement retrieval or data disruption and anomalies can significantly affect a patient's health.

Second, some ICUMDs operate autonomously based on medical data collected from the patient. For example, the body heater device measures the patient's body temperature and the room temperature, adjusting the patient accordingly. While this type of care provided by a device operating in autonomous mode can free the medical team up, allowing them to tend to other important medical issues, and help address the shortage of ICU caregivers, it can also expose the patient to harm in the case of a compromised ICUMD. These are some of the ways in which the properties of specialized ICU medical devices affect the security of the devices.

Because of the nature of ICU patients and the devices themselves, the ICU medical team and patients rely upon ICUMDs, and this dependency emphasizes the great importance of securing ICUMDs from potential cyber-attacks.

Cyber-attacks may be aimed at the ICU for three main reasons. The first is for economic gain. Attackers can launch cyber-attacks on the ICU in order to demand ransom, either from the hospital or a patient's family, knowing that the desperate condition of the patients and the limited number of ICUMDs increases the likelihood that the ransom demanded will be paid quickly, allowing the victimized patient to receive the necessary treatment. Hackers can get around \$1 per record if they sell them in bulk or up to \$1000 for the records of specific people [81].

The second reason, to improve business, is directly related to damaging an ICUMD vendor's reputation. Due to the importance of the reliability and full functionality of ICUMDs, an ICUMD company may launch a cyber-attack on a competitor's device in order to compromise the competitor's reputation; this may result in reduced sales and revenue for

the competitor and increased sales for the attacker. The third reason is to perform acts of terrorism or threaten national security; cyber-attacks have already been used in warfare, both for reconnaissance [65] and to damage an enemy's battle infrastructure [66]. By disrupting the operation of an ICUMD, an attacker (i.e., a state actor) could, for example, harm or even assassinate a specific VIP hospitalized in an ICU. A cyber-attacker leaves a light footprint, making identification of the attacker difficult. The attacker can also perform an attack in such a way that the patient's death appears natural, thus avoiding suspicion and repercussions from the VIP's state.

While the awareness of security problems in the medical world has increased in recent years, research performed has raised fundamental questions about the effectiveness and response of existing defense mechanisms [3]; in fact, Perakslis [3] states that there are various types of policies in place to protect the privacy and security of medical systems, but they will not necessarily ensure security of the devices.

In addition, as was indicated by Sametinger *et al.* [18], the security risks in the hardware and software of medical systems are too varied and numerous to prevent all of them, and we must focus on methods of analyzing temporal behavior to detect potential vulnerabilities. In addition, the article highlights the difficulty of preventing data flow delays resulting from the development of defense mechanisms; such delays may affect the efficiency of the medical devices and threaten ICU ecosystems and patients.

The obvious need for medical system security on the one hand and inadequate defense mechanisms on the other highlights the need to develop clear and effective security mechanisms to protect ICUMDs and the patients that rely on them. An understanding of ICU medical devices and their interactions and vulnerabilities, ICU ecosystems, potential cyber-attacks, and existing security gaps is required in order to develop such security mechanisms, and this paper provides this essential information. In order to achieve our aims, we structured a hypothetical ICU based on published data and personal knowledge, which does not necessarily describe a specific ICU [71] but rather presents a more generic one. The medical device photos that appear in this paper represent some of the different electronic devices prevalent in the ICU. All brand names were removed in order to prevent any association between specific devices and possible cyber-security attacks, vulnerabilities, or breaches.

The main purpose of this paper is to present a comprehensive survey of ICUMDs, focusing on possible vulnerabilities and cyber-attacks. We analyzed each of the attacks, as well as the ICU ecosystems, through meaningful comparisons. We also present a set of attack building blocks upon which the attacks are based; such building blocks will serve as the basis for evaluating the risks associated with each attack, as well as for the future development of accurate and designated security mechanisms. We also address existing security mechanisms and map their coverage of the attacks in order to identify gaps in the security of ICUMDs.

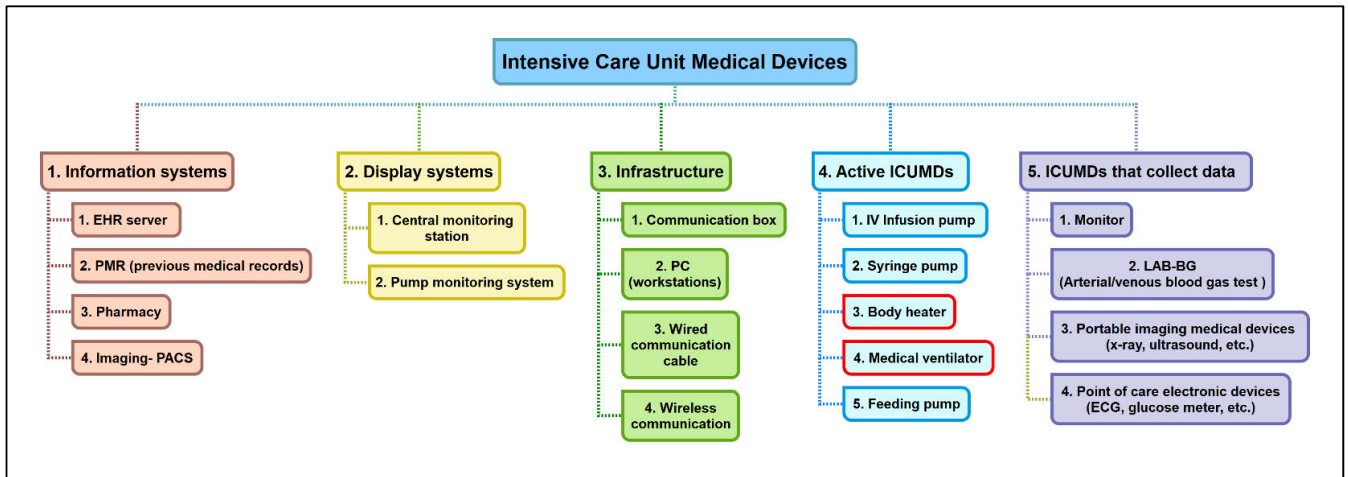


FIGURE 2. Taxonomy of intensive care unit medical devices.

The contributions of this paper are as follows:

- This paper provides a taxonomy of existing ICUMDs based on their medical functionality (including some specific device models).
- We describe the ICU ecosystem and the relationships between the various ICUMDs and entities in the ICU in terms of the flow of information and mutual influences.
- A survey of potential attacks targeting ICUMDs is provided, in an up-to-date, comprehensive manner, including details about attack scenarios, attack vectors, and prerequisites.
- An “attack flow” diagram has been created for each section/room of a generic ICU. Each diagram includes relevant ICUMDs associated with its section/room. These diagrams reveal the most vulnerable vectors and components of the ICUMD ecosystems (these weak links represent the areas that require an appropriate security mechanism or a policy change to prevent a vulnerability from becoming an attack vector).
- We present basic, yet important, building blocks, by which the presented attacks are carried out. These will serve as the basis of a novel risk analysis methodology for medical devices, which will enable us to assess the risk and prevalence associated with each attack, and identify the most dangerous attacks (those that should be addressed first); these buildings blocks will also help define the security mechanism required to address the attacks.
- In this paper, we assess and review the existing security mechanisms for ICUMDs in the face of the attacks presented (both existing and novel), in order to identify the current security gaps and to offer improvements for security of the ICUMD ecosystems.

The paper encompasses the following: an ICUMD taxonomy and description of the ICUMDs, ICUMD ecosystems, and attack diagrams, detailed information on potential attacks and

the existing security mechanisms, and our conclusions and suggestions for future work.

## II. ICUMD TAXONOMY AND DESCRIPTION

Since ICUMDs were developed in order to treat a variety of medical conditions that ICU patients may suffer from, an understanding of the various categories of ICUMDs, and their properties, abilities, and uniqueness is needed before evaluating the risk and vulnerabilities they might conceal in the context of cyber-attacks. Therefore, we provide a taxonomy of ICUMDs that includes five main categories of devices (information systems, data display systems, infrastructure, active medical devices, and data collection devices), categorized based on their main functionality and goal, and 19 devices associated with them in Figure 2. This is followed by description of each category and device.

### 1) ICU MEDICAL DEVICE TAXONOMY

In Figure 2, we present a taxonomy of 19 widely used ICUMDs based on their main functionality (1-5).

As can be seen in Figure 2, the ICU contains many devices which are used to treat patients who often suffer from multi-systemic injuries or multiple organ failure and require complex and integrated therapeutics. The taxonomy reflects the fact that information systems are key players in the ICU and emphasizes the impact and significance of the information technology revolution in healthcare, specifically in the ICU. Therapeutic equipment can be roughly divided into two main categories: 1) **Active ICUMDs** - devices that actively treat the patient’s medical condition, and 2) **ICUMDs which collect data** - devices designed to collect various physiological measures from the patient in order to monitor the patient’s medical condition. Note that ICUMDs that are marked in red are autonomous ICUMDs, which means that they have the ability to provide the patient specific treatment and care autonomously (without human intervention), using advanced

technology and algorithms that analyze and monitor the patient's condition.

## 2) ICUMD DESCRIPTIONS

In this subsection, we describe 19 major ICUMDs used in the ICU. The material is organized according to the ICUMD categories used in the taxonomy. Figures 6-17 in Section VII present some of these ICUMDs.

### *a: INFORMATION SYSTEMS*

#### *i) EHR SERVER*

An electronic medical record (EMR) [27], [28] or electronic health record (EHR) is an electronic information system that contains and manages the medical history of a patient. Using electronic medical records enables sharing medical information across various medical facilities, regardless of their location and history with the patient. These files contain important information about the patient, from the patient's age and weight, to test result, allergies, and prescription medication. In addition, computerized systems provide convenient access to medical information and features such as dose calculators and fluid calculators, and offer tips for physicians and nurses that support decision-making.

#### *ii) PMR (EXTERNAL SYSTEMS)*

The previous medical record (PMR) system is an additional information system external to the internal EMR information system, which is aimed at managing electronic health records that originate from external systems (e.g., patient data that belongs to external organizations, like health maintenance organizations). These systems share prior medical records with the hospital's internal system, so the medical team can see a wider medical picture [61].

#### *iii) PHARMACY*

This type of information system is used for managing medications, ABX (antibiotic) prescriptions, and the transfer of medication orders from the physician (who is at the bedside) to the nurse (who is in the medication preparation room) or pharmacist (who is at the pharmacy) [68]. The pharmacist gets the order, approves it, prepares the medicine, and informs the doctor/nurse when the medicine is ready. The Pyxis MedStation system<sup>7</sup> is an example of such a system. There is a pharmacy inventory in the ICU which is used to supply drugs to patients, and a pharmacy information system serves as an efficient interface between the medical team and the pharmacy.

#### *iv) MEDICAL IMAGING–PACS*

A picture archiving and communication system (PACS) [34] is a medical imaging technology that enables cost-effective storage and easy access to images from multiple modalities.

<sup>7</sup><https://www.bd.com/en-us/offerings/capabilities/medication-and-supply-management/medication-and-supply-management-technologies/pyxis-medication-technologies/pyxis-medstation-system>

ties. These electronic images are transmitted digitally via the PACSs.

### *b: DISPLAY SYSTEMS*

#### *i) CENTRAL MONITORING STATION*

Real-time central monitoring systems offer the clinical team easy access to the monitors' (see Subsection 2.2.5.1 below) information. This important device, which displays the monitor data of all ICU patients in real-time, is located at the nurses' station, and satellite monitors can be placed in the rooms of the ICU director, on call physician, senior physician, etc. This type of system includes limited monitor configuration and limited operation capabilities which are operated remotely (e.g., delivering commands to measure non-invasive blood pressure (NBP), setting thresholds for "normal" medical measurements, etc.).

#### *ii) PUMP MONITORING SYSTEM*

The real-time monitoring system (described above) presents the data from each of a patient's different pumps (e.g., IV infusion pump and syringe pump).

### *c: INFRASTRUCTURE*

#### *i) COMMUNICATION BOX*

The communication box<sup>8</sup> is connected to all devices in the patient's room via LAN cables. It does not store information or have any processing capabilities. Some devices (mainly infusion and syringe pumps) can transfer information to the communication box via a LAN cable or direct cable communication, using an infrared interface. Data is transferred directly from the communication box to the EMR system.

#### *ii) PC (WORKSTATIONS)*

The ICU workstations used by nurses and doctors in their daily work are simple personal computers with access to EMR systems, an Ethernet connection (including institutional email), and access to other external systems such as civil registry and hospital management systems. Workstations may have a limited or fully secure Internet connection, in accordance with the hospital's institutional policies. A workstation can also be connected to a printer via a USB cable or LAN communication. A standard USB keyboard and computer mouse are usually connected to the workstation.

#### *iii) WIRED COMMUNICATION CABLE*

LAN cables are used for communication between devices, for example, to transfer data (via the communication box) from the patient's monitor directly to the central monitoring station at the nurses' station.

#### *iv) WIRELESS COMMUNICATION*

The wireless capabilities of medical devices in most ICUs are disabled for security reasons, as a general institutional policy.

<sup>8</sup><https://r-stahl.com/en/global/products/junction-and-terminal-boxes/>

However, in some cases, short-range wireless communication between devices is enabled (e.g., infrared radiation (IR) between the IV pump and the pump's pole).

#### d: ACTIVE ICUMD

##### i) IV (Intravenous) INFUSION PUMP

An infusion pump [35] infuses fluids, medications, or nutrients into a patient's circulatory system. These pumps are generally used intravenously.

##### ii) SYRINGE PUMP

A syringe pump [36] is a small infusion pump which is used to gradually administer a very specific quantity of liquid (with or without medication) to a patient. Unlike the IV infusion pump, this pump injects smaller volumes. It is usually used intravenously, but it although can be used for epidural, subcutaneous, and arterial infusions. These pumps are connected to patients in accordance with their medical condition and treatment.

##### iii) BODY HEATER/COOLER

A heat emitting device is designed to balance the patient's body temperature.<sup>9</sup> This device is positioned above the patient's bed and emits focused heat/cold on the patient using different interfaces: a direct radiation heating lamp, a heating/cooling water blanket system, or a heating/cooling air blanket. The temperature is set manually by ICU staff and is adjusted autonomously based on patient body temperature sensors (which monitor the skin temperature, core temperature, etc.). The device autonomously adjusts its activity according to the target temperature (defined by the medical team) and the temperature of the patient's body (the sensor is usually located on the patient's buttocks).

##### iv) MEDICAL VENTILATOR

A mechanical ventilator is a device designed to maintain adequate ventilation and/or oxygenation, taking over for patients or partially assisting them in this area [62]. This major life support system is a pillar of the modern ICU. Modern ventilators are highly sophisticated computerized machines. Today, most ventilators have closed loop ventilation capabilities, supporting the patient's changing needs according to sensitive sensing devices and autonomously changing the oxygen concentration, respiratory rate, and ventilation pressure. Some ventilators have the advanced capability of self-activating a weaning process for the patient, meaning, gradually decreasing ventilatory support. These devices adjust respiratory support according to data sensed (by respiration sensors) from the patient, and monitor the patient's condition based on alarm settings determined by the medical team. The ventilator communicates with the EHR system via a communication port to input real-time patient and ventilator settings into the patient's EHR.

<sup>9</sup>[https://www.researchgate.net/figure/Heat-transfer-mechanisms-of-a-newborn-inside-an-open-radiant-warmer-C-MedIT-2010\\_fig5\\_210290210](https://www.researchgate.net/figure/Heat-transfer-mechanisms-of-a-newborn-inside-an-open-radiant-warmer-C-MedIT-2010_fig5_210290210)

##### v) FEEDING PUMP

A feeding pump is responsible for delivering liquid nutrition to the patient. The pump delivers the liquid nutrition through a tube connected to the patient's digestive system (nasogastric, orogastric, percutaneous gastric, etc.). The pump can be a standalone device or connect to a central pump system just like the syringe pumps. Many ICU patients suffer from medical problems that prevent them from eating independently and are therefore connected to feeding pumps. The feeding pumps are usually located next to the patient's bed [69].

#### e: ICUMDs THAT COLLECT DATA

##### i) ICU MONITOR

An ICU monitor is a medical device used to display the patient's vital signs and other electronical measurements collected from sensors connected to the patient [64]. It can consist of one or more sensors, processing components, and display devices, as well as communication links for displaying or recording the results elsewhere through a monitoring network. ICU monitors have capabilities to measure and display the following type of data: **electrical** - ECG, cardiac arrhythmias, respiratory rate, O<sub>2</sub> saturation, EtCO<sub>2</sub>, body temperature (e.g., skin, rectal, urinary bladder temperature); **pressure** - blood (venous, arterial, intracardiac chambers), intracerebral, intracavitary (e.g., intra-abdominal, urinary bladder) pressure; and **biochemical** - intravascular biochemical measurements (venous PH, O<sub>2</sub> sat, CO<sub>2</sub>), EtCO<sub>2</sub>, etc.). The monitor has some internal calculation capabilities (cerebral perfusion pressure, cardiac pulmonary catheter calculations, etc.). The monitor can store the data over time in order to review trends and transfer data to the EHR. The device contains an IR port (for a printer connection) and a USB port (which is usually disabled). The device enables the medical team in the ICU to fully and continuously monitor the patient's main medical measurements.

##### ii) LAB-BG

An arterial/venous blood gas (ABG/VBG) test measures the pressure of different gases in the blood serum, such as oxygen and carbon dioxide [67]. Depending on the device, it may also measure different electrolytes (sodium, potassium, calcium, bicarbonate, lactic acid), PH in the serum, and the sample's hematocrit. It requires a small volume of heparinized blood drawn from the patient. Modern ICU's contain blood gas or other blood analysis machines. Each sample is related electronically to a single patient, and the results are sent electronically to the patient's EHR. The results of these tests inform the medical team about the patient's medical status, and are used as an evaluation for the need for frequent monitoring of the patient's medical condition; given this, the medical team performs frequent blood tests. The presence of this device in the ICU allows the medical team the ability to perform such tests as easily and immediately.

### iii) PORTABLE IMAGING MEDICAL DEVICES (X-RAY, ULTRASOUND, ETC.)

A portable imaging device enables the medical team to perform imaging studies at the patient's bedside, without the need to transfer the patient to the imaging department. Images are processed and sent to the PACS; these images may be viewed at the patient's bedside monitor or on any other monitor that has PACS capabilities connected to the hospital's system. The imaging that can be performed includes x-rays (chest, abdomen, bones, etc.), Doppler echocardiography, ultrasounds (brain, chest, visceral organs and cavities, etc.) and others [60], [63].

### iv) POINT OF CARE ELECTRONIC DEVICES (ECG, GLUCOSE METER, ETC.)

Some small electronic medical devices are used to perform medical analysis at the patient's bedside; the results of these analyses are transferred via Wi-Fi to the EHR. Such devices include devices that measure whole blood ketone body level and whole blood dextrose level through a finger prick, portable ECG device, glucose meter, etc., [73].

## 3) INTERACTIONS AND VULNERABILITIES WITHIN ICUMD ECOSYSTEMS

In this section, our goal is to provide an in depth understanding regarding the ICUMD ecosystems, knowledge that is crucial for understanding the cyber-attacks presented later in the paper, as well as the approaches to address, detect, and prevent such attacks. First, we discuss the interactions between the different ICUMDs within the ICU, as these interactions are of great importance and are, in fact, one of the unique characteristics of ICUMDs compared to other medical devices. Many other medical devices (which do not belong to ICUMD ecosystems) do not have rich ecosystems that incorporate a variety of additional medical devices, and therefore they rarely interact, communicate, or affect other medical devices, while within the ICU, some of the devices are used to operate other devices, provide input and output to one another, or take an active role in the task of treating and stabilizing the patient. Then, we present the entire ICUMD ecosystem and individual device ecosystems, based on their daily use in the context of their ICU role, taking into consideration their physical location within the ICU. The placement of the ICUMDs within the overall ICU ecosystem has great importance, as the ICU medical team is triggered by and responds to the ICUMDs, and any malfunctioning of ICUMDs may affect the response time of the medical team. Then, in addition to the ecosystem diagrams we present, we also indicate the existing and potential attacks that can compromise ICUMDs, so the reader can understand the various vulnerabilities and attack vectors within the ICU.

#### Interactions Between the Devices:

The following table (Table 1) presents the interactions between the various ICUMDs and indicates the exact information flow between the various devices in the ICU. The

leftmost column contains the ICUMD from which the information is being sent, and the top row represents the ICUMD which receives the information. Based on the information we presented in Figure 2 above, the table lists each device, along with the number in Figure 2 (according to the different functionality categories they belong to). As can be seen, most of the ICUMDs transmit information to another ICUMD; there are also trivial connections (such as connections between the pumps and the pump monitoring system), and there are non-trivial connections which are more important to understand in the context of the vulnerabilities and attack vectors. Such non-trivial interactions include: 1) the autonomous activity of the body heater, (2) the ability to control the monitor from the central monitoring station, and 3) the autonomous activity of the medical ventilator. The numbers inside the cells represent whether an interaction exists and the type of interaction between devices, as explained in the legend below the table. The numbers of non-trivial interactions appear in red, and those of trivial interactions appear in blue. The list of the 10 different interactions presented below is divided into trivial interactions and non-trivial ones.

#### Non-Trivial Interaction Index:

1. The device is controlled remotely (commands, mute alarms, etc.).
2. The heater senses the patient's temperature and adjusts its activity according to the target temperature (defined by the medical team) and the patient's temperature.
3. The ventilator regulates its activity according to a defined plan and the patient's respiratory measures (such as oxygen supply based on the patient's target O<sub>2</sub> saturation level).
4. Controls the monitor remotely (mute alarms, define "normal" values per patient, etc.).

#### Trivial Interaction Index:

1. Data from the device is transferred to the central monitoring station via physical cables.
2. The data from the communication box is transferred to the EHR server via LAN.
3. Data from the device is transferred via IR to the docking station, and from there the data is transferred to the communication box via LAN.
4. Data from the device is transferred via IR to the docking station, and from there the data is transferred to the pump monitoring system via LAN.
5. Data from the device is transferred to the communication box via physical cables.
6. Data flows via LAN.

As can be seen, 40% of the total interactions are not trivial and might be abused or utilized by an attacker.

## III. ICUMD ECOSYSTEMS AND ATTACK DIAGRAMS

The purpose of this subsection is to map (simply) the devices that can be found in the ICU and the information transferred between them. First, we map the devices to actual rooms in the ICU to understand the physical location of

**TABLE 1.** Interaction between medical devices in the ICU.

| Device (From/to)                | 1.1. EHR Server | 1.3. Pharmacy | 2.1. Central monitoring station | 2.2. Pump monitoring system | 3.1. Communication box | 3.2. Workstation | 4.1. IV infusion pump | 4.2. Syringe pump | 4.3. Body heater | 4.4. Medical ventilator | 5.1. Monitor | 5.2. LAB-BG |
|---------------------------------|-----------------|---------------|---------------------------------|-----------------------------|------------------------|------------------|-----------------------|-------------------|------------------|-------------------------|--------------|-------------|
| 1.1. EHR Server                 | -               | 10            |                                 |                             |                        | 10               |                       |                   |                  |                         |              |             |
| 1.3. Pharmacy                   | 10              |               |                                 |                             |                        |                  |                       |                   |                  |                         |              |             |
| 2.1. Central monitoring station |                 |               | -                               |                             |                        |                  |                       |                   |                  |                         | 4            |             |
| 2.2. Pump monitoring system     |                 |               |                                 | -                           |                        |                  | 1                     | 1                 |                  |                         |              |             |
| 3.1. Communication box          | 6               |               |                                 |                             | -                      |                  |                       |                   |                  |                         |              |             |
| 3.2. Workstation                | 10              |               |                                 |                             |                        | -                |                       |                   |                  |                         |              |             |
| 4.1. IV Infusion pump           |                 |               |                                 | 8                           | 7                      |                  | -                     |                   |                  |                         |              |             |
| 4.2. Syringe pump               |                 |               |                                 | 8                           | 7                      |                  |                       | -                 |                  |                         |              |             |
| 4.3. Body heater                |                 |               |                                 |                             |                        |                  |                       |                   | 2                |                         |              |             |
| 4.4. Medical ventilator         |                 |               |                                 |                             | 9                      |                  |                       |                   |                  | 3                       |              |             |
| 5.1. Monitor                    |                 |               | 5                               |                             | 9                      |                  |                       |                   |                  |                         | -            |             |
| 5.2. LAB-BG                     | 10              |               |                                 |                             |                        |                  |                       |                   |                  |                         |              |             |

the different devices (this information is based on published ICU literature [71]). Then, we drill down and analyze the ICUMDs within each room, considering the connections and interactions between the various ICUMDs, their impact on each other, and the interaction between the ICUMDs and the medical environment (patient/medical personnel). The diagrams in the upcoming subsections help us delineate and map possible vulnerabilities and cyber-attacks aimed at the ICU.

**A. ICUMDs (BROKEN DOWN BY ROOM)**

Figure 3.1 describes the various ICUMDs in the ICU, broken down by physical rooms. In addition, it describes the level of interactions and flow of information between the rooms. As can be seen, the nurses’ station is a central room (serves as the ICU hub), connecting the various rooms and systems.

Figures 3.2 and 3.3 provides the general structure of the patient’s room and nurses’ station.

Figures 3.4-3.7 provide a more in depth look at each of the rooms. These diagrams provide detailed information about the interactions and the information flow between the devices.

The following notes apply to all the figures:

1. The devices in a patient’s room can transfer the data to the EHR server via a communication box or directly (by LAN cables), depending on hospital policy.
2. The servers of the EHR, the central monitoring station, and the LAB-BG may be located in different places, again, depending on hospital policy. In most cases they are located at the nurses’ station (or very close to it). In our examples we placed these devices in a general “service” area.
3. The ability to insert a USB device into servers, such as workstations or the server of the central monitoring station, also depends on hospital policy.

The numbers on each edge represent potential attacks on this connection: numbers that appear in blue represent existing



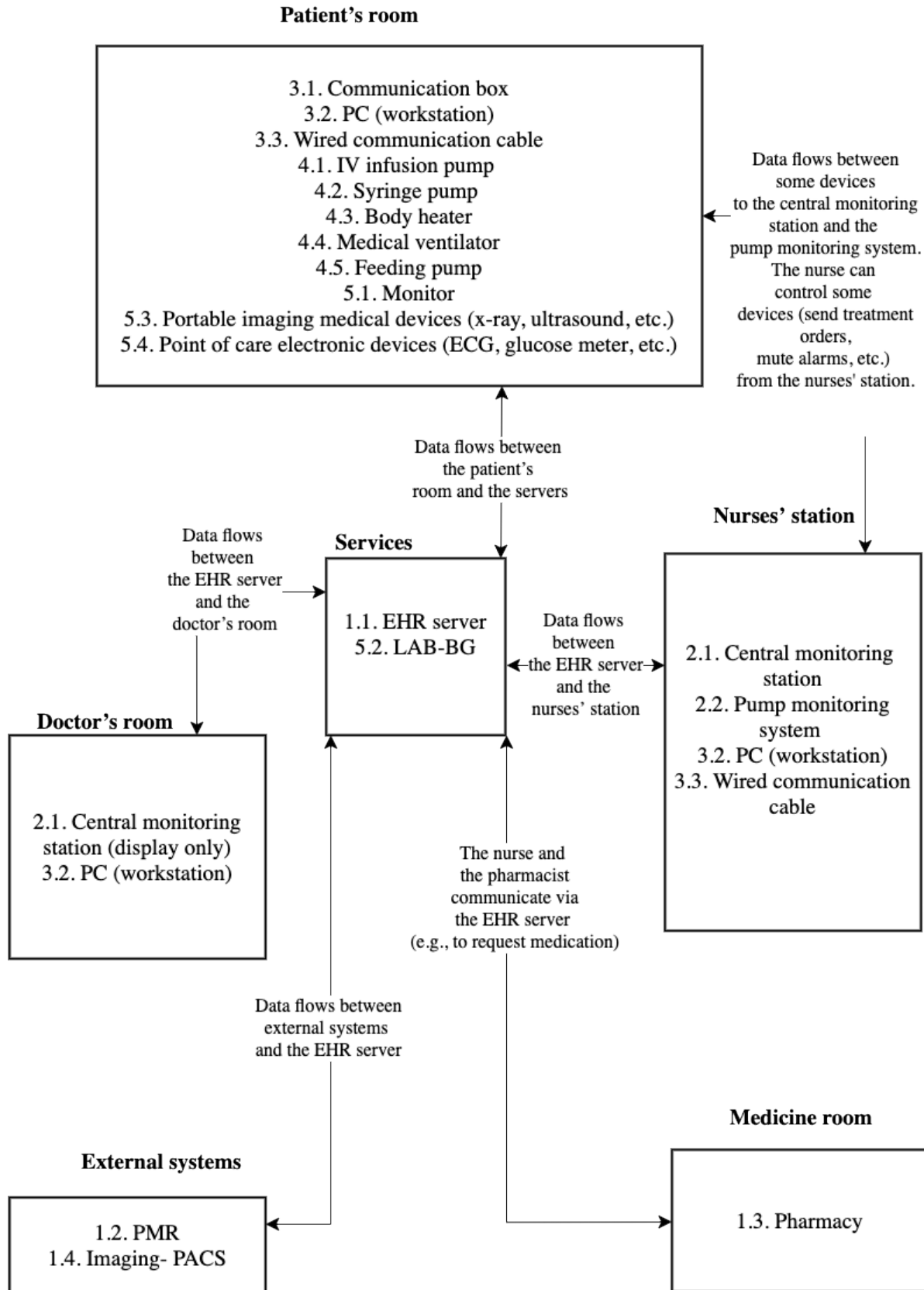


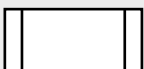




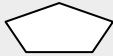
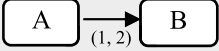


FIGURE 3.1. Devices in the ICU, broken down by room.

**TABLE 2.** Legend describing the components of the ICUMD ecosystem diagrams.

| Shape   | Description   |
|---|---|
|    | Component – usually represents a device(s)  |
|    | Autonomous device – represents an active device that regulates treatment autonomously   |
|    | Subcomponent – represents a module that is responsible for a specific task within a component   |
|    | A terminator – indicates the beginning or end of the flow   |
|    | An open network – Internet  |
|    | Internal network – Intranet   |
|   | A logical encapsulation – represents devices with shared attributes (usually the same physical location)  |
|  | Human factor  |
|  | A directed edge – connecting a component (e.g., A) to another component (e.g., B), only if information flows from A to B (a dashed arrow indicates a possible, but not mandatory, connection) |

cyber-attacks (known attacks), and those in red represent proposed attacks (unknown attacks). Table 2 contains the legend, explaining the components making up the ICUMD ecosystem diagrams.

Blue- represents an existing cyber-attack (known attack).

Red- represents a proposed attack (unknown attack).

**B. GENERAL STRUCTURE OF A PATIENT’S ROOM**

Figure 3.2 presents the general structure of a patient’s room. As can be seen, the patient’s bed is in the middle of the room, and all of the devices surround the bed. Some of the devices communicate with the communication box, and some are standalone devices.

**C. GENERAL STRUCTURE OF A NURSES’ STATION**

Figure 3.3 presents the general structure of a nurses’ station. As can be seen, the nurses’ station is in the center of the ICU, and it contains three main systems that enable the nurses to

monitor and track the patients. The patients’ beds are facing the nurses’ station, so the nurses can see them.

**D. PATIENT’S ROOM**

Figure 3.4 describes the ecosystem in the patient’s room, illustrating the multiplicity of ICUMDs to which the patient is connected, as well as the interaction and communication between these ICUMDs. As can be seen, there are some active medical devices that function autonomously or in a closed loop (body heater and medical ventilator). In addition, in this room there is a communication box where the medical information that comes from the various ICUMDs accumulates and transferred to a variety of information systems. As can be seen in the figure below, denial-of-service, delay attacks, and configuration manipulation are the most common attacks targeting devices in the patient’s room. These attacks may damage any of the devices in the patient’s room, and because

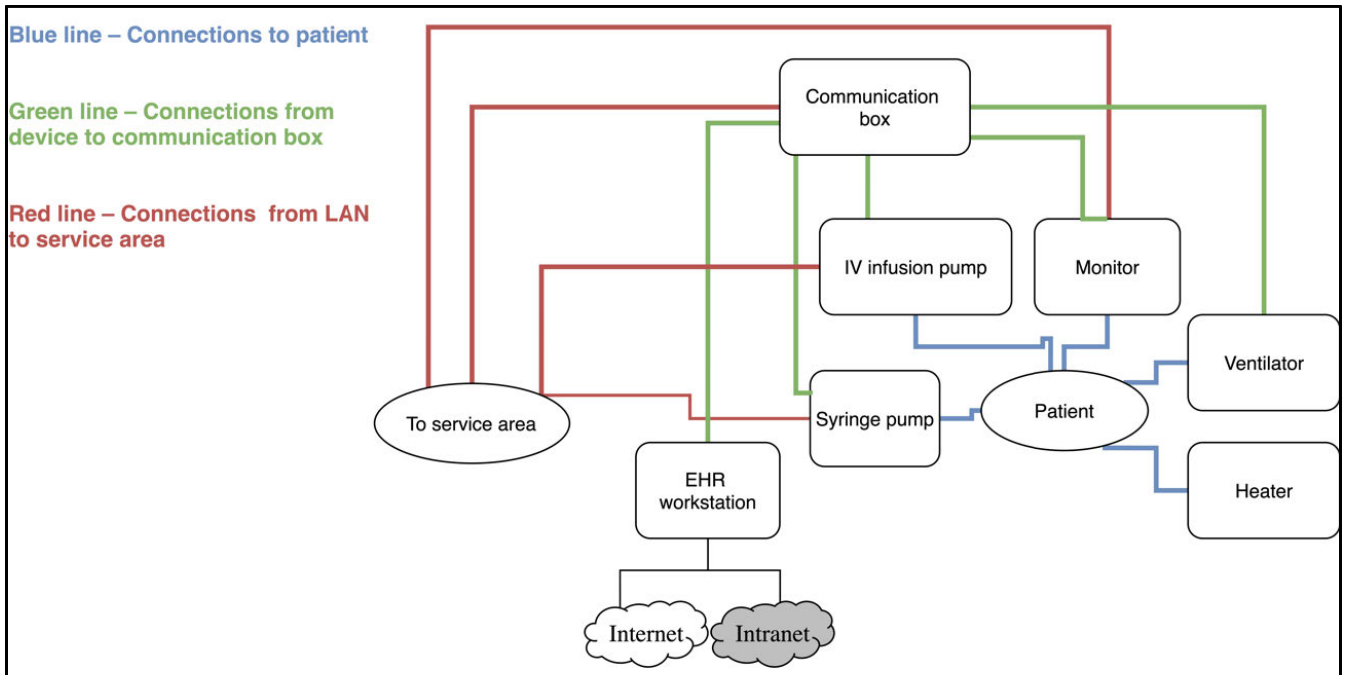


FIGURE 3.2. General structure of a patient’s room.

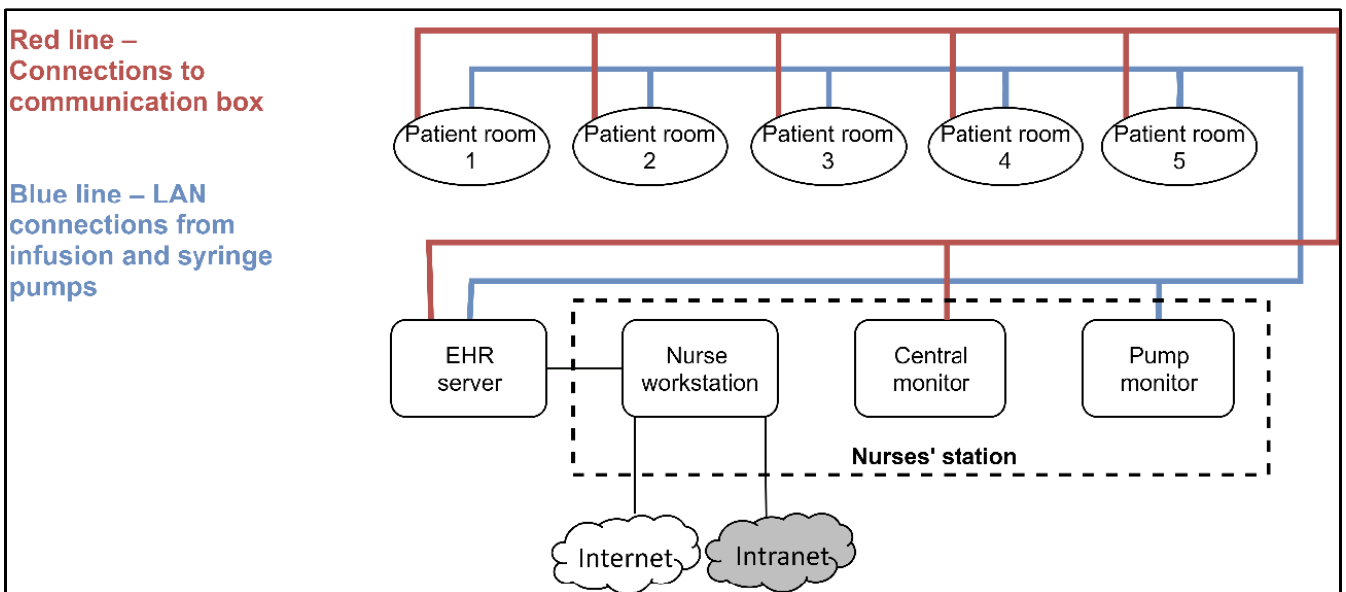


FIGURE 3.3. General structure of the nurses’ station.

of the interconnectivity between the devices, an attack on a single device will likely compromise additional devices. Based on the information presented in Table 3 which appears below, the most vulnerable devices in the patient’s room are the monitor, syringe pump, and IV infusion pump which are exposed to 56% of the possible attacks.

**E. NURSES’ STATION**

ICU nurses treat patients who suffer from acute conditions and are being cared for in a very structured and controlled

setting. In order to treat the most critical patients in the most thorough manner, critical care nurses use their specialized skills and extensive knowledge of disease pathology to provide interventions that sustain life. ICUs nurses are required to work quickly, efficiently, and meticulously. Most ICU patients are intubated, ventilated, and treated with life-sustaining medication. The nurses work closely with doctors in order to provide appropriate treatment for the patients. Among other things, they are responsible for documentation, providing medications, and monitoring the

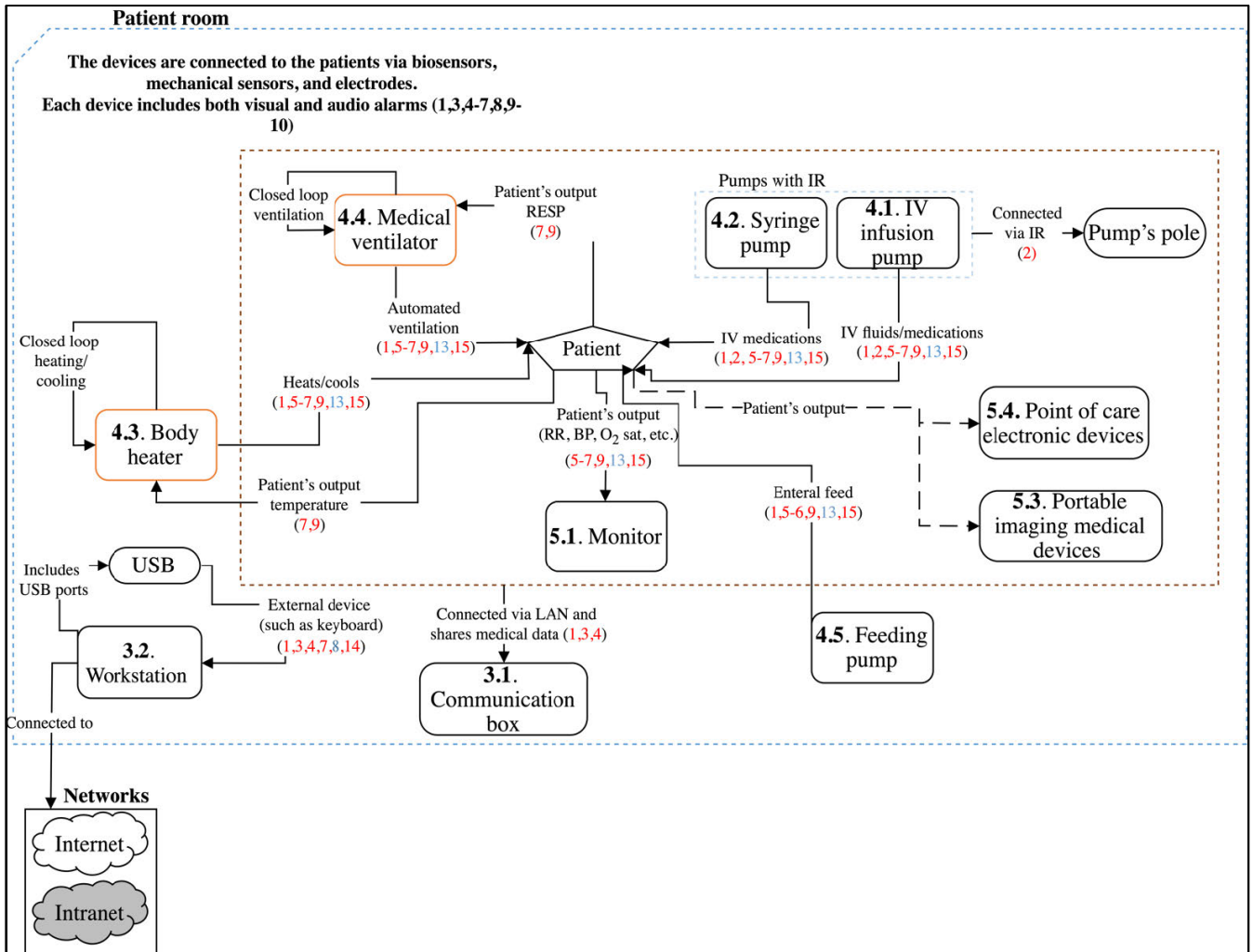


FIGURE 3.4. Ecosystem of the patient's room.

patient's condition, most of these responsibilities are based on nurse's interaction with the ICUMDs. Figure 3.5 describes the nurses' station ecosystem. As the diagram indicates, there are two display systems located in the nurses' station: a central monitoring station and a pump monitoring system. These two ICUMDs help the nurses monitor and control the patient's condition. Another important device located in the nurses' station is the EHR server where the patients' EHRs are stored. As can be seen in the figure, denial-of-service, man-in-the-middle, and configuration manipulation are the most common attacks targeting devices in the nurses' station. The most vulnerable devices in the nurses' station are the central monitoring station, the pump monitoring system, and the workstation, which are exposed to 63% of the possible attacks.

**F. DOCTOR'S ROOM**

An ICU doctor is responsible for the treatment of extremely ill patients who usually suffer from multiple organ failure.

Therefore, the doctor is expected to recognize a wide range of medical problems and provide appropriate treatment. Because the patient's medical condition is often unstable, the doctor is required to respond in a short amount of time, and his/her decisions rely heavily on the information provided by ICUMDs. Figure 3.6 describes the doctor's room ecosystem. The only vulnerable device in this room is the workstation, which is exposed to 63% of the possible attacks.

**G. ICU (INCLUDING ITS ROOMS)**

Figure 3.7 presents the overall ecosystem of the ICU, including the flow of information and interactions between the different medical devices and the various factors in the ICU. The diagram illustrates the enormous complexity of the ICU which includes devices that communicate with other devices, some of which operate autonomously based on the information they receive from other devices. As can be seen in the figure, denial-of-service, delay attacks, and configuration manipulation are the most common attacks targeting

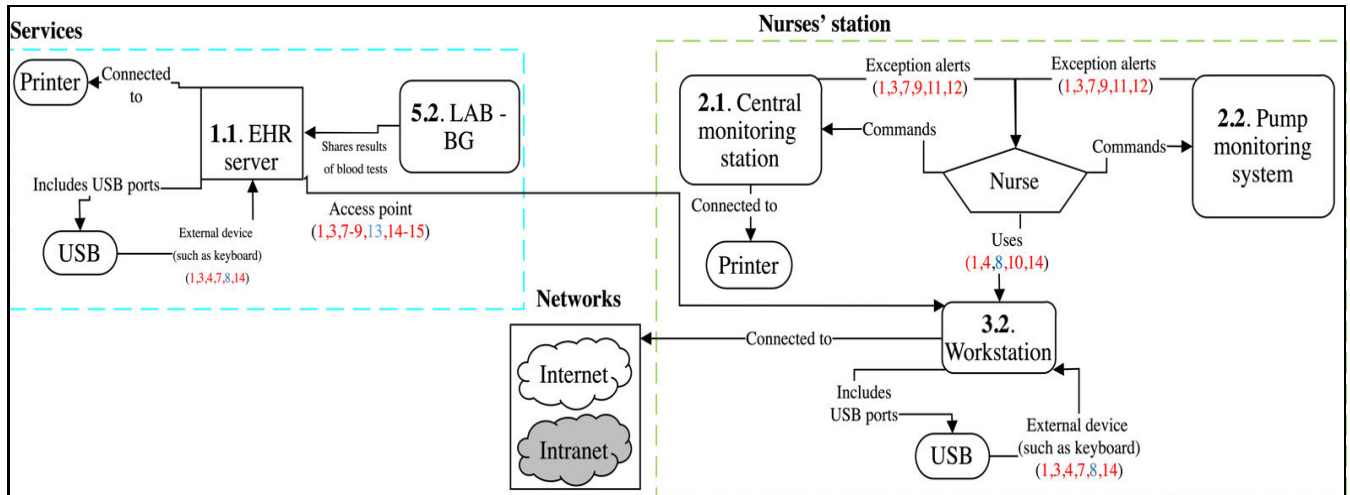


FIGURE 3.5. Ecosystem of the nurses' station.

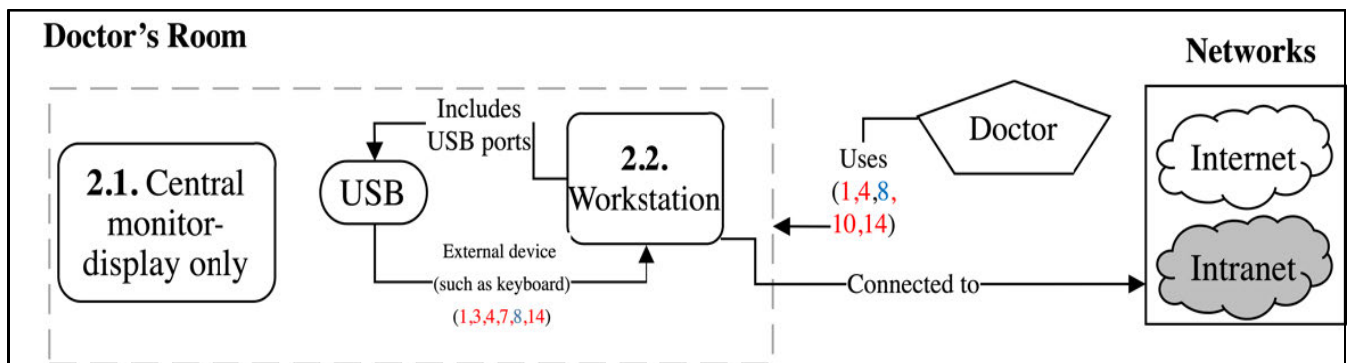


FIGURE 3.6. Ecosystem in doctor's room.

the devices in the ICU. The most vulnerable devices in the ICU are the central monitoring station, the pump monitoring system, and the workstations, which are exposed to 63% of the possible attacks.

#### IV. ATTACKS AND SECURITY MECHANISMS

##### 1) CYBER-ATTACKS AIMED AT ICUMDs

In this section, we present 16 different cyber-attacks aimed at the 19 ICUMDs discussed in this paper, including existing and new attacks. We start with a table that summarizes the information presented in this section and maps the attacks (see Table 3) and the ICUMDs exposed or vulnerable to each attack. In addition, we provide a breakdown of the attacks, presenting the building blocks for each attack; this breakdown allows us to identify the components and functionalities that serve as weak links in the ICU ecosystem and will enable researchers to focus their efforts on the development of appropriate security mechanisms in the future. Finally, we provide a detailed description of each of the 16 attacks. Some of the attacks are known attacks in the medical field, and others are attacks that were shown to be effective in

other domains which we've adapted to the ICUMD domain. References are included for each of the existing attacks. The table can be used to identify the most common attacks and most vulnerable devices. As can be seen, the most common attacks are configuration manipulation, delay attacks, and denial-of-service, all of which can affect all of the ICUMDs. In addition, the table shows that the most vulnerable devices are the central monitoring station, the pump monitoring system, and the workstation, which are each exposed to 63% of the presented attacks; for more devices see Figure 4 below. Moreover, for each attack we indicate whether the attack affects a single ICU patient or several patients, and our results show that 81% of the attacks endanger a single patient, while more than 93% of the attacks endanger several ICU patients. Lastly, we analyzed the impact of the attack on the medical team and found that more than 68% of the attacks also reduce the medical team's functionality, and consequently reduce the team's ability to provide the needed treatment to the patients. In addition, we include a qualitative comparative indicator in Table 3, column "CIA", where we identify the security principle of the CIA triad [78] that was compromised: confidentiality, integrity, or availability. As presented

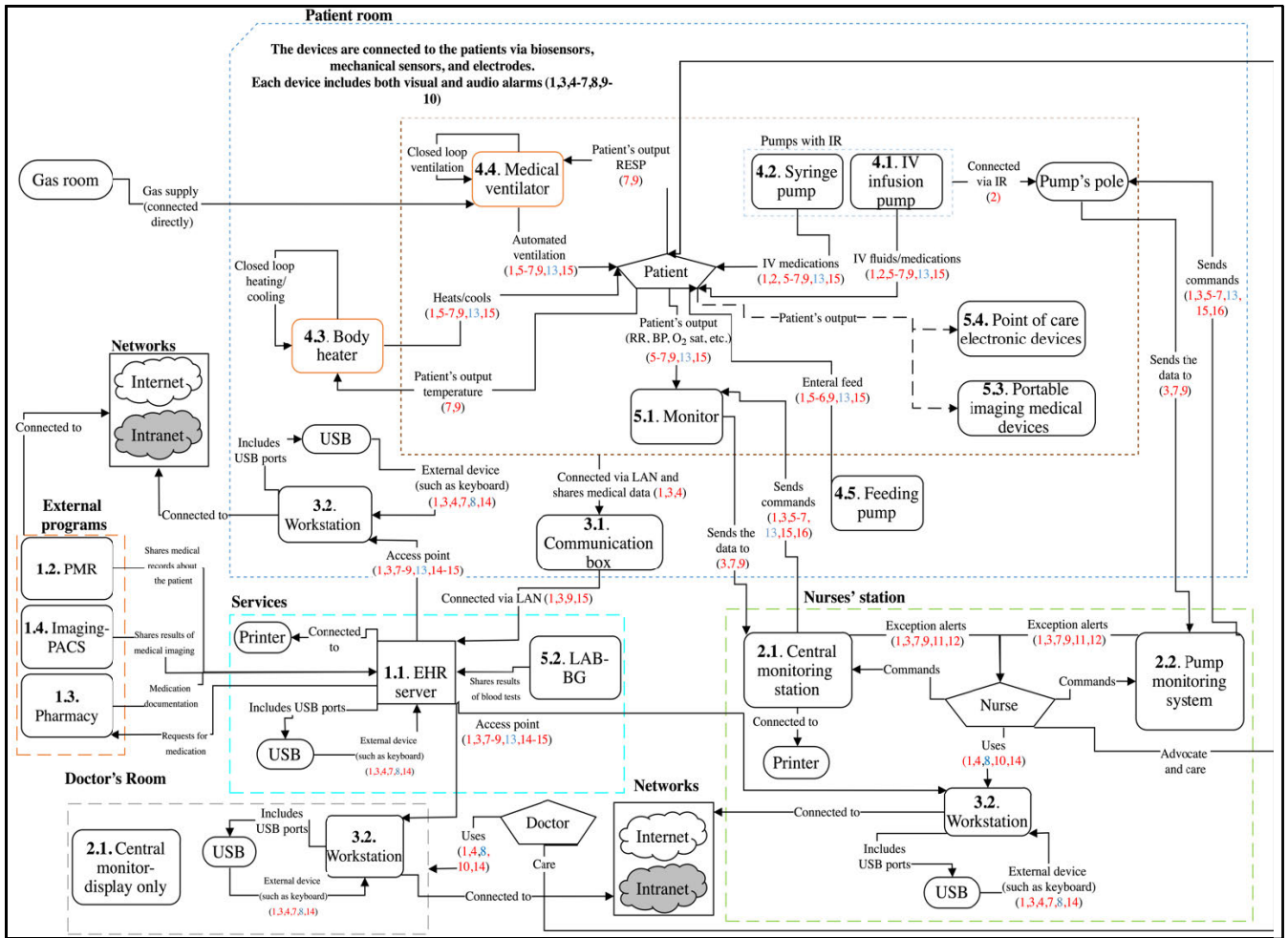


FIGURE 3.7. Overall ecosystem of the ICU.

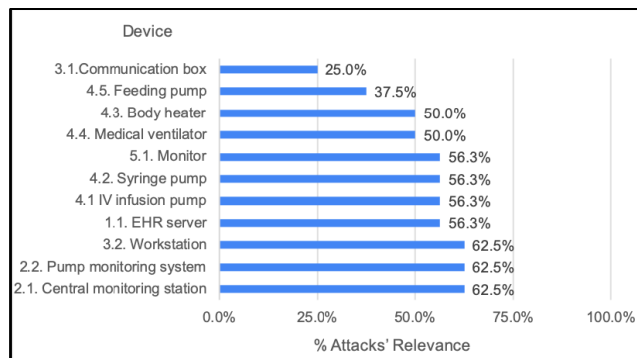


FIGURE 4. Percentage of attacks' relevance per ICUMD.

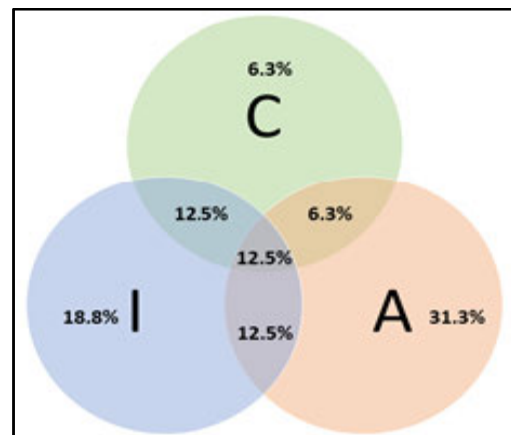


FIGURE 5. Distribution of the compromised security principles among the attacks we presented.

in the table below, confidentiality is compromised in 38% of the attacks, integrity is compromised in 56% of the attacks, and availability is compromised in 63% of the attacks.

For a detailed description of the distribution of the compromised security principles per attack see Figure 5 below, where 'C' stands for confidentiality, 'A' for availability, and 'I' for integrity.

*a: DETAILED DESCRIPTION OF THE CYBER-ATTACKS AIMED AT ICUMDs*

In this section, we provide a detailed description of each of the 16 attacks aimed at ICUMDs; a relevant reference

TABLE 3. Mapping the attacks and the devices they affect.

| Attack ID and Name  | Ref                                     | CIA     | Percent of vulnerable ICUMDs | Affects a specific patient directly | Affects several patients | Reduces the medical team's functionality | Devices         |                                 |                             |                        |                  |                      |                   |                  |                         |                   |              |
|---|---|---------|------------------------------|-------------------------------------|--------------------------|--|-----------------|---------------------------------|-----------------------------|------------------------|------------------|----------------------|-------------------|------------------|-------------------------|-------------------|--------------|
|   |   |         |                              |                                     |                          |  | 1.1. EHR Server | 2.1. Central monitoring station | 2.2. Pump monitoring system | 3.1. Communication box | 3.2. Workstation | 4.1 IV infusion pump | 4.2. Syringe pump | 4.3. Body heater | 4.4. Medical ventilator | 4.5. Feeding pump | 5.1. Monitor |
| 1) Denial-of-Service  | [4], [5], [23], [24], [41]              | A       | 100                          | V                                   | V                        | V  | V               | V                               | V                           | V                      | V                | V                    | V                 | V                | V                       | V                 | V            |
| 2) Electromagnetic Interference                                 | [6]                                     | I, A    | 18.2                         | V                                   | V                        |  |                 |                                 |                             |                        | V                | V                    |                   |                  |                         |                   |              |
| 3) Man-in-the-Middle  | [7], [12], [25], [26], [40], [41], [57] | C, I    | 90.9                         | V                                   | V                        |  | V               | V                               | V                           | V                      | V                | V                    | V                 | V                |                         |                   | V            |
| 4) Spyware  | [8], [9], [37], [58]                    | C       | 36.4                         | V                                   | V                        |  | V               | V                               | V                           |                        | V                |                      |                   |                  |                         |                   |              |
| 5) Alert Attack - Missing Alerts (devices)                      | [4]                                     | A       | 54.5                         | V                                   | V                        |  |                 |                                 |                             |                        | V                | V                    | V                 | V                | V                       | V                 | V            |
| 6) Alert Attack - False Alerts (devices)                        | [4]                                     | I       | 54.5                         | V                                   |                          | V  |                 |                                 |                             |                        | V                | V                    | V                 | V                | V                       | V                 | V            |
| 7) Data Manipulation  | [4], [39]                               | I       | 72.7                         | V                                   | V                        | V  | V               | V                               | V                           |                        | V                | V                    | V                 | V                |                         |                   | V            |
| 8) Ransomware   | [10], [11], [17], [31]                  | C, A    | 18.2                         | V                                   | V                        | V  | V               |                                 |                             |                        | V                |                      |                   |                  |                         |                   |              |
| 9) Delay Attack   | -                                       | A       | 100                          | V                                   | V                        |  | V               | V                               | V                           | V                      | V                | V                    | V                 | V                | V                       | V                 | V            |
| 10) Session Hijacking   | [12], [29], [30]                        | C, I    | 27.2                         | V                                   | V                        | V  |                 | V                               | V                           |                        | V                |                      |                   |                  |                         |                   |              |
| 11) Centralized Alert Attack - Missing Alerts (nurses' station) | -                                       | A       | 27.2                         | V                                   | V                        | V  |                 | V                               | V                           |                        | V                |                      |                   |                  |                         |                   |              |
| 12) Centralized Alert Attack - False Alerts (nurses' station)   | -                                       | I       | 27.2                         |                                     | V                        | V  |                 | V                               | V                           |                        | V                |                      |                   |                  |                         |                   |              |
| 13) Malicious Firmware update                                   | [13], [14]                              | C, I, A | 81.8                         | V                                   | V                        | V  | V               | V                               | V                           |                        | V                | V                    | V                 | V                | V                       | V                 | V            |
| 14) Cryptominer   | [15], [16]                              | A       | 18.2                         |                                     | V                        | V  | V               |                                 |                             |                        | V                |                      |                   |                  |                         |                   |              |
| 15) Configuration Manipulation                                  | -                                       | I, A    | 100                          | V                                   | V                        | V  | V               | V                               | V                           | V                      | V                | V                    | V                 | V                | V                       | V                 | V            |
| 16) Abuse of Legitimate Operations                              | -                                       | C, I, A | 9                            | V                                   | V                        | V  |                 |                                 |                             |                        |                  |                      |                   |                  |                         |                   | V            |
| Attacks' Relevance Percentage per ICUMD (%)                     |   |         |                              |                                     |                          |  | 56.3            | 62.5                            | 62.5                        | 25                     | 62.5             | 56.3                 | 56.3              | 50               | 50                      | 37.5              | 56.3         |

**TABLE 4. Denial-of-service attack.**

| Name                 | REF   | Year of publication |
|----------------------|---|---------------------|
| 1. Denial-of-service | [4], [5], [23], [24], [41]  | 1999                |
| Prerequisites        | A device with a USB port/infrared port/connection to the Internet or other vulnerable system  |                     |
| Scenario             | An attacker causes a device or service to be unavailable by sending multiple communication packets, thereby flooding and overloading the system. For example, an attacker can flood the workstation in the patient's room by sending multiple communication packets over the Internet; this might prevent the medical team from accessing the EHR, interfering with patient care. In this case, the medical team would have to revert to using paperwork which will be inefficient. |                     |
| Objective            | Harm the patient, interfere with the ability of the medical team to function  |                     |
| Vector               | Social engineering (human factor) techniques, insertion of infected USB, malicious email (for devices that are connected to the Internet), electromagnetic interference   |                     |
| Incident             | Note that such an attack has not been discussed in the ICU domain, but it has occurred in hospitals. <sup>10, 11</sup>  |                     |
| Implications         | Endangers the patient, affects the reliability and availability of the device, damages the reputation of the hospital and ICUMD vendor, financial repercussions   |                     |

**TABLE 5. Electromagnetic interference.**

| Name                            | REF   | Year of publication |
|---------------------------------|---|---------------------|
| 2. Electromagnetic interference | [6]   | 1994                |
| Prerequisites                   | A device with infrared ports  |                     |
| Scenario                        | An attacker emits disruptive radiation near a device which affects the availability or activity of the device. For example, an attacker can emit disruptive radiation near the syringe pump, which operates based on infrared radiation technology. As a result, pump's operation is disrupted, causing the wrong amount of medication to be injected. Thus, the patient would not receive the proper treatment (likely without the awareness of the medical team). |                     |
| Objective                       | Harm the patient  |                     |
| Vector                          | Disruptive radiation near the device  |                     |
| Incident                        | Such an attack has not been mentioned in the ICU domain.  |                     |
| Implications                    | Endangers the patient, affects the reliability and availability of the device   |                     |

from the literature is specified for each attack, including year of publication, the prerequisites needed for the attack to be conducted, a description of a scenario in which the attack can be carried out, and the objective of the attack. In addition, we include the attack vector by which the attack is initiated and the attack's implications. This information is presented below in Tables 4-19.

#### *i) DENIAL-OF-SERVICE (DoS)*

This attack prevents the functionality of a device or service (completely or partially) and affects its availability. There are generally two types of DoS attacks: attacks that cause the target system or service to crash and attacks that flood services (by sending too much traffic to the target system or service). The attack can damage various devices in the ICU. Since ICU patients are in an unstable state, a disruption in the proper functioning of a medical device can cause the patient's condition to deteriorate.

#### *ii) ELECTROMAGNETIC INTERFERENCE (EI)*

This attack uses electromagnetic radiation to disrupt the activity of various devices. Devices that operate with wireless infrastructure (e.g., infrared) may be affected by electromagnetic radiation in the environment; this radiation can disrupt

the device's normal operation. Some docking stations (e.g., syringe and IV infusion pumps) and monitors operate with an infrared infrastructure or have infrared ports, so these devices may be vulnerable to this attack.

#### *iii) MAN-IN-THE-MIDDLE (MITM)*

This attack occurs in the middle of two devices/systems that believe they are communicating directly with each other. This attack is used for sniffing, hijacking, injecting, or filtering data. In the ICU, this attack may act between two medical devices communicating with one another, causing the leakage of medical information or disruption of the delivery of medical instructions or information, which may harm the patient.

#### *iv) SPYWARE (PRIVACY VIOLATION) (S-PV)*

Spyware is a software that tries to access and use information about a person or organization (most of the time without their awareness or consent); spyware can also send the information obtained to another entity without the user's consent. Medical data is confidential; it can be misused in the wrong hands. For example, exposing medical details about a country's leaders may lead to political/security threats, extortion, and more.

<sup>10</sup><https://www.cso.com.au/article/608338/cyber-terrorism-final-frontier/>

<sup>11</sup><https://www.npr.org/sections/health-shots/2017/07/26/539290596/hospitals-face-growing-cybersecurity-threats>



**TABLE 6. Man-in-the-middle.**

| Name                 | REF  | Year of publication |
|----------------------|--|---------------------|
| 3. Man-in-the-middle | [7], [12], [25], [26], [40], [41], [57]  | 1981                |
| Prerequisites        | An insecure connection between two devices   |                     |
| Scenario             | An attacker secretly relays or alters the communication between two devices that assume they communicate with each other directly. The attacker can steal the data or change it, so the recipient doesn't receive the original (intended) data. In this case, the patient may not receive the proper treatment, since the medical information shared between devices is incorrect. For example, an attacker can send an email with an infected link to the nurses' workstation; the nurse then clicks on the link, allowing the attacker to obtain access to the nurses' workstation. The attacker can change the information transmitted between the EHR server and the workstation. The nurse receives incorrect medical information (e.g., measurements, treatment plan, medication doses). |                     |
| Objective            | Invasion of privacy, harm the patient  |                     |
| Vector               | Social engineering (human factor) techniques, insertion of infected USB, malicious email (for devices connected to the Internet)   |                     |
| Incident             | Such an attack has not been mentioned in the ICU domain.   |                     |
| Implications         | Invasion of privacy, affects the medical team's decision-making capabilities, affects the reliability and availability of the device   |                     |

**TABLE 7. Spyware (privacy violation).**

| Name                           | REF   | Year of publication |
|--------------------------------|---|---------------------|
| 4. Spyware (privacy violation) | [8], [9], [37], [58]  | 1995                |
| Prerequisites                  | A server or display system  |                     |
| Scenario                       | An attacker installs spyware on a system/server. Such spyware enables the attacker to steal medical and private information about the patient and his/her treatment. For example, an attacker can install spyware on the nurses' workstation by sending an email with an infected link connected to a malicious server. By installing such spyware, the attacker can steal the medical data of a VIP. This information can be used by the attacker to blackmail the patient or obtain a business/political advantage. |                     |
| Objective                      | Invasion of privacy   |                     |
| Vector                         | Social engineering (human factor) techniques, insertion of infected USB, malicious email (for devices connected to the Internet)  |                     |
| Incident                       | Such an attack has not been mentioned in the ICU domain, but it has occurred in hospitals. <sup>12</sup>  |                     |
| Implications                   | Invasion of privacy   |                     |

**v) ALERT ATTACK - MISSING ALERTS (DEVICES) (FA-MA)**

The multiplicity of devices in the ICU and the patient's instable state present the need for ongoing alerts regarding unusual medical events. Therefore, most therapeutic devices include audible and visual alerts (lights) to attract the attention of the medical team when needed. In this attack, the attacker interferes with the alarms of a device, thereby preventing the patient from receiving the medical team's attention in situations where it is needed.

**vi) ALERT ATTACK - FALSE ALERTS (DEVICES) (FA-AA)**

As described in the previous attack, ICUMDs include both audible and visual alerts. As known, the ICU medical team is under great stress due to the large number of extremely ill patients treated in the ICU. In this attack, the devices issue frequent false alerts. This may increase the stress of the medical team and cause confusion, which will impair the team's functioning. In addition, the team may ignore real alarms when the patient requires treatment, due to the large number of false alarms.

**vii) DATA MANIPULATION (DM)**

In this attack, the attacker aims to change the data pertaining to a particular ICUMD display or manipulate the data stored on a device. Various ICUMDs display and store medical data (e.g., measurements) collected about the patient; such data enables the medical team to deliver appropriate treatment (including the provision of medication, the use of other medical devices, etc.) The medical team makes decisions based on both real-time medical data and historical medical information about the patient (both of which may be stored on the device). In this attack, the information provided by the ICUMD is disrupted, and an incorrect picture of the patient's medical condition is provided.

**viii) RANSOMWARE (RW)**

A ransomware attack is an attack in which the attacker encrypts the data of the victim or causes a denial-of-service by locking the attacked systems. The attacker demands a ransom payment in order to restore the victim's access

<sup>12</sup><https://www.cso.com.au/article/608338/cyber-terrorism-final-frontier/>

**TABLE 8. Alert attack - missing alerts (devices).**

| Name                                       | REF   | Year of publication |
|--|---|---------------------|
| 5. Alert attack - missing alerts (devices) | [4]   | 2016                |
| Prerequisites                              | A device with an alert mechanism  |                     |
| Scenario                                   | An attacker can cause the device to fail to issue alerts when they are needed. In this case, the medical team will be unaware of the patient's condition, preventing the patient from receiving proper treatment. For example, an attacker can insert an infected USB (such as a keyboard) into the server of the central monitoring station in order to disable the monitor's alerts remotely. The patient's condition deteriorates, necessitating medical treatment (such as an electric shock). Because the patient's actual condition is unknown to the medical staff, the patient does not receive the treatment required. |                     |
| Objective                                  | Interfere with the medical team's ability to respond to a patient's medical needs   |                     |
| Vector                                     | Social engineering (human factor) techniques, insertion of infected USB, malicious email (for devices connected to the Internet), firmware updates  |                     |
| Incident                                   | Such an attack has not been mentioned in the ICU domain.  |                     |
| Implications                               | Endangers the patient, affects the reliability and availability of the device   |                     |

**TABLE 9. Alert attack - false alerts (devices).**

| Name                                     | REF   | Year of publication |
|--|---|---------------------|
| 6. Alert attack - false alerts (devices) | [4]   | 2016                |
| Prerequisites                            | A device with an alert mechanism  |                     |
| Scenario                                 | An attacker can cause a device to issue an alert when it is not needed. The sound of the alarms may frustrate the medical team, and over time this may cause them to ignore the alarms (e.g., they may fail to respond to a patient's deteriorating condition). For example, an attacker can utilize social engineering techniques in order to encourage someone to insert an infected USB (such as a keyboard) into the server of the central monitoring station; this will enable the attacker to change the required threshold for alerts, so the monitor's alerts are triggered frequently. |                     |
| Objective                                | Interfere with the ability of the medical team to function, harm the patient  |                     |
| Vector                                   | Social engineering (human factor) techniques, insertion of infected USB, malicious email (for devices connected to the Internet), firmware updates  |                     |
| Incident                                 | Such an attack has not been mentioned in the ICU domain.  |                     |
| Implications                             | Endangers the patient, affects the reliability and availability of the device   |                     |

**TABLE 10. Data manipulation.**

| Name                 | REF   | Year of publication |
|----------------------|---|---------------------|
| 7. Data manipulation | [4], [39]   | 2013 <sup>13</sup>  |
| Prerequisites        | A device which collects, stores, transfers, or displays patient data  |                     |
| Scenario             | An attacker can change existing data, so the patient's medical condition will be displayed incorrectly on the device. The fact that the patient is in critical condition and often without the ability to communicate causes the medical team to rely heavily on the medical data provided and stored on ICUMDs. Data manipulation may cause the medical team to make the wrong decisions or provide the wrong treatment. For example, an attacker can influence a nurse, encouraging the nurse to insert an infected computer mouse into the server of the central monitoring station. The attacker can then change the data that comes from the monitor and display other information on the central monitoring station (e.g., different heart rate measurements). Therefore, the medical team misunderstands the patient's condition and fails to provide the correct medical treatment. |                     |
| Objective            | Harm the patient, mislead the medical team  |                     |
| Vector               | Email/phishing, firmware updates, insertion of infected USB   |                     |
| Incident             | Such an attack has not been mentioned in the ICU domain.  |                     |
| Implications         | Endangers the patient, affects the reliability and availability of the device (mainly from the medical team's point of view)  |                     |

by decrypting the data or unlocking the system. In recent years, ransomware attacks have become widespread and have spread to the medical field; for example, WannaCry ransomware was used to attack many hospitals in 2017 [10], [17]. This attack may prevent the medical team from using various

medical devices and interfere with their ability to access a patient's EHR.

<sup>13</sup><https://www.cloudmask.com/blog/is-data-manipulation-the-next-step-in-cybercrime>

TABLE 11. Ransomware.

| Name          | REF   | Year of publication |
|---------------|---|---------------------|
| 8. Ransomware | [10], [11], [17], [31]  | 2009                |
| Prerequisites | An ICUMD that has an operating system into which ransomware malware can be injected (e.g., via a USB, Wi-Fi, Internet connection)   |                     |
| Scenario      | An attacker can use ransomware for financial gain. The attacker may publish the patient’s personal information, encrypt data, or prevent access to critical patient information. In these scenarios, the medical team would have incomplete (or no) information about the medical state of the patient. The patient may then receive improper treatment. Knowledge of the attack could cause the medical team to panic. For example, an attacker can install ransomware (by sending an infected email to the nurses' workstation). This would allow the attacker to disable the workstation in a patient’s room, preventing the medical team from accessing the patient’s EHR and causing them to provide improper treatment to the patient. The medical team would also have to revert to using paperwork which will be inefficient. |                     |
| Objective     | Harm the patient, mislead the medical team  |                     |
| Vector        | Malicious email attachments and links, malicious USB device, firmware update via Wi-Fi  |                     |
| Incident      | 1. In February 2016, the medical team at a Los Angeles hospital could not access their computers (including emails and electronic records) as a result of a ransomware attack. The attacker demanded a ransom of \$3.4 million [31].<br>2. In May 2017, 48 hospitals in the United Kingdom were attacked by WannaCry ransomware. <sup>14, 15</sup> The medical team was unable to access medical records; therefore, the treatments’ availability was limited.  |                     |
| Implications  | Endangers the patient, invasion of privacy, interferes with the medical team’s functioning, financial repercussions to the hospital   |                     |

TABLE 12. Delay attack.

| Name            | REF   | Year of publication |
|-----------------|---|---------------------|
| 9. Delay attack | -   | -                   |
| Prerequisites   | A device which generates important and continuous online medical data   |                     |
| Scenario        | <p>An attacker delays the transmission of data to medical devices or online displays. Most of the devices in the ICU require continuous and real-time data, so the medical team can monitor the patient’s condition and provide him/her appropriate and timely treatment. A delay in data transmission will affect the relevance of the data; this may cause the medical team to make the wrong decisions or provide the wrong treatment. For example, each patient’s ventilator has alarms which are set by the medical team (e.g., the length of time a ventilator allows a patient not to spontaneously breathe before the ventilator issues an alert signifying apnea and generates a mechanical breath). An attacker can use a firmware update to change the settings of the ventilator monitor, for example, delaying the monitor's alarms; in this case a patient that fails to breathe spontaneously will not receive a mechanical breath, and the ventilator will not issue an alert indicating apnea. As a result, the medical team does not receive real-time alerts, and the medical treatment will be delayed. Such a delay in the ICU can cause the patient to deteriorate, since the patient's condition is unstable.</p> <p>The main difference between this attack and a DoS attack is that during a delay attack the data keeps on flowing continuously, but the data becomes irrelevant and outdated in terms of a real-time system. Data that is received at an incorrect time becomes incorrect or misleading to a real-time system (such as ICUMDs) and can put the patient in danger. The attack has already been observed in the field of real-time pricing in smart grids, where attackers used a delay attack in order to present old prices to the smart meters [76]. In the medical domain, such a delay increases the risk to the patient (for example, in case of a heart attack) [77].</p> |                     |
| Objective       | Harm the patient, interfere with the efficiency of the medical team   |                     |
| Vector          | Malicious email attachments and links, firmware update  |                     |
| Incident        | Such an attack has never occurred.  |                     |
| Implications    | Endangers the patient, affects the reliability and availability of the device (the devices would no longer be reliable/useful)  |                     |

ix) DELAY ATTACK (DATK)

A delay attack, in the cyber-security context, is an attack that causes a delay in transmitting data or commands from one part of a system to another. The attack becomes significant when real-time medical data or clinical commands are involved. The condition of ICU patients requires continuous online monitoring of a variety of measurements, and thus full functioning of the ICUMDs is vital. Therefore,

such a delay may cause irreversible damage to the patient’s condition.

<sup>14</sup><https://www.cisecurity.org/ransomware-in-the-healthcare-sector/>

<sup>15</sup><https://www.cyberrisk.biz/healthcare-cyber-attacks-hospitals-critical-unit-cyber-threat/>

**TABLE 13. Session hijacking.**

| Name                  | REF  | Year of publication |
|-----------------------|--|---------------------|
| 10. Session hijacking | [12], [29], [30]   | 2001                |
| Prerequisites         | A device that maintains and supports sessions  |                     |
| Scenario              | An attacker uses an existing session between devices in order to gain unauthorized access to information in a computer system. In this case, the attacker can send malicious commands, steal medical data, etc. For example, an attacker can use an existing session between the workstation and the EHR server by sending an email with malicious link to the nurses' workstation. The attacker has full access to the medical data of patients by taking control of the session. The attacker can also use this access to change existing orders (such as prescriptions) and therefore harm the patient. |                     |
| Objective             | Harm the patient, invasion of privacy  |                     |
| Vector                | Malicious emails (with malicious files/links), packet sniffing (cookie thefts)   |                     |
| Incident              | Such an attack has not been mentioned in the ICU domain.   |                     |
| Implications          | Endangers the patient, invasion of privacy, financial repercussions to the hospital (severe fines [51])  |                     |

**TABLE 14. Centralized alert attack - missing alerts (nurses' station).**

| Name  | REF   | Year of publication |
|---|---|---------------------|
| 11. Centralized alert attack - missing alerts (nurses' station) | -   | -                   |
| Prerequisites   | A monitor/pump display in the nurses' station   |                     |
| Scenario  | An attacker can cause the central monitoring station and the pump monitoring system to fail at detecting and issuing alarms (both visual and audible). In this case, the patient may not receive proper treatment since the nurses at the nurses' station won't be aware of the patient's condition. For example, an attacker can use social engineering to encourage a nurse to insert an infected USB (such as a keyboard) into the server of the central monitoring station; then the attacker can turn off the monitor's alerts on the display system. The patient's condition can deteriorate to the point that he/she requires additional medical treatment (e.g., cardioversion in the case of arrhythmia). The nurses at the nurses' station won't receive alerts and are therefore unaware of the patient's needs. Thus, the patient won't get the required treatment. |                     |
| Objective   | Harm the patient  |                     |
| Vector  | Social engineering (human factor) techniques, insertion of infected USB, malicious email/phishing (for devices connected to the Internet)   |                     |
| Incident  | Such an attack has never occurred.  |                     |
| Implications  | Endangers the patient, affects the reliability and availability of the device (the displays would no longer be reliable), damages the reputation of the hospital  |                     |

*x) SESSION HIJACKING (SHKNG)*

Each session between a user and the server has a unique ID, a session ID, which is usually saved to cookies or connection tables, and sometimes is transmitted through the URL. In this attack, an attacker uses an existing session to communicate with the server using the identity of the victim. The attacker can use this attack in the ICU in order to steal a session between the nurses' station and the server, allowing the attacker to view medical data and change medical orders that may harm the patient.

*xi) CENTRALIZED ALERT ATTACK - MISSING ALERTS (nurses' STATION)*

In addition to the alarms of each of the ICUMDs themselves, there is a centralized alert system located at the nurses' station that enables the nurses to follow the patient's condition by both audible and vocal alarms, and respond if necessary. The large number of patients hospitalized in the ICU, as well as the continuous presence of nurses at the nurses' station, which is located a distance away from the patients' beds, demands constant and reliable monitoring, and sensitive alarms. As part of this attack, alarms are not issued at the nurses' station when necessary. Such an attack will prevent

the nurses from responding to the patient's needs in time and harm the patient as a result. This can be combined with an attack that mutes a patient's bedside alarms for the various devices connected to the patient, further endangering the patient.

*xii) CENTRALIZED ALERT ATTACK - FALSE ALERTS (nurses' STATION)*

Similar to the previous attack, in this attack false alarms are displayed at the nurses' station. These false alarms may exhaust the medical team's resources and lead to a high level of pressure among the medical team. In addition, the medical team may ignore true alarms due to a large number of false alarms, so the patient might receive a delayed (or no) response from the medical team.

*xiii) MALICIOUS FIRMWARE UPDATE*

Firmware is software that defines the activity of a hardware component. A firmware update [54], also known as a device firmware upgrade (DFU), is a legitimate process supported by a variety of devices; such updates are very common among devices with a USB socket [53]. During the update, the host receives the updated firmware version; this can only be done

**TABLE 15. Centralized alert attack - false alerts (nurses' station).**

| Name  | REF   | Year of publication |
|---|---|---------------------|
| 12. Centralized alert attack - false alerts (nurses' station) | -   | -                   |
| Prerequisites   | A monitor/ pump display in the nurses' station  |                     |
| Scenario  | An attacker can cause the displays to issue alerts (both visual and audible alarms) when they are not needed. The sound or display of the false alarms may frustrate the nurses at the nurses' station. Nurses may also ignore the alarms, causing them to fail to respond to a patient when treatment is required. For example, an attacker can use social engineering to encourage a nurse to insert an infected USB (such as a keyboard) to the centralized monitoring server; then the attacker can cause alarms to be triggered continuously in the nurses' station. This may cause the nurses' concentration to decrease and affect their ability to function. In addition, the nurses may assume that all of the alarms are false alarms and therefore fail to check the condition of the patients when an alarm is issued (thus, if this isn't a false alarm, the patient will not receive the required treatment). |                     |
| Objective   | Harm the patient  |                     |
| Vector  | Social engineering (human factor) techniques, insertion of infected USB, malicious email/phishing (for devices connected to the Internet)   |                     |
| Incident  | Such an attack has never occurred.  |                     |
| Implications  | Endangers the patient, affects the reliability and availability of the device   |                     |

**TABLE 16. Malicious firmware update.**

| Name                          | REF  | Year of publication |
|-------------------------------|--|---------------------|
| 13. Malicious firmware update | [13], [14]   | 2013                |
| Prerequisites                 | A device that includes firmware, a USB connection, or Wi-Fi for transferring the malicious firmware  |                     |
| Scenario                      | An attacker can install a malicious firmware update in order to change default commands or settings, so the device will perform different actions than those required. For example, an attacker can impersonate a software company and send a malicious firmware update of the syringe pump to the hospital IT department, as part of a routine process. The attacker can use the update to change the pump's measurement scale (e.g., to change the command to administer one drop to the patient to 1.5 drops). The patient will thus receive too much medication, causing the patient's condition to deteriorate. |                     |
| Objective                     | Harm the patient   |                     |
| Vector                        | Social engineering (the attacker impersonates the software company)  |                     |
| Incident                      | In June 2019, researchers from CyberMDX, a healthcare security firm, found that attackers could install malicious firmware on a pump's on-board computer, enabling them to obtain full control of the infusion pumps (allowing them to adjust the infusion rate). <sup>16</sup>  |                     |
| Implications                  | Endangers the patient, affects the reliability and availability of the device  |                     |

if the device's original firmware supports DFU, as described in [53]. The moment such a device is connected to a host with access to maliciously modified firmware, that malicious version of the firmware can be used during the DFU process, and thus the device will become a malicious device. Attackers can obtain a patched version of the firmware by reverse engineering the firmware software, as described by [52]. Legitimate and benign DFU processes are usually offered by the device manufacturer, and the actual update can be performed by the user or a technician (on behalf of the company). In this attack, the attacker runs a malicious firmware update on the device; this update defines additional actions that are not included as part of the intended operation of the device or otherwise interferes with the intended operation of the device. The user may find it difficult to identify the harmful updates because doing so requires advanced technical knowledge.

<sup>16</sup><https://techcrunch.com/2019/06/13/alaris-infusion-pump-security-flaws/>

#### xiv) CRYPTOMINER

Virtual currencies such as MBitcoin [56] have become very common in recent years. Virtual coins are based on blockchain technology [59], a kind of command book that exists in a distributed way in the cloud and manage transactions. Blockchain allows distributed transfers; encryption is used for security and to prevent counterfeiting. Encryption (and decryption for transactional validation) requires the formulation and resolution of complex mathematical equations, which requires considerable computational power. In order to encourage users to contribute their computer for the computing process, these computers receive virtual currencies in return (this process is called cryptocurrency mining). The mining process requires a server and an Internet connection; this process might cause the server to slow down or overheat, etc. In this attack, an attacker uses the server in order to mine virtual coins and therefore harm the server. The cryptojacking [55] of powerful organizational servers has recently become quite popular. Therefore, it is only a matter of time before the

TABLE 17. Cryptominer.

| Name            | REF  | Year of publication |
|-----------------|--|---------------------|
| 14. Cryptominer | [15], [16]   | 2017                |
| Prerequisites   | A server with an Internet connection   |                     |
| Scenario        | An attacker can use the server in order to mine cryptocurrency. The mining may impair system performance and cause high power consumption. For example, an attacker can send a link to a malicious Web page (via email). Then a nurse may click on the link, causing a cryptomining malware to run on the computer. The system’s performance is reduced and the high power consumption interferes with the nurse's work. |                     |
| Objective       | Damage the medical devices (which may harm the patient), cause financial repercussions   |                     |
| Vector          | Cryptojacking (code hosted on Web applications), social engineering (penetration of malware cryptomining) <sup>17</sup>  |                     |
| Incident        | Such an attack has not been mentioned in the ICU domain.   |                     |
| Implications    | Financial repercussions to the hospital, compromises the performance of the hospital’s IT services (particularly in the ICU), affects the reliability and availability of the device, endangers the patient  |                     |

first cryptominers hit medical devices in hospitals, and more particularly, ICUMDs. Note that cryptojacking attacks can also be initiated via Web browsers and do not require malware resident on the attacked host itself, making it much easier to utilize social engineering techniques to encourage the medical team to open a malicious website, in order to exhaust the ICU’s computational resources and mine cryptocurrencies on behalf of the attacker.

xv) CONFIGURATION MANIPULATION

In this attack, an attacker manipulates the settings of the target device/application, which affects the behavior of that device/application. The attacker changes legitimate settings (existing in the system) in a way that compromises the desired operation of the system. As part of this attack, the attacker may also change different measurements in the device. This change can be made by manipulating the measurements (e.g., an addition or subtraction change in the measurement scale). Changes in the measurements can disrupt medical activity in two ways:

1. The measurement data presented by the ICUMD might be incorrect and therefore will lead to incorrect decision-making by the medical team.
2. The internal data measurement of the devices may vary. In this case, different orders that the device receives (e.g., drug dosage) will be incorrectly translated by the device, so the patient will not receive proper care. In the ICU, the attack may cause the disruption of various devices, so that the functioning of the devices will be impaired. Such a fault can make it difficult for the medical team to function and may interfere with the treatment provided to patients.

xvi) ABUSE OF LEGITIMATE OPERATIONS

In this attack, an attacker sends commands to the system in order to execute legitimate operations, meaning that the attacker causes a certain device to perform an action. As a result, the device will perform actions that the medical team is unaware of (a covert attack), and by that, the patient may

receive treatment that is not needed or fail to receive required treatment.

b: ATTACK BUILDING BLOCKS

In this section, we present 19 attack building blocks (ABBs) for the implementation of the various attacks. A building block is an essential part of the complete cyber-attack, required for carrying out the attack (meaning that in the absence of the building block, the attack could not be accomplished successfully). The definition of the building blocks and their association with various attacks constitutes the basis for future risk analysis. Table 20 lists the relevant building blocks for the attacks aimed at ICUMDs presented in this paper.

2) EXISTING SECURITY MECHANISMS

In this section, we present existing security mechanisms which are aimed at addressing, preventing, and detecting cyber-attacks and anomalies. Some of the existing security mechanisms are designed to be more general (e.g., for computerized systems), others are aimed at medical devices in general, and a few of them are designated for ICUMDs. After describing the security mechanisms, we present a table that summarizes the mechanisms, and maps the security mechanisms and their coverage against the attacks on ICUMDs presented in this paper. Before discussing the security mechanisms, one should note that in addition to security mechanisms, there are policies, regulations, and security measures that help organizations and hospitals take the best security actions and apply them within their organization. The Medical Device Innovation, Safety and Security Consortium (MDISS)<sup>18</sup> offers two services: 1) WHISTL – World Health Information Security Testing Lab facilities, which consist of a federated network of testing labs for medical device security. The goal of these labs is to help organizations tackle cyber-security challenges in the public health domain more effectively, focusing on testing multi-device critical care environments. 2) The HealthTrust Purchasing Group’s Pilot Program – The HealthTrust Purchasing Group is pioneering an

<sup>17</sup><https://jask.ai/cryptocoin-mining-attack/>

<sup>18</sup><https://www.mdiss.org/initiatives>

**TABLE 18. Configuration manipulation.**

| Name                           | REF   | Year of publication |
|--------------------------------|---|---------------------|
| 15. Configuration manipulation | -   | -                   |
| Prerequisites                  | A device with settings and configurations that can be adjusted by the medical team  |                     |
| Scenario                       | An attacker modifies/sets device settings without the medical team’s awareness, causing the device to operate differently than intended.<br>For example, an attacker can insert an infected USB (such as a computer mouse or keyboard) [72] into the server of the central monitoring station. The attacker can then change an existing setting in the monitor, e.g., change the upper/lower heart rate limits to more extreme values. As a result, the system does not issue alerts about changes in the heart rate that should be reported to the medical team. The medical team may not provide the patient with the necessary treatment because of a lack of reporting. |                     |
| Objective                      | Interfere with the ability of the medical team to function, harm the patient  |                     |
| Vector                         | Social engineering (human factor) techniques, insertion of infected USB, firmware update  |                     |
| Incident                       | Such an attack has never occurred.  |                     |
| Implications                   | Endangers the patient, affects the reliability and availability of the device, damages the reputation of the hospital and ICUMD vendor  |                     |

**TABLE 19. Abuse of legitimate operations.**

| Name                               | REF   | Year of publication |
|------------------------------------|---|---------------------|
| 16. Abuse of legitimate operations | -   | -                   |
| Prerequisites                      | A device that is operated by the medical team (e.g., central monitoring station/ medical ventilator)  |                     |
| Scenario                           | An attacker obtains access to a device (e.g., by influencing a member of the medical team to insert an infected USB into the device); then the attacker can send commands to the device without the medical team’s awareness.<br>For example, an attacker can insert an infected USB (such as a computer mouse or keyboard) [72] into the server of the central monitoring station and send "discharge" commands to the patient’s monitor. As a result, all of the saved data will be deleted, and the monitor turns off (meaning that it no longer is monitoring the patient’s state). |                     |
| Objective                          | Interfere with the ability of the medical team to function, harm the patient  |                     |
| Vector                             | Social engineering (human factor) techniques, insertion of infected USB, malicious email/with malicious file/link (for devices connected to the Internet), firmware update  |                     |
| Incident                           | Such an attack has never occurred.  |                     |
| Implications                       | Endangers the patient, affects the reliability and availability of the device   |                     |

initiative across its more than 1000 member hospitals to share cyber vulnerability information as a necessary element of their procurement process. In addition, the MDS<sup>2</sup> (Manufacturer Disclosure Statement for Medical Device Security),<sup>19</sup> which was established by the Healthcare Information and Management Systems Society (HIMSS) and the American College of Clinical Engineering (ACCE), is a platform that provides a comprehensive set of medical device security questions, allowing easy comparison of security features across different devices and manufacturers, and enabling the review of the large volume of security-related information.

As can be seen in this section, the existing security mechanisms provide just a partial and limited response to the attacks presented in this paper. There are attacks, such as malicious firmware updates, that are not mitigated by any of the existing security mechanisms. Earlier in the paper, we presented the

many dangerous implications of the attacks on a patient’s medical treatment and the dangers they pose to the smooth operation of the ICU and the medical devices that are so critical there.

As technology continues to advance and understanding of the advantages of using intelligent medical devices that communicate with each other, operate autonomously, and enable a wider range of functionality, the risks of implementing the attacks presented will increase, as does the need for sophisticated and advanced security mechanisms that will prevent and manage the attacks correctly.

*a: DYNAMIC PROTECTION USING CISCO CWS (2014)*

The author, a former CTO of Cisco Healthcare Solutions, suggested using Cisco’s Cloud Web Security [44] (Cisco CWS) in order to leverage big data and performance anomaly detection, behavioral analysis, evasion resistance, and rapid detection. This solution uses flow-based, signature-based,

<sup>19</sup><https://www.himss.org/resource/library/MDS2>

**TABLE 20.** Relevant building blocks.

| ABB # | Brief Description of the Attack Building Blocks (ABBs)  |
|-------|---|
| 1     | Ease of remotely connecting to the device   |
| 2     | Ease of sending data to the device  |
| 3     | Ease of being in physical proximity of the targeted device (not necessarily including physical access)  |
| 4     | Ease of having physical access  |
| 5     | Ease of manipulating the device's original software   |
| 6     | Ease of manipulating the device's configuration files   |
| 7     | Ease of disturbing the data flow through the communication channel used   |
| 8     | Ease of changing the content of the data transmitted over the communication channel   |
| 9     | Ease of changing the content of the metadata transmitted over the communication channel   |
| 10    | Ease of interfering with non-medical private information about the patient displayed or stored on/handled by the device   |
| 11    | Ease of interfering with medical information about the patient (e.g., information originating from medical device or its operation) which is stored or displayed on/handled by the device |
| 12    | Sensitivity of the device to external electromagnetic fields  |
| 13    | Ease of interfering with the device's alert system  |
| 14    | Ease of sniffing and collecting data via communication channels   |
| 15    | Ease of understanding the communicated data (e.g., encrypted, packed)   |
| 16    | Ease of misusing the device's security mechanisms   |
| 17    | Ease of misusing the device's safety mechanisms   |
| 18    | Ease of bypassing the user authentication mechanism   |
| 19    | Ease of evading the data integrity mechanism  |

behavior-based, and full packet capture models in order to identify threats. Cisco CWS enables continuous monitoring and analysis across the network and throughout the entire continuum of the attack - before, during, and after.

All inbound Web traffic to the healthcare organization is analyzed in real-time using context-aware scanning engines to identify and block untrusted domains. CWS identifies unknown or uncommon behavior through Cisco Outbreak



TABLE 21. Building blocks for each attack.

| Building Block Attack   | 1    | 2    | 3    | 4    | 5  | 6    | 7    | 8  | 9  | 10   | 11   | 12  | 13   | 14  | 15   | 16   | 17   | 18   | 19  | Attack's Complexity Based on ABBs (%) |
|---|------|------|------|------|----|------|------|----|----|------|------|-----|------|-----|------|------|------|------|-----|---------------------------------------|
| 1) Denial-of-Service  |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 31.6                                  |
| 2) Electromagnetic Interference                                 |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 10.5                                  |
| 3) Man-in-the-Middle  |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 36.8                                  |
| 4) Spyware  |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 36.8                                  |
| 5) Alert Attack - Missing Alerts (devices)                      |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 42.1                                  |
| 6) Alert Attack - False Alerts (devices)                        |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 42.1                                  |
| 7) Data Manipulation  |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 68.4                                  |
| 8) Ransomware   |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 31.6                                  |
| 9) Delay Attack   |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 31.6                                  |
| 10) Session Hijacking   |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 47.4                                  |
| 11) Centralized Alert Attack - Missing Alerts (nurses' station) |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 36.8                                  |
| 12) Centralized Alert Attack - False Alerts (nurses' station)   |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 36.8                                  |
| 13) Malicious Firmware Update                                   |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 42.1                                  |
| 14) Cryptominer   |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 26.3                                  |
| 15) Configuration Manipulation                                  |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 73.7                                  |
| 16) Abuse of Legitimate Operations                              |      |      |      |      |    |      |      |    |    |      |      |     |      |     |      |      |      |      |     | 31.6                                  |
| ABB's Frequency (%)   | 87.5 | 37.5 | 11.8 | 81.3 | 50 | 43.8 | 37.5 | 25 | 25 | 18.8 | 18.8 | 6.3 | 12.5 | 6.3 | 13.3 | 81.3 | 81.3 | 81.3 | 6.3 |                                       |

Intelligence, a heuristics-based engine that runs Web page components in a secure environment before enabling user access.

*b: gLite MIDDLEWARE (2009)*

Luna et al. [45] suggested using GLITE Middleware in order to implement a secure intensive care grid system, which captures, stores, and manages data and metadata from ICUs. The specific goal was to avoid data and metadata attacks (such as leakage, change, or destruction of data). The paper proposed building a cryptographic mechanism using a cryptographic

storage resource manager (CryptoSRM) service. CryptoSRM uses a cryptographic engine to encrypt and decrypt data that is stored in the local cache. The repository itself uses a fragmentation algorithm in order to ensure confidentiality and high availability of the cryptographic data.

*c: THREATS IDENTIFICATION AND ADAPTIVE SECURITY COUNTERMEASURES (2015)*

The authors discussed [46] the importance of using a dynamic security mechanism in the field of eHealth systems in order to identify attacks, such as privacy violation, denial-of-service,

data manipulation, man-in-the-middle, etc. The authors suggested using environmental sensors and system monitoring components in the devices, in order to explore security events in the internal and external environment. These events are then further analyzed by an analyzer function to identify whether the current event is a threat to a system. The planning function can use a knowledge base or learning mechanism to determine a new action from a set of existing actions. The action selected by a planning function is executed in order to return the system's behavior to a normal state.

*d: LIMITATION OF THE FUNCTIONALITY OF THE NETWORK INTERFACE (2011)*

An approach for reducing possible attacks is to limit some of the functionalities that are not vital for the patient's treatment. In [47], the authors claimed that in most cases, manufacturers choose to limit the device's functionality, so it can send out data, such as sensor readings or event logs, but not accept commands from the network. Although this approach improves the security of the system, it severely limits the ability to deploy closed loop scenarios, which can improve the treatment provided and reduce the medical team's workload.

*e: PROTECTING COMMUNICATION (2016)*

In [48], the authors presented a method of protecting communications within an integrated clinical environment (ICE) framework, where the devices interact with each other using the fine-grained security mechanisms which the OMG DDS Security specification provides. The authors offered two prototypes that respectively utilize secure transports (such as TLS/DTLS) and the DDS Security Architecture. In their research, they explained why transport-level security solutions may not provide enough protection against inside attacks.

*f: METRICS-DRIVEN SECURITY OBJECTIVE DECOMPOSITION (2013)*

In [49], the authors presented an adaptive security management model which is based on the monitor-analyze-adapt methodology in order to learn and adapt to changes in environmental dynamics and predict unknown threats. They provided security objective decomposition strategies aimed at the growth of security metrics. They also developed a context-aware Markov game theory model which helps to estimate and predict risk damages and adapt security decisions based on those estimates.

*g: CENTRALIZED MANAGEMENT OF MEDICAL BIG DATA IN THE ICU (2016)*

In [50], the authors suggested a method of centralized management (CM) of the medical big data environment in the ICU, which includes cyber infrastructure equipment. The cyber infrastructure is a cloud computing (CC) environment constructed according to security specifications. The CM is employed alongside the CC availability zones in order to ensure a high level of availability. These zones can be used as

a defensive mechanism against certain types of attacks (e.g., denial-of-service attacks). Moreover, in order to control and monitor the outbound and inbound traffic, the system uses virtual firewalls.

*h: PROMENADES (2013)*

This approach utilizes state-of-the-art security techniques from other industries (such as the financial sector) and incorporates them into prebuilt comprehensive solutions for protecting medical devices.

The techniques include:<sup>20</sup>

- 1) Using private/public key infrastructure in order to ensure secured authentication
- 2) Enabling communications over secure TLS tunnels only
- 3) Using encryption methods, such as RSA or elliptic-curve cryptography
- 4) Easy revocation of certificate in the case of a failure.
- 5) Keeping remote services secured and validating cloud updates

Suggested solutions:

Parlay – This is a combination of ready-made tools, libraries, and code bases designed specifically to secure medical devices. It exposes all of the software, so the system can be instrumented, tested, and tuned.

Parlay Cloud – This offers a cloud solution that meets the medical devices' needs. The system enables fast and secure collection of data from the devices and the execution of analytics on patient data and data from the devices. This analysis may help identify vulnerabilities and anomalous behavior.

*i: CYBER-NEXUS (2017)*

This is a two-layered security solution for existing medical ecosystems that enables secured communications and protection of any device.<sup>21</sup> The solution provides protection of each medical device individually, with an additional isolated security layer. The first layer connects each medical device to the existing network via a cyber-nexus secured device. Once this connection is established, the cyber-nexus device creates a secure connection directly to the second layer, which is a management unit that provides a strict policy for full protection of different levels and areas.

*j: SECURE MEDICAL DATA SHARING SCHEME BASED ON BLOCKCHAIN*

Cheng et al. [82] offered a solution that integrates blockchain [83] and clouds to securely share medical information between medical organizations (such as hospitals). Each hospital generates a hash of medical record M, encrypts it, and stores it in the cloud's storage. The authors suggested implementing a two-way authentication model for the communication between two entities; such a model avoids ove-

<sup>20</sup><https://promenadesoftware.com/cybersecurity>

<sup>21</sup><http://cyber-nexus.net/#what-is-cyber-nexus>

reliance on a trusted third party center and meets the security requirements for medical data as well.

*k: ENHANCING SECURITY AWARENESS AND RESPONSE AMONG ICU MEDICAL STAFF: RECOMMENDATIONS FOR NURSING EDUCATION AND REGULATION*

Realizing that human error, especially among nurses, can cause breaches in healthcare security, the authors [84] made recommendations for nursing education and regulation, for example, they suggested guidelines on how to deal with suspicious emails, how to manage password security, how to keep programs and systems up-to-date, how to work securely with ICUMDs, etc. Such regulations may reduce the potential attacks that can be initiated by social engineering techniques, which are commonly used by attackers.

*l: SECURING ELECTRONICS HEALTHCARE RECORDS: A BIOMETRIC-BASED APPROACH*

Hathaliya et al. [85] proposed a biometric-based authentication scheme to ensure secure access to the patient's EHR from any location. The solution is mainly aimed at securely accessing patients' EHRs remotely using mobile devices. We propose implementing such a solution in ICUs as well (each nurse and doctor will be requested to use a biometric authentication in order to access the EHR). The proposed secure biometric-based scheme consists of the following steps: Registration: First, the user provides his/her biometric identity, using a biometric reader. Based on the biometric identity, the system generates a secret key and stores it on the cloud server. Login and Authentication: The client logs in, using the Kerberos authentication [89] mechanism, with their biometric identifier, and a request for the service is sent to the authentication server. The cloud server verifies the biometric with the database of already registered biometrics.

Although not a security mechanism, **USB Port Access Mitigation (2006)** is an example of a policy that can be implemented in order to address and disable a vector that can serve as a gateway for launching many other attacks; note that on its own, USB port mitigation does provide hermetic protection from an attack. There are a few options for disabling USB port access, as the disabling process can either be done by using a physical blocking object that covers the USB socket, or alternatively by changing the system so that the USB socket is not enabled at the electronic circuit level. Either of these blocking approaches prevents the possibility of malware, viruses, and other attacks performed by inserting an infected USB. This mechanism, like many others, protects against a specific attack vector and does not offer hermetic protection from certain attacks; it only increases the difficulty of carrying out and launching an attack [70].

Tables 22 and 23 summarize the existing security mechanisms for each attack presented. The leftmost column lists the attacks, and the top row lists the security mechanisms. A black square indicates that the specific security mechanism prevents/deals with the attack. For example, security mechanisms 1, 3, 6, and 7 deal/prevent a denial-of-service attack.

## V. DISCUSSION AND CONCLUSION

Our primary goals in this study are to provide the reader with a comprehensive understanding regarding ICUMDs, and their sub-categories, ecosystems, and vulnerability to attacks (using the attack flow diagrams which show the attacks each ICUMD is exposed to and how), and to identify the security gaps between these attacks and existing security mechanisms.

We have provided a detailed description of the different ICUMDs and presented an ICUMD taxonomy, which categorizes the ICUMDs into five main categories, based on their main functionality and medical goal. In addition, we presented the interactions that exist between the different ICUMDs; in doing so, we found that 40% of the interactions between the devices are not trivial, which emphasizes the complexity and dependencies between the ICUMDs and implies that when connected to ICUMDs, patients' vulnerability increases. This finding demonstrates and emphasizes the necessity of securing ICUMDs.

Such understanding and information also establishes a foundation for the security enhancement of ICUMDs and can be used to assist ICUMD vendors, health service providers, and security companies in the process of developing and implementing essential security mechanisms for ICUMDs, taking the gaps we identified into consideration. These security mechanisms will allow society to benefit from the technological advancements and improved quality of treatment that ICUMDs provide, while mitigating the serious risks of cyber-attacks.

Our study also helps strengthen the weak link in any modern technological ecosystem, the human factor. Currently, many methods of social engineering are employed by attackers who take advantage of innocent users, which in our context can be patients, physicians, and even technicians. Such social engineering techniques can actually allow the attacker to evade existing security mechanisms by utilizing innocuous human intervention to launch the attack. Our attack flow diagrams show that in most ICUMDs, the doctor and nurses have an active role in the patient's treatment. Therefore, in this study we also hope to increase the medical team's awareness and knowledge, exposing team members to the potential risks and attacks associated with their ICUMDs; such exposure will likely result in more secured use of ICUMDs by the medical team, which will reduce the risk and probability of such attacks.

We began our study by providing a thorough and convenient taxonomy and extensive explanation of the most relevant and widely used ICUMDs.

According to our analysis, the most vulnerable devices are the central monitoring station, the pump monitoring system, and the workstation (each of which could be affected by 63% of the attacks) due to their widespread functionality, connectivity to numerous additional components, critical role in patient care, and their popularity. We also showed which of the CIA (confidentiality, integrity, and availability) triad security principles were compromised by each of the

**TABLE 22.** Existing security mechanisms and the year they were published.

| Security Mechanism ID and Name   |  |
|--|--|
| 1) Dynamic Protection using Cisco CWS (2014)                           | 7) Centralized Management of Medical Big Data in ICU (2016)  |
| 2) gLite Middleware (2009)   | 8) Promenades (2013)   |
| 3) Threats Identification and Adaptive Security Countermeasures (2015) | 9) Cyber-Nexus (2017)  |
| 4) Limitation of the Functionality of the Network Interface (2011)     | 10) Secure medical data sharing scheme based on blockchain (2020)  |
| 5) Protecting Communication (2016)                                     | 11) Enhancing security awareness and response among ICU medical staff: recommendations for nursing education and regulation (2020) |
| 6) Metrics-Driven Security Objective Decomposition (2013)              | 12) Securing electronic healthcare records: A biometric-based approach (2019)  |

**TABLE 23.** Existing security mechanisms and their ability to provide protection against the attacks presented.

| Attack  | 1    | 2    | 3    | 4    | 5    | 6    | 7    | 8    | 9    | 10   | 11   | 12   | Percentage of Security Mechanisms that Provide Protection Against the Attack |
|---|------|------|------|------|------|------|------|------|------|------|------|------|--|
| 1) Denial-of-Service  | ■    |      | ■    |      |      | ■    | ■    |      |      |      |      |      | 33.3   |
| 2) Electromagnetic Interference                                 |      |      |      |      |      |      |      |      |      |      |      |      | 0  |
| 3) Man-in-the-Middle  | ■    |      | ■    | ■    | ■    | ■    |      | ■    | ■    | ■    | ■    |      | 75   |
| 4) Spyware  | ■    | ■    | ■    | ■    | ■    | ■    | ■    | ■    |      | ■    | ■    | ■    | 91.7   |
| 5) Alert Attack - Missing Alerts (devices)                      |      |      |      |      |      |      |      |      |      |      | ■    |      | 8.3  |
| 6) Alert Attack - False Alerts (devices)                        |      |      |      |      |      |      |      |      |      |      | ■    |      | 8.3  |
| 7) Data Manipulation  | ■    | ■    | ■    |      |      | ■    |      |      |      | ■    | ■    |      | 50   |
| 8) Ransomware   |      |      |      |      |      |      |      |      |      |      | ■    |      | 8.3  |
| 9) Delay attack   | ■    |      |      |      |      |      |      |      |      |      |      |      | 8.3  |
| 10) Session Hijacking   | ■    |      |      |      | ■    | ■    | ■    | ■    | ■    |      |      | ■    | 58.3   |
| 11) Centralized Alert Attack - Missing Alerts (nurses' station) |      |      |      |      |      |      |      |      |      |      |      |      | 0  |
| 12) Centralized Alert Attack - False Alerts (nurses' station)   |      |      |      |      |      |      |      |      |      |      |      |      | 0  |
| 13) Malicious Firmware Update                                   |      |      |      |      |      |      |      |      |      |      | ■    |      | 8.3  |
| 14) Cryptominer   | ■    |      |      |      |      |      |      |      |      |      |      |      | 8.3  |
| 15) Configuration Manipulation                                  |      |      |      |      |      |      |      |      |      |      | ■    |      | 8.3  |
| 16) Abuse of Legitimate Operations                              |      |      |      |      |      |      |      |      |      |      | ■    |      | 8.3  |
| Percentage of Attacks Addressed by the Security Mechanism       | 43.8 | 12.5 | 18.8 | 12.5 | 18.8 | 31.3 | 18.8 | 18.8 | 12.5 | 18.8 | 56.3 | 12.5 |  |

attacks presented in our study. As seen, confidentiality is compromised in 38% of the attacks, integrity is compromised in 56% of the attacks, and availability is compromised in 63% of the attacks. Based on the high reliance of ICU patients on ICUMDs, this finding shows that enhancing the security of ICMUDs will directly improve patients' security and healthcare.

We presented "building blocks," the components of a cyber-attack that are essential for carrying out the attack. We mapped the building blocks that are essential for carrying

out each of the attacks presented in this paper; by doing so, we observed that ABB number 1 (Ease of remotely connecting to the device) is a key building block that affects 88% of the attacks. In addition, the most complex attack is attack number 15 (configuration manipulation) which includes 74% of the building blocks.

We described each of the potential attacks aimed at ICUMDs in great detail. This information was presented in an attack-ID table for each of the attacks, which included important characteristics of the attack, such as prerequisites

for launching the attack, the attack vector, and objectives, and an example of a scenario by which the attack could be carried out.

We presume that new and evolved attacks will be formed which have not yet been employed or suggested, as this is the nature of the dynamic cyber security domain.

Thus, we also assessed and reviewed all nine of the ICUMD security mechanisms that were developed and published since 2006 against the 16 attacks we presented (both existing and novel attacks) in order to understand whether or not they fully address the attacks and to identify the existing security gaps in an attempt to suggest directions for security enhancements for the ICUMD ecosystems. The security abilities of the existing mechanisms vary; some of them cover only three attacks, but most of them cover 4-5 attacks. The Cisco CWS security mechanism (number 1) covers seven attacks, constituting less than 44% of the 16 attacks. There is no doubt that designated and comprehensive security mechanisms need to be developed and should combine several different layers and modules in order to deal with as many attacks as possible.

There are a few open issues regarding the security of the ICU; as shown in this paper, one of these issues is the human factor, which could be utilized as an attack vector through social engineering techniques [79] in 15 of the attacks we presented (for example, by sending a malicious link or inserting an infected USB into an operating system). Moreover, the trend of using social engineering techniques in healthcare, such as phishing, has been continuously growing [86]. Based on our understanding, the medical team is not well trained regarding security issues or aware of the security problems that exist. In addition, the systems in the ICU do not currently restrict the use of insecure platforms (for example, members of the medical team can access their private email accounts from the workstations or connect USB devices which could be infected or compromised and result in an attack). Another issue, as seen in Table 23, is that eight attacks are not covered by any of the mechanisms: electromagnetic interference, alert attack - missing alerts (devices), alert attack - false alerts (devices), centralized alert attack - missing alerts (nurses' station), centralized alert attack - false alerts (nurses' station), malicious firmware update, configuration manipulation, and abuse of legitimate operations. A third issue is the fact that the medical team has a significant workload; this reality points to the need for a centralized system that easily controls, monitors, and displays the security status of each of the ICUMDs; such a system would allow the team to monitor and follow the ICU in terms of security.

The advancement of machine learning algorithm capabilities has led to an increase in their integration within security mechanisms. The reason for this is linked to the effectiveness that machine learning algorithms have demonstrated in predicting and detecting anomalies as part of the detection of new and unknown cyber-attacks [90]. While the use of machine learning algorithms in existing security mechanisms

for ICUMDs is very limited [44], these algorithms have the potential to contribute to improved ICUMD security.

After reviewing the range of cyber threats in the intensive care unit and their potential dangerous effects on the patient and the work environment, we observed that the existing security mechanisms only provide a partial, and relatively outdated, response. For example, the developers of the Cisco CWS [44] security mechanism proposed using predictive analytics and machine learning algorithms for the purpose of analyzing network traffic and identifying anomalies, thereby providing alerts and a response to attacks.

## VI. FUTURE WORK

Based on our finding in this study, in future work we suggest to improve three aspects of the protection of ICUMDs: (a) the technological-security aspect: in order to address this aspect, we recommend to increase the use and integration of technological security mechanisms, in order to minimize the ability of known attacks to be carried out via the various ICUMD devices and identify attacks and anomalies as soon as possible, in order to minimize the potential damage. (b) the ICUMD development aspect: in order to address this aspect, when designing and developing ICUMDs, vendors should consider the security of ICUMDs, in addition to their medical functionality; this process will reduce the vulnerability of ICUMDs, increasing the security of each ICUMD as well as the interaction and dependencies between ICUMDs. (c) the behavioral-educational aspect: in order to address this aspect, we recommend to increase the ICU medical staff's security awareness and providing them with training regarding risks, potential attacks, prevention procedures, and the attack vectors by which the ICUMDs and their ecosystems can be compromised. This will limit an attacker's ability to launch a cyber-attack by taking advantage of the medical staff's innocence or unawareness. In recognition of the wide range of attacks and vulnerabilities, we suggest studying this lack of awareness in terms of "attack class," as was recently proposed in the field of mobile security and described by Bitton *et al.* [87].

In addition, with the emerging trend of machine learning and data science methods in variety of domains, we suggest developing machine learning-based algorithms as an effective tool for identifying and issuing alerts in real-time. Due to the many weaknesses of the central monitoring station, as well as its great importance for the medical team and their decision-making processes, we suggest focusing on learning normal and manipulated data in order to induce an anomaly detection model, by which manipulation of the system's data can be identified based on the various medical parameters presented.

Thus, in future work we plan to develop a machine learning and time-oriented security mechanism based on the five prominent measurements acquired and displayed on this device:

**RESP**– the number of breaths per minute; this is measured by counting the number of times the chest rises. The normal range for a healthy adult at rest is 12-18 breaths per minute.

**Heart rate**– the speed of the heartbeat. This is measured by the number of heart beats per minute (bpm). The normal range for a healthy adult at rest is 60-100 bpm. **% SpO<sub>2</sub>** – the fraction of oxygen-saturated hemoglobin relative to total hemoglobin in the blood (unsaturated and saturated). The normal value for a healthy adult at rest is 94% and above. **NBP** (non-invasive blood pressure) – the arterial pressure in the systemic circulation. It is generally expressed in terms of systolic pressure (maximum during one heart beat) and diastolic pressure (minimum in between two heart beats). It is measured in millimeters of mercury (mmHg). The normal range of the systolic pressure is 90-129 mmHg, and the normal range of the diastolic pressure is 60-84 mmHg.

We assume that by learning the behavior of the various measures over time [75], as well as the way they interact, it will be possible to identify anomalies and deviations in the system's data. In a future application of the security mechanism, the medical team would receive alerts regarding anomalous events. A real-time warning may save the life of a patient exposed to an attack. In addition, we plan to try to incorporate a general model and a personal model based on a specific patient's data, in order to increase the model's precision and improve the probability of identifying manipulated data.

Another recommendation is to physically reduce access to the various ICUMDs, making it difficult for an attacker to penetrate and compromise the device. Currently, in the ICU setting, visitors (including those who may be hostile), can approach an ICUMD connected directly to the patient and compromise it. As a countermeasure, policies aimed at protecting the ICUMDs in a patient's room, could be implemented, e.g., the devices could be placed in transparent boxes; this would allow the ICUMD screen to be seen, ensuring that indications of device performance and patient status are still available, while providing an additional layer of physical protection (the attacker won't have easy access to the device). Keys and credentials could be used to provide medical staff with access to the devices for maintenance and treatment purposes.

Future work may also be centered on developing a management mechanism for firmware updates and specific versions of the various ICUMDs. As we noted, configuration manipulation (attack number 15) is an attack that can affect all ICUMDs; this attack can be performed by malicious firmware updates or the insertion of an infected USB (a security risk that we have addressed in prior work) [72]. We plan to establish a trusted system to manage ICUMD firmware updates in order to find a solution to these possible attacks. The system will manage and install updates for the latest software versions available on the market and offers two significant advantages: first, it will maintain up-to-date software (including security updates), and second, it will prevent the installation of "fictitious" updates provided by an attacker.

A last suggestion for future work centers on the development of a central monitoring system which is responsible

for indicating the availability and proper functionality of all ICMUMDs within the ICU. Such monitoring systems are usually referred to as security information and event management (SIEM) systems, and they are used in a variety of settings (e.g., critical infrastructure, industry). As we mentioned in this survey, the ICU ecosystem is extremely complex and threatened by a variety of cyber-attacks. Such a monitoring system will help manage and handle the risks, alerting the medical staff regarding the unavailability or anomalies associated with the ICUMDs in real time and enabling them to respond quickly and provide the patient with alternative treatment.

#### AUTHOR CONTRIBUTIONS

**Nir Nissim** - Study's Principle Investigator, study concept and design, cyber-security expertise, and design of solution.

**Isaac Lazar** – Clinical and medical expertise, clinical guidance.

**Nir Nissim, Carmel Eliash, Isaac Lazar** - Writing the manuscript, analysis of interactions and ecosystems.

**Nir Nissim, Carmel Eliash** – Analysis of the attacks and security mechanisms.

#### REFERENCES

- [1] S. Chacko, R. R. Sarin, A. Voskanyan, M. S. Molloy, and G. R. Ciottone, "Maintaining continuity of care in the recovery phase with military medicine," *Prehospital Disaster Med.*, vol. 32, no. S1, pp. S72–S73, Apr. 2017.
- [2] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," *Biomed. Instrum. Technol.*, vol. 48, no. s1, pp. 38–41, May 2014.
- [3] E. D. Perakslis, "Cybersecurity in health care," *New England J. Med.*, vol. 371, no. 5, pp. 395–397, 2014.
- [4] L. Ayala, *Cybersecurity for Hospitals and Healthcare Facilities*. Berkeley, CA, USA: Apress, 2016.
- [5] N. Long and R. Thomas. (2001). "Trends in denial of service attack technology." CERT Coordination Center, Pittsburgh, PA, USA, pp. 648–651. [Online]. Available: <https://ci.nii.ac.jp/naid/10012958905/en/>
- [6] V. I. Gurevich. (2005). "Electromagnetic terrorism: New hazards." Israel Electric Corp., Central Electric Laboratory. [Online]. Available: <http://dspace.nbu.gov.ua/handle/123456789/142612>
- [7] G. N. Nayak and S. G. Samaddar, "Different flavours of man-in-the-middle attack, consequences and feasible solutions," in *Proc. 3rd Int. Conf. Comput. Sci. Inf. Technol.*, Jul. 2010, pp. 491–495.
- [8] S. C. Ball, "Ohio's aggressive attack on medical identity theft," *JL Health*, vol. 24, no. 1, p. 111, 2011.
- [9] E. M. Decisions. (2004). *What is Spyware?* [Online]. Available: <https://www.taugh.com/levine-23mar04-spyware.pdf>
- [10] J. M. Ehrenfeld, "WannaCry, cybersecurity and health information technology: A time to act," *J. Med. Syst.*, vol. 41, p. 104, 2017, doi: [10.1007/s10916-017-0752-1](https://doi.org/10.1007/s10916-017-0752-1).
- [11] G. O'Gorman and G. McDonald, *Ransomware: A Growing Menace*. Chennai, India: Symantec Corporation, 2012.
- [12] S. Kapoor. (2006). *Session Hijacking Exploiting TCP, UDP and HTTP Sessions*. [Online]. Available: [https://infosecwriters.com/text\\_resources/.../SKapoor\\_SessionHijacking.pdf](https://infosecwriters.com/text_resources/.../SKapoor_SessionHijacking.pdf)
- [13] A. Cui, M. Costello, and S. J. Stolfo, "When firmware modifications attack: A case study of embedded exploitation," in *Proc. NDSS*, Feb. 2013, pp. 1–13.
- [14] Z. Basnight, J. Butts, J. Lopez, and T. Dube, "Firmware modification attacks on programmable logic controllers," *Int. J. Crit. Infrastruct. Protection*, vol. 6, no. 2, pp. 76–84, Jun. 2013.
- [15] A. Zimba, Z. Wang, M. Mulenga, and N. H. Odongo, "Cryptomining attacks in information systems: An emerging threat to cyber security," *J. Comput. Inf. Syst.*, pp. 1–12, May 2018, doi: [10.1080/08874417.2018.1477076](https://doi.org/10.1080/08874417.2018.1477076).
- [16] S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark, "A first look at browser-based cryptojacking," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2018, pp. 58–66.

- [17] S. Mohurle and M. Patil, "A brief study of wannacry threat: Ransomware attack 2017," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 5, pp. 1–3, 2017.
- [18] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, no. 4, pp. 74–82, 2015.
- [19] R. Hillestad, J. Bigelow, A. Bower, F. Girosi, R. Meili, R. Scoville, and R. Taylor, "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs," *Health Affairs*, vol. 24, no. 5, pp. 1103–1117, Sep. 2005.
- [20] H. Löhr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proc. ACM Int. Conf. Health Informat. (IHI)*, 2010, pp. 220–229.
- [21] I. Lee and O. Sokolsky, "Medical cyber physical systems," in *Proc. 47th ACM/IEEE Design Automat. Conf. (DAC)*, Jun. 2010, pp. 743–748.
- [22] D. B. Kramer, M. Baker, B. Ransford, A. Molina-Markham, Q. Stewart, K. Fu, and M. R. Reynolds, "Security and privacy qualities of medical devices: An analysis of FDA postmarket surveillance," *PLoS ONE*, vol. 7, no. 7, 2012, Art. no. e40200.
- [23] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2011.
- [24] S. M. Specht and R. B. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures," in *Proc. ISCA PDCS*, Sep. 2004, pp. 543–550.
- [25] A. Ornaghi and M. Valleri, "Man in the middle attacks," in *Proc. Blackhat Conf. Eur.*, 2003, pp. 1–61.
- [26] K. M. J. Haataja and K. Hyppönen, "Man-in-the-middle attacks on Bluetooth: A comparative analysis, a novel attack, and countermeasures," in *Proc. 3rd Int. Symp. Commun., Control Signal Process. (ISCCSP)*, Mar. 2008, pp. 1096–1102.
- [27] J. Mantas, "Electronic health record," *Stud. Health Technol. Inform.*, vol. 65, pp. 250–257, 2002. [Online]. Available: <https://europepmc.org/article/med/15460229>
- [28] D. G. Katehakis and M. Tsiknakis, "Electronic health record," in *Wiley Encyclopedia of Biomedical Engineering*. 2006, doi: [10.1002/9780471740360.ebs1440](https://doi.org/10.1002/9780471740360.ebs1440).
- [29] F. Skopik and P. D. Smith, Eds., *Smart Grid Security: Innovative Solutions for a Modernized Grid*. Rockland, MA, USA: Syngress, 2015.
- [30] H. Berghel, "Hijacking the Web," *Commun. ACM*, vol. 45, no. 4, p. 23, Apr. 2002.
- [31] K. Chinthapalli, "The hackers holding hospitals to ransom," *Brit. Med. J.*, vol. 357, 2017.
- [32] D. Arney, K. K. Venkatasubramanian, O. Sokolsky, and I. Lee, "Biomedical devices and systems security," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Sep. 2011, pp. 2376–2379.
- [33] K. K. Venkatasubramanian, E. Y. Vasserman, O. Sokolsky, and I. Lee, "Security and interoperable-medical-device systems, part 1," *IEEE Secur. Privacy*, vol. 10, no. 5, pp. 61–63, Sep. 2012.
- [34] K. J. Dreyer, D. S. Hirschorn, J. H. Thrall, and A. Mehta, *PACS: A Guide to the Digital Revolution*. New York, NY, USA: Springer, 2006.
- [35] S. D. Larson, A. F. Mickelson, and P. M. Eisenberg, U.S. Patent 5 609 575, 1997. [Online]. Available: <https://patentimages.storage.googleapis.com/37/24/4b/9e9fe9f7f81624/US5609575.pdf>
- [36] G. G. Sanderson, M. Massaglia, and M. J. Palmer, "Syringe pump and the like for delivering medication," U.S. Patent 5 176 502, Jan. 5, 1993. [Online]. Available: <https://patents.google.com/patent/US5176502A/en>
- [37] S. Kahn and V. Sheshadri, "Medical record privacy and security in a digital environment," *IT Prof.*, vol. 10, no. 2, pp. 46–52, Mar. 2008.
- [38] P. A. Williams and A. J. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices*, vol. 8, p. 305, Jul. 2015.
- [39] A. Shoufan, H. AlNoon, and J. Baek, "Secure communication in civil drones," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy*. Cham, Switzerland: Springer, Feb. 2015, pp. 177–195.
- [40] H. C. Van Tilborg and S. Jajodia, Eds., *Encyclopedia of Cryptography and Security*. Springer, 2014.
- [41] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Security issues and challenges for cyber physical system," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun. Int. Conf. Cyber, Phys. Social Comput.*, Dec. 2010, pp. 733–738.
- [42] O. Salem, Y. Liu, A. Mehaoua, and R. Boutaba, "Online anomaly detection in wireless body area networks for reliable healthcare monitoring," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 5, pp. 1541–1551, Sep. 2014.
- [43] N. A. Halpern and S. M. Pastores, "Critical care medicine in the united states 2000–2005: An analysis of bed numbers, occupancy rates, payer mix, and costs," *Crit. Care Med.*, vol. 38, no. 1, pp. 65–71, Jan. 2010.
- [44] R. Vargheese, "Dynamic protection for critical health care systems using Cisco CWS: Unleashing the power of big data analytics," in *Proc. 5th Int. Conf. Comput. Geospatial Res. Appl.*, Aug. 2014, pp. 77–81.
- [45] J. Luna, M. D. Dikaiakos, H. Gjermundrod, M. Flouris, M. Marazakis, and A. Bilas, "Using the glide middleware to implement a secure intensive care grid system," in *Grid and Services Evolution*, vol. 11, 2009, p. 87. [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.149.2151&rep=rep1&type=pdf>
- [46] K. Habib and W. Leister, "Threats identification for the smart Internet of Things in eHealth and adaptive security countermeasures," in *Proc. 7th Int. Conf. New Technol., Mobility Secur. (NTMS)*, Jul. 2015, pp. 1–5.
- [47] I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. Mullen-Fortino, S. Park, A. Roederer, and K. K. Venkatasubramanian, "Challenges and research directions in medical cyber-physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 75–90, Jan. 2012.
- [48] H. Soroush, D. Arney, and J. Goldman, "Toward a safe and secure medical Internet of Things," *IIC J. Innov.*, vol. 2, no. 1, pp. 4–18, Jun. 2016.
- [49] R. M. Savola and H. Abie, "Metrics-driven security objective decomposition for an e-health application with adaptive security management," in *Proc. Int. Workshop Adapt. Secur. (ASPI)*, Sep. 2013, p. 6.
- [50] T. Mavroeidakos, N. Tsolis, and D. D. Vergados, "Centralized management of medical big data in intensive care unit: A security analysis," in *Proc. 3rd Smart Cloud Netw. Syst. (SCNS)*, Dec. 2016, pp. 1–5.
- [51] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*, document 32016R0679, European Union, 2016.
- [52] K. S. BlackHat, K. Nohl, and J. Lel. (Aug. 7, 2014). *Slides*. [Online]. Available: <https://srlabs.de/blog/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf>
- [53] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein, and M. Bailey, "Users really do plug in USB drives they find," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 306–319.
- [54] N. Nissim, R. Yahalom, and Y. Elovici, "USB-based attacks," *Comput. Secur.*, vol. 70, pp. 675–688, Sep. 2017.
- [55] K. Sigler, "Crypto-jacking: How cyber-criminals are exploiting the cryptocurrency boom," *Comput. Fraud Secur.*, vol. 2018, no. 9, pp. 12–14, Sep. 2018.
- [56] J. M. Seigen, M. Jameson, T. Nieminen, Neocortex, and A. M. Juarez. (2013). *CryptoNight Hash Function*. [Online]. Available: <https://cryptonote.org/cns/cns008.txt>
- [57] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.
- [58] Y. Lee and K. A. Kozar, "An empirical investigation of anti-spyware software adoption: A multitheoretical perspective," *Inf. Manage.*, vol. 45, no. 2, pp. 109–119, Mar. 2008.
- [59] S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, and R. Cunningham, "Blockchain technology: What is it good for?" *Queue*, vol. 17, no. 5, pp. 41–68, Oct. 2019.
- [60] B. P. Cholley, A. Vieillard-Baron, and A. Mabazza, "Echocardiography in the ICU: Time for widespread use!" *Intensive Care Med.*, vol. 32, no. 4, p. 634, Apr. 2006.
- [61] B. P. Goodman and A. J. Boon, "Critical illness neuromyopathy," *Phys. Med. Rehabil. Clinics North Amer.*, vol. 19, no. 1, pp. 97–110, 2008.
- [62] L. A. Geddes, "The history of artificial respiration [retrospectroscope]," *IEEE Eng. Med. Biol. Mag.*, vol. 26, no. 6, pp. 38–41, Nov. 2007.
- [63] D. Lichtenstein and O. Axler, "Intensive use of general ultrasound in the intensive care unit," *Intensive Care Med.*, vol. 19, no. 6, pp. 353–355, Jun. 1993.
- [64] J. M. Crawford, Jr., "Medical monitor system," U.S. Patent 5 331 549, Jul. 19, 1994. [Online]. Available: <https://patents.google.com/patent/US5331549A/en>
- [65] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Privacy Mag.*, vol. 9, no. 3, pp. 49–51, May 2011.
- [66] K. Munro, "Deconstructing flame: The limitations of traditional defenses," *Comput. Fraud Secur.*, vol. 2012, no. 10, pp. 8–11, Oct. 2012.
- [67] P. L. Bailey, S. W. McJames, M. L. Cluff, D. T. Wells, J. A. Orr, D. R. Westenskow, and S. E. Kern, "Evaluation in volunteers of the VIA V-ABG automated bedside blood gas, chemistry, and hematocrit monitor," *J. Clin. Monitor. Comput.*, vol. 14, no. 5, pp. 339–346, 1998.
- [68] T. Saha, R. H. Bhuiya, Z. U. Masum, M. R. Islam, and J. A. Chowdhury, "Hospital pharmacy management system and future development approaches in bangladeshi hospital," *Bangladesh Pharmaceutical J.*, vol. 20, no. 2, pp. 180–187, 2017.
- [69] H. White and L. King, "Enteral feeding pumps: Efficacy, safety, and patient acceptability," *Med. Devices: Evidence Res.*, vol. 7, p. 291, Aug. 2014.
- [70] M. Al-Zarouni, "The reality of risks from consented use of USB devices," in *Proc. Austral. Inf. Secur. Manage. Conf.*, 2006. [Online]. Available: <https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1061&context=ism>

- [71] D. R. Thompson, D. K. Hamilton, C. D. Cadenhead, S. M. Swoboda, S. M. Schwindel, D. C. Anderson, E. V. Schmitz, A. C. S. Andre, D. C. Axon, J. W. Harrell, M. A. Harvey, A. Howard, D. C. Kaufman, and C. Petersen, "Guidelines for intensive care unit design," *Crit. Care Med.*, vol. 40, no. 5, pp. 1586–1600, 2012.
- [72] N. Farhi, N. Nissim, and Y. Elovici, "Malboard: A novel user keystroke impersonation attack and trusted detection framework based on side-channel analysis," *Comput. Secur.*, vol. 85, pp. 240–269, Aug. 2019.
- [73] A. Murakami, M. A. Gutierrez, S. H. G. Lage, M. F. S. Rebelo, R. H. G. Guiraldelli, and J. A. F. Ramires, "A continuous glucose monitoring system in critical cardiac patients in the intensive care unit," in *Proc. Comput. Cardiol.*, Sep. 2006, pp. 233–236.
- [74] M. Kintzlinger and N. Nissim, "Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems," *J. Biomed. Inform.*, vol. 95, Jul. 2019, Art. no. 103233.
- [75] E. Sheehrit, N. Nissim, D. Klimov, and Y. Shahar, "Temporal probabilistic profiles for sepsis prediction in the ICU," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2019, pp. 2961–2969.
- [76] J. Giraldo, A. Cardenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: Impact and countermeasures," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2249–2257, Sep. 2017.
- [77] K. J. Kappiarukudil and M. V. Ramesh, "Real-time monitoring and detection of 'heart attack' using wireless sensor networks," in *Proc. 4th Int. Conf. Sensor Technol. Appl.*, Jul. 2010, pp. 632–636.
- [78] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013.
- [79] B. D. Medlin, J. A. Cazier, and D. P. Foulk, "Analyzing the vulnerability of U.S. hospitals to social engineering attacks: How many of your employees would share their password?" *Int. J. Inf. Secur. Privacy*, vol. 2, no. 3, pp. 71–83, Jul. 2008.
- [80] D. S. McDermott, J. L. Kamerer, and A. T. Birk, "Electronic health records: A literature review of cyber threats and security measures," *Int. J. Cyber Res. Educ.*, vol. 1, no. 2, pp. 42–49, Jul. 2019.
- [81] B. Owens, "How hospitals can protect themselves from cyber attack," *Can. Med. Assoc. J.*, vol. 192, no. 4, pp. E101–E102, Jan. 2020.
- [82] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *J. Med. Syst.*, vol. 44, no. 2, Feb. 2020.
- [83] S. Ammous. (2016). *Blockchain Technology: What is It Good For?*. [Online]. Available: <https://pdfs.semanticscholar.org/0f75/78d3b14efc547d2bee8b971de1218b5d073f.pdf>
- [84] J. L. Kamerer and D. McDermott, "Cybersecurity: Nurses on the front line of prevention and education," *J. Nursing Regulation*, vol. 10, no. 4, pp. 48–53, Jan. 2020.
- [85] J. J. Hathaliya, S. Tanwar, S. Tyagi, and N. Kumar, "Securing electronics healthcare records in healthcare 4.0: A biometric-based approach," *Comput. Electr. Eng.*, vol. 76, pp. 398–410, Jun. 2019.
- [86] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, and N. J. Sebire, "Phishing in healthcare organisations: Threats, mitigation and approaches," *BMJ Health Care Inform.*, vol. 26, no. 1, pp. 1–6, 2019.
- [87] R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach, and A. Shabtai, "Taxonomy of mobile users' security awareness," *Comput. Secur.*, vol. 73, pp. 266–293, Mar. 2018.
- [88] L. Rooney, S. Rimpiläinen, C. Morrison, and S. L. Nielsen, "Review of emerging trends in digital health and care: A report by the Digital Health and Care Institute." 2019, doi: [10.17868/67860](https://doi.org/10.17868/67860).
- [89] J. G. Steiner, B. C. Neuman, and J. I. Schiller, "Kerberos: An authentication service for open network systems," in *Proc. USENIX Winter*, Feb. 1988, pp. 191–202.
- [90] R. Moskovitch, N. Nissim, and Y. Elovici, "Acquisition of malicious code using active learning," in *Proc. 2nd Int. Workshop Privacy, Secur., Trust KDD*, Aug. 2008, pp. 1–9.



**ISAAC LAZAR** received the M.D. degree from the Faculty of Health Sciences, Ben-Gurion University of the Negev, Beer-Sheva, Israel, in 1994. After his graduation, he remained as a Senior Physician with the Pediatric Intensive Care and a Faculty at the Yale School of Medicine, New Haven. From 2001 to 2004, he did his Postdoctoral Fellowship in the field of pediatric critical care with the Department of Critical Care and Applied Physiology, Yale University, New Haven, CT, USA. He is currently the Director of the Pediatric Intensive Care Unit, Soroka University Medical Center, and a Lecturer at the Faculty of Health Sciences, Ben-Gurion University of the Negev, Beer-Sheva, Israel. He further completed the Pediatric Residency at the Rambam Medical Center, The Technion, Haifa, Israel. Since 2007, he works at the Soroka University Medical Center, as a Senior Physician in the pediatric ICU, and he serves as the Pediatric ICU Director, since 2013. He was an Academic Clinician and a Scientist is deeply involved in pediatric ICU work, running a state of the art busy ICU in the only tertiary hospital in Southern Israel. The PICU cares for over 400,000 children of diverse population who lives in a desert which covers 2/3 of the country's geographical area. This creates a big clinical challenge but also a large field for medical research. During his carrier, he was and is deeply involved in basic translational and clinical research as a member of the Faculty of Health Sciences, Ben-Gurion University.



**NIR NISSIM** received the Ph.D. degree (Hons.) from the Department of Information Systems Engineering, Ben-Gurion University (BGU), in 2016. He was a Postdoctoral Fellow at Stanford University and served as a Data-Scientist in a neuroscience research dealing with analyzing spike-level data of primates. In 2018, he has joined the Department of Industrial Engineering and Management, Ben-Gurion University, where he is currently a Researcher and the Head of the Malware Lab, Cyber Security Research Center. He is also a Lecturer at the Information Systems Engineering Department, BGU, and at the Industrial Engineering and Management Department, Tel Aviv University, both on cyber security and machine learning topics. He is recognized as an expert in information systems security and machine learning solutions and has been leading several large-scale research projects in the field, including collaborative projects between academia and industry. He published several noteworthy articles dealing with the development of a generic active learning framework aimed at the detection and acquisition of various types of malware in a variety of platforms. His main areas of interests are mobile and computer security, security of medical devices, machine learning, and data science. In addition to his contributions to the cyber security domain, he is also interested in the bioinformatics domain and has published a number of articles regarding the efficient classification of condition severity. He received the prestigious prize in recognition of his ranking as the Faculty of Engineering Sciences' Top Doctoral Student, in 2016. During his Ph.D. research, he won several best paper awards in top ranked scientific international conferences and awards of excellence at BGU, and he was one of the few doctoral students at BGU to win an exclusive doctoral cyber security scholarship granted by the Israeli Cyber Security Bureau. In addition, he is also the Head of the ICSML Program which is an International Cyber-Security and Machine Learning Academic and Professional Program for international students.



**CARME ELIASH** is currently a Research Student of the master's program for outstanding students in industrial engineering (Business Analytics) at Tel-Aviv University. He is also a Researcher at the Malware Lab, Cyber Security Research Center, Ben-Gurion University, focusing on securing ICU (Intensive Care Unit) medical devices using machine learning techniques. In his thesis, he is being supervised jointly by two researchers Dr. N. Nissim and Prof. I.-B.-Gal. Prior to this, he was an

Intelligence Officer and a Projects Lead in the IDF and worked at Advanced Analytics Group, Intel.

• • •