Attack Detection for Medical Cyber-Physical Systems–A Systematic Literature Review

Simon B. Weber, Stefan Stein, Michael Pilgermann, Thomas Schrader

Article - Version of Record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 April 2023, accepted 19 April 2023, date of publication 25 April 2023, date of current version 3 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3270225

SURVEY

Attack Detection for Medical Cyber-Physical Systems–A Systematic Literature Review

SIMON B. WEBER[1], STEFAN STEIN[2], MICHAEL PILGERMANN[2], AND THOMAS SCHRADER[2]

[1]Department of Computer Science, Heinrich Heine University Düsseldorf, 40225 Düsseldorf, Germany
[2]Department of Computer Science and Media, Brandenburg University of Applied Sciences, 14770 Brandenburg an der Havel, Germany

Corresponding author: Simon B. Weber (Simon.Weber@hhu.de)

ABSTRACT The threat situation due to cyber attacks in hospitals is emerging and patient life is at risk. One significant source of potential vulnerabilities is medical cyber-physical systems (MCPS). Detecting intrusions in this environment faces challenges different from other domains, mainly due to the heterogeneity of devices, the diversity of connectivity types, and the variety of terminology. To summarize existing results, we conducted a structured literature review (SLR) following the guidelines of Kitchenham et al. for SLRs in software engineering. We developed six research questions regarding detection approach, detection location, included features, adversarial focus, utilized datasets, and intrusion prevention. We identified that most researchers focused on an anomaly-based detection approach at the network layer. The primary focus was on the detection of malicious insiders. While several researchers used publicly available datasets for training and testing their algorithms, the lack of suitable datasets resulted in the development of testbeds consisting of various medical devices. Based on the results, we formulated five future research topics. First, the special conditions of hospital networks, the MCPS deployed within them, and the contrasts to other IT and OT environments should be examined. Thereupon, MCPS-specific datasets should be created that allow researchers to address the health domain's unique requirements and possibilities. At the same time, endeavors aimed at standardization in this area should be supported and expanded. Moreover, the use of medical context for attack detection should be further explored. Last but not least, efforts for MCPS-tailored intrusion prevention should be intensified. This way, the emerging threat landscape can be addressed, IT security in hospitals can be improved, and patient health can be protected.

INDEX TERMS Detection, IDS, intrusion prevention, medical cyber-physical systems, medical CPS, internet of health things, IoMT, medical IoT, connected health, healthcare 4.0.

I. INTRODUCTION

The healthcare sector faces an increasing threat of cyber attacks. A Comparitech study explored the threat landscape of the US sector and found that in the time 2016 to 2022, 6,835 healthcare companies were hit by ransomware [1]. Already in 2014, a SANS report admonished the risks of MCPS and identified ''Nontraditional medical endpoints'' as one of the main malicious traffic sources [2]. Gartner predicts for the year 2025 that operational technology (OT) environments will be weaponized to harm or kill people and that the resulting financial impact from such attacks will amount to $50 billion per year [3].

Coventry et al. surveyed hospital staff to determine the reasons for clinics' high IT security risks. One key finding is that medical device software is often outdated and unsupported [4]. This corresponds to the report of the European Union Agency for Network and Information Security (ENISA). They stress that legacy software and unpatched vulnerabilities are particularly critical in the healthcare sector. Accordingly, imaging systems, patient monitoring, and medical device gateways root for 86% of hospital security issues [5]. As Coventry et al. emphasized, securing legacy medical devices seems more crucial than ever. Despite these findings, current security scanners often fail to detect

The associate editor coordinating the review of this manuscript and approving it for publication was Peng-Yong Kong.

vulnerabilities in the healthcare environment because they do not have modules for medical devices and systems [6].

Intrusion detection is a technology that has been around for more than three decades [7]. Many organizations rely on it even more in a time of increasing cyber threats. Its most widespread application is in the field of (office) information technology (IT). In contrast, the used OT is not as covered in many sectors. Only in recent years, there have been efforts to transfer insights from IT to OT, primarily because of the emerging threat situation [8]. Many sectors can interoperate and share their sector-specific discoveries and perceptions. The health sector differs in this regard. There are three reasons: The heterogeneity of OT devices in healthcare, the diversity of connectivity types, and the variety of terminology. The heterogeneity of devices and missing regulations lead to a situation where no central management of devices from assorted manufacturers is possible. Furthermore, the different needs of different devices lead to different requirements for connectivity. E.g., while computed tomography scanners are regularly connected via a wired connection, wearable medical devices require a wireless connection for obvious reasons. Researchers cover this domain as wireless sensor networks (WSN), of which subgroups are medical smartphone networks (MSN) and wireless body area networks (WBAN). These networks consist of devices known as wearables, which are worn by a person and can also be connected to each other. Since devices of those groups are carried around, they not only have special requirements for connectivity but also for an intrusion detection system (IDS). In addition, the need for real-time detection for all MCPS, regardless of the device type, is argued to be even more critical than in existing mechanisms because lives could depend on a timely detection [9]. While some researchers try to detect intrusions in a protocol-agnostic way, others are motivated by the particular conditions of a subset of medical devices. This leads to different categorizations and definitions of groups and, thereby, to various terms. We further discuss the diversity of terms in section III-B.

This paper aims to outline the existing research on attack detection in the healthcare sector. We focus on the current state of research in detecting attacks on medical devices available for hospitals and clinics. The challenges of hospital networks, attached medical devices, and the plethora of protocols used by those devices are of particular interest. By discussing this environment's background and special requirements, we identify research gaps and give future endeavors direction.

The paper is organized as follows. In section II, we present other secondary studies and point out how this paper complements the existing work. Thereafter, in section III, we describe our methodology and present the research questions, according to which we have evaluated the studies. The results are presented in section IV. In section V, we discuss the findings and work out the implications. Finally, we draw a conclusion in section VI.

II. RELATED WORK

Existing reviews and survey papers on MCPS attack detection can be summarized into four groups. The papers of the first group discuss work about general IoT and merely touch the area of medical devices. They refer to MCPS either as motivation or to highlight them as a unique area with particular characteristics. One example is Banerjee et al., who discuss the security of several sectors in which IoT is used and how blockchain could improve it in the future. The healthcare domain is a characteristic example in which very sensitive data must be shared, and privacy is essential [10].

The second group concentrates on medical device security and attempts a comprehensive overview. Either they use broad definitions of security and include not only IT security but also privacy and patient safety, or the review outlines several IT security measures. Examples are Yaacoub et al., Tervoort et al., and Ferrag et al., who provide a detailed overview of relevant attack scenarios for medical devices and discuss which defensive measures can protect the devices from which attacks. These measures range from technical to non-technical aspects. Yaacoub et al. recommend a layered security architecture, ranging from raising awareness through employee training to sophisticated intrusion detection, mainly through a machine learning (ML)-based intrusion detection and prevention system cooperating with honeypots and security information and event management (SIEM) to gain the latest insights into attacks [11]. Tervoort et al. conduct a scoping review presenting an overview of security solutions for medical software vulnerabilities that do not require the software to be replaced. Besides intrusion detection, monitoring specific aspects of medical devices, such as software execution characteristics and tunneling legacy protocols, have been examined [12]. Ferrag et al. outline security solutions for the Internet of medical things (IoMT) of five categories: authentication and access control, key management and cryptography, intrusion detection systems, blockchain-based solutions, and privacy-preserving solutions [13].

The third group of papers focuses on a specific aspect or a specific type of approach. Thomasian and Adashi summarize the policy and regulatory measures (primarily concentrated on the US) to secure medical devices. Furthermore, they provide an overview of the emerging threats in this context on a high level [14]. Hameed et al. elucidate ML-based approaches in their structured review of security and privacy in the context of the IoMT. Besides insightful statistical data surrounding the publications, such as the geographical distribution of research groups and the development of publications per year, a focal point of the work of Hameed et al. is ML-based intrusion detection [15]. Rbah et al. concentrate their efforts on comparing deep learning methods utilized for IDSs in the IoMT. They observe that many researchers develop their approaches in an isolated environment for a limited number of attacks [16]. Pelekoudas-Oikonomou et al. review blockchain-based security mechanisms for IoMT

edge networks. While they describe several ways in which attack detection in IoMT-edge networks could benefit from a blockchain extension, they state that, to their knowledge, there are no blockchain-based IDSs specifically designed for IoMT-edge networks yet. Instead, they outline approaches from other IoT environments and show how they could be applied to IoMT-edge networks [17].

The fourth group of papers compares approaches tailored to small subsets of MCPS. Eliash et al. discuss the security of the subset of medical devices used in intensive care units (ICUMDs), introduce a taxonomy for these devices, and explain how these devices interact with each other. They develop scenarios for 16 attacks on medical devices and derive the main building blocks. Additionally, they analyze the applicability of existing security mechanisms, including detection mechanisms [18]. Similarly, Kintzlinger and Nissim establish a taxonomy for personal medical devices (PMDs) and collect attack scenarios and building blocks for attacks on this group of devices. Furthermore, they review the existing security solutions and identify the gaps between them and the identified attack vectors [19]. Ghosal et al. present a survey for ML approaches utilized for IT security in cloud-based IoT healthcare systems [20], Wa Umba et al. review security measurements exclusively for software-defined WSNs (SDWSNs) [21], and Wazid et al. compare detection approaches for malware in the IoMT environment [22].

This paper differs from those presented as it aims to provide an overview of all intrusion detection approaches for all kinds of medical devices available for hospitals and clinics. The main contributions can be summarized as follows:

- We present the current state of research on attack detection in medical cyber-physical system environments. In particular, we show the various challenges that are special or unique to the health sector and frame our research questions around these specifics.
- As a distinct difference from other secondary studies based on a single or small number of keywords (e.g., IoMT), we identified 22 synonyms for MCPS. We included them in an extensive database search as a basis. The high number of synonyms allows a comprehensive and profound analysis of the research state.
- By following the guidelines of Kitchenham et al. for structured literature reviews in software engineering, we minimized the risk of a biased consideration of the studies available. This includes:
  1) A structured two-step screening process
  2) Transparent inclusion and exclusion criteria for study selection
  3) The independent review of studies by at least two researchers in every selection and extraction step.
- By answering six research questions, we structure the confusing and convoluting state of literature and highlight commonalities and differences. For exceptional approaches, we present a detailed description.
- We critically engage with the selected aspects of the research and discuss the applicability of the proposed approaches.
- The resulting discrepancies will help researchers conduct more focused research through five derived future research topics.

III. METHODOLOGY

We adopted the guidelines for performing systematic literature reviews (SLR) in software engineering [23]. According to Kitchenham et al., the goal of such a review is threefold: Firstly, the review shall summarise the existing results in a field. Secondly, it should identify gaps in the current research, and thirdly, it should provide the background to position future research endeavors.

A. RESEARCH QUESTIONS

We developed six research questions to determine the state of research in the field of MCPS attack detection. These are outlined in the following.

1) WHICH DETECTION APPROACH IS USED?

First, we wanted to ascertain what detection approaches are utilized most to detect attacks in hospital environments. Research knows three types of IDSs:

- signature-based detection
- anomaly-based detection
- specification-based detection

The two best-known subcategories are signature-based and anomaly-based IDSs. Signature-based IDSs use predefined patterns of known attacks to detect intrusions in a pattern-matching approach. The major downside is that those systems can only detect known attacks. Even the smallest changes that modify the signature of the attack might evade detection. The upside is few false alarms.

The counterpart is anomaly-based intrusion detection which has drawn much interest in the research community. Those IDSs model the expected behavior of a system or network and warn in the case of deviation from baseline behavior. Advantages and disadvantages are contradictory: While this approach might detect even zero-day attacks, it is difficult to consider every borderline case in the baseline, which ultimately leads to a higher count of false positives. Other often-named challenges in the context of MCPS are limited sources of energy and constrained computational power. Often, especially in the case of wearable devices, those resources are already utilized by the device's primary purpose, so few resources remain for the intrusion detection algorithm. Moreover, even if one may argue that some wearables have an easily changeable battery, the need for energy-saving algorithms and protocols cannot get clearer for implantable medical devices (IMD). Consequently, motivated by these considerations, several research endeavors focus on energy and resource-efficient intrusion detection approaches (e.g., [24], [25], [26], [27]).

A third category, sometimes also considered a subcategory of anomaly-based IDSs, is specification-based intrusion detection [28]. In this approach, all possible behaviors of the given medical device are specified. The device's operation is then monitored. An alarm is triggered if the device transitions to an unspecified operating state. We decided to follow Mitchell and Chen's definition and consider specification-based intrusion detection as a standalone category [29] because the medical sector offers unique possibilities for specifications. It, therefore, enjoys special attention in the field of MCPS intrusion detection. The researchers promise that it combines the advantages of signature-based and anomaly-based detection, namely the ability to identify previously unknown attacks while limiting false positives and requiring less computational power than ML-based anomaly detection. However, very detailed knowledge of the monitored medical device is needed, and this approach is therefore associated with a high initial implementation effort.

Furthermore, hybrid approaches combine two or more variants into a new approach. Here it is essential to state that several authors combined different ML algorithms and called their approach hybrid. Since the distinction to, e.g., ensemble learning methods was too small from our point of view, we did not follow this subsumption. Therefore, we only classified an approach as hybrid if it comprised variants from different main categories (e.g., anomaly-based and signature-based).

2) WHERE IS THE ATTACK DETECTION SYSTEM LOCATED?

Classically, there are two locations where attack detection systems are usually placed. On the one hand, a host-based IDS (HIDS) runs on the device and monitors the station's operating system, processes, or logs. On the other hand, a network-based IDS (NIDS) inspects the network traffic and often monitors the traffic of all devices connected to the network. The locality of the NIDS, particularly in segmented networks, can, in turn, influence its effectiveness and therefore be decisive. Both locations have their advantages and disadvantages. An NIDS is able to detect external threats at an early stage, but the mass of data can cause limitations, especially in large networks. While an HIDS might not notice external threats as early as an NIDS, it might detect malicious insiders that remain hidden to NIDSs [28]. In addition to this distinction, we observed a third location often chosen by the researchers in the MCPS domain: cloud or cloudlet-based IDSs. Here, too, hybrid approaches are conceivable and in other sectors pervasive.

3) WHAT KIND OF DATA IS ANALYZED BY THE ATTACK DETECTION APPROACH?

This question often interrelates with the location of the detection system (or at least with the collector's location). At the network level, detection approaches might use metadata of captured packets or analyze the whole packet, more or less understanding the entailed sector-specific protocols. At the host level, various information about the operating system, processes, or log files can be evaluated. Of course, all this data can also be conglomerated in a cloud to be processed centrally.

TABLE 1. Digital libraries consulted for study selection.

Electronic Source	Results
ACM Digital Library	139
IEEE Xplore Digital Library	2116
ScienceDirect	933
Springer Link	1356
PubMed	810
Total	**5354**

4) WHAT ATTACK SCENARIO IS THE PRIMARY FOCUS OF THE DETECTION SYSTEM?

Frequently, detection approaches specialize in the defense against specific scenarios. This is because an outside attack is detectable by different indicators than an insider abusing valid privileges. We identified the scenarios with the greatest research interest and those that may be underrepresented in current research.

5) WHICH DATASETS AND SOURCES ARE UTILIZED TO EVALUATE THE EFFECTIVENESS OF THE DETECTION APPROACH?

Publicly available datasets make the detection approaches of different researchers comparable. Sometimes, however, researchers cannot find a dataset that fits their use case and look for alternatives. Some build test environments with simulators or real devices, while others generate data in other ways. We examined the approaches and the most used datasets and -sources in the field of MCPS attack detection.

6) WHAT APPROACHES GO BEYOND DETECTION AND ALSO INCLUDE PREVENTIVE MEASURES?

It is often of particular research interest to not only detect but also mitigate attacks as quickly as possible. This is also appealing in healthcare, as any attack might endanger human life. On the other hand, one of the biggest challenges in the field of attack detection, especially in the case of anomaly detection, is the false-positive rate. This gets even more relevant if automated mitigation measures are taken. By reviewing the relevant articles, we explored how researchers address the potentials and risks in this regard.

B. IDENTIFICATION OF RESEARCH

To capture the current state of research, the variety of terms used in the literature for networked medical devices alone necessitated a structured approach. We were not the first to find that IT security terms and definitions diverge in healthcare. Athinaiou et al. surveyed the IT security language and observed that definitions of concepts differed in health environments [30]. We identified 22 terms used in reference to such systems (Connected Health, Connected Healthcare, Digital Healthcare, e-health network, Healthcare

TABLE 2. Inclusion criteria used during study selection.

#	Inclusion Criteria
1	Research is peer-reviewed
2	Study is published and available in full length
3	Research is within the focus area (intrusion detection in the context of MCPS)
4	Study has been published before March 2023

TABLE 3. Exclusion criteria used during study selection.

#	Exclusion Criteria
1	Study is not written in English
2	Study is a duplicate result
3	Paper has been retracted
4	Paper published other than conferences, journals, patents, technical reports
5	Study lies outside the IT security domain
6	Study focuses on medical devices without hospital context

IoT-based Systems, Healthcare 4.0, (Industrial) Healthcare Systems, Internet of Health Things, Internet of Healthcare Things, Internet of Medical Things, IoMT, IoT-Health, Medical Cyber-Physical Systems, Medical CPS, MCPS, Medical Information Systems, Medical Internet of Things, Medical IoT, Medical Sensor Networks, Networked Healthcare, Networked Medical Devices, (Smart) Medical Devices).

While there are no precise definitions, it is our impression that term combinations of *medical/health* and *internet of things* (IoT) like IoMT, mIoT, or IoHT have been used to refer not only to medical devices in hospitals but also to devices used to monitor specific health values at home. In contrast, the term MCPS was used almost exclusively for medical devices in a hospital context. However, this observation did not apply to all publications, and we noticed a convergence of the device classes. Researchers hypothesize that all sensors monitoring patients' health parameters in hospitals will be connected to local gateway devices in the future [31]. This evolution can already be observed and is the reason for the prevalence of so-called medical device gateways in hospitals that connect medical devices to the hospital network. According to ENISA, these devices presently account for 34% of all devices in the healthcare sector [5]. Besides, it is quite similar to the convergence of general IoT and cyber-physical systems (CPS). NIST established in a special publication in 2019 that the concepts of CPS and IoT have become more and more equal and that the definitions can recently often be used interchangeably [32]. However, to clarify that this work focuses on detecting attacks on medical devices available for hospitals, we used the term MCPS.

In addition, we identified five expressions describing the detection of attacks (Detection, Network Security Monitor, Network flow, IDS, and Intrusion Prevention). The combined search strings were employed to search five electronic libraries. The results per library can be seen in table 1. In total, we obtained 5354 papers matching our search strings.

C. SELECTION OF PRIMARY STUDIES

Following Kitchenham et al., two authors performed a two-step screening of all obtained papers and selected those relevant to the research topic. To make the process comprehensible and verifiable, we defined the selection criteria in tables 2 and 3. In the first quantitative screening, the title and abstract of the publications were evaluated. The vast majority of the papers was excluded in this step. For the qualitative screening, 358 papers remained. The high rejection rate is attributable to the fact that many intrusion detection synonyms are also used in medical regard. Two examples of major fields in medical research are disease detection and monitoring of patients' health parameters utilizing various medical devices. Unfortunately, those terms could not be excluded from our search terms for obvious reasons, which led to a high rate of false positive results.

In the following qualitative screening, the full-text versions of the 358 papers have been consulted to single out those relevant to our research questions. The papers were screened by two researchers independently, and the resulting selection of included papers differed. The agreement has been measured using the Cohen Kappa statistic [33]. The initial value of the Kappa statistics was 0,826. Afterward, all disagreements were discussed and resolved. In the end, 118 papers were selected for data extraction.

D. DATA EXTRACTION AND SYNTHESIS

For data extraction, the remaining studies were read in full and categorized by the research questions defined in section III-A. Thereby, we were able to answer the questions as comprehensively as possible. Here we followed the recommendation of Kitchenham et al. and assigned one researcher as the data extractor and the other as the data checker. Emerging disagreements have been discussed, and all researchers have agreed on the final classification.

Finally, the results of the review were summarized. In the following section, we will provide the gained insights.

IV. RESULTS

We identified 118 papers that could contribute to answering the research questions. However, not every paper could be consulted to answer every research question. One example is the study by Ardito et al., who outline a framework but did not implement it or test it using a dataset [34]. Therefore, while we were able to use this publication to evaluate the proposed detection approach (RQ 1), it was not suitable for answering the question about the used data sources (RQ 5). The exact number of papers included in the evaluation of each research question is indicated in each subsection.

A. RQ 1–UTILIZED DETECTION APPROACH AND EMPLOYED TECHNOLOGY

We identified three main approaches in the context of MCPS attack detection: anomaly-based detection, signature-based detection, and specification-based detection.

TABLE 4. An overview of the different detection approaches.

Detection Approach	Paper	Count
Anomaly-based	Ahmed et al. [35], Akram et al. [36], Akshay Kumaar et al. [37], Alamleh et al. [38], Almaiah et al. [39], Alotaibi [40], Alrashdi et al. [41], Ardito et al. [34], Arfaoui et al. [42], Ashraf et al. [43], Astillo et al. [44], Awotunde et al. [45], Ayoub et al. [46], Balasubramanyn et al. [47], Basharat et al. [48], Bassene and Gueye [49], Cai et al. [50], Carreon-Rascon and Rozenblit [51], Chowdhury et al. [52], Fernandez et al. [53], Ferrag et al. [54], Fouda et al. [55], Gao and Thamilarasu [56], Ghourabi [57], Gupta et al. [58], Gupta et al. [59], Gupta et al. [60], Hady et al. [61], Hajder et al. [62], Hameed et al. [63], Hameed et al. [64], Hameed et al. [65], Haque et al. [66], Haque et al. [67], He et al. [68], Hei et al. [69], Hussain et al. [70], Igbe et al. [71], Iqbal et al. [72], Kamble and Gawade [27], Karthick Kumar et al. [73], Khan et al. [74], Khan et al. [75], Kilincer et al. [76], Kintzlinger et al. [77], Kumar et al. [78], Kumar et al. [79], Kumar et al. [80], Li et al. [81], Liaqat et al. [9], Mahler et al. [82], Manimurugan et al. [83], Mishra and Bagade [84], Mohammed and Aiheeti [85], Mowla et al. [86], Muhammed et al. [87], Nandy et al. [31], Nayak et al. [88], Newaz et al. [89], Newaz et al. [90], Odesile and Thamilarasu [26], Otoum et al. [91], Otoum et al. [92], Otoum et al. [93], Panagoda et al. [94], Priya et al. [95], Radoglou-Grammatikis et al. [96] Radoglou-Grammatikis et al. [97], Rahmadika et al. [98], Ram and Kumar [99], Rao et al. [100], Rao et al. [101], Ravi et al. [102], Rehman et al. [103], Saba [104], Saheed and Arowolo [105], Said et al. [106], Salem and Mehaoua [107], Schneble and Thamilarasu [108], Sehatbakhsh et al. [109], Sharma et al. [110], Singh et al. [111], Siniosoglou et al. [112], Spegni et al. [113], Tabassum et al. [114], Tahir et al. [115], Thamilarasu et al. [116], Thamilarasu et al. [24], Thapa et al. [117], Toor et al. [118], Wa Umba et al. [119], Wagan et al. [120], Wahab et al. [121], Wang et al. [122], Yan et al. [123], Zaabar et al. [124], Zachos et al. [125], Zubair et al. [126]	98
Specification-based	Abdulhammed et al. [127], Choudhary et al. [128], Fang et al. [129], Mitchell and Chen [29], Mitchell and Chen [130], Li et al. [131], Raiyat Aliabadi et al. [132], You et al. [133], Zhang et al. [134]	9
Signature-based	Boujrad et al. [135], Meng et al. [25], Mpungu et al. [136], Zhang et al. [137]	4
Hybrid	Begli et al. [138], Chen et al. [139], Dupont et al. [140], Meng et al. [141], Kolokotronis et al. [142], Lakka et al. [143], Tariq et al. [144]	7

As shown in table 4, most researchers focus on an anomaly-based detection approach (98). The majority proposes an ML algorithm they tweaked to be most suitable for MCPS (42). Often, the approaches consist of an optimized feature/dimensionality reduction algorithm and an ML algorithm that performs the actual detection. While most researchers substantiate why their approach works best (e.g., Saheed et al. with their swarm-based approach [105]), others focus on optimizing parts of their approach. E.g., Priya et al. measure the benefits of different dimensionality reduction approaches [95]. The detection algorithm then classifies the traffic, flow, or packet into malicious/benign (binary classification) or even categorizes it into specific attack groups. One example of the latter is the work of Mowla et al., which attempts to identify an attack and classify the attack type [86]. Astillo et al. focus on one specific MCPS: a diabetes management control system consisting of three separate components: a sensor that steadily measures a patient's glucose level (continuous glucose monitor (CGM)), an insulin pump, and a controller. Their detection approach first estimates the blood glucose level of the patient. Thereafter, estimated and actual values are compared and derived as features. Eventually, the classification module evaluates if the current event cycle is anomalous [44]. Khan et al. criticize that researchers have so far focused on optimizing accuracy and false alarm rate while no attention has been paid to interpreting the prediction model. Therefore, they use an explainable model that provides information about the features leading to the prediction. Their motivation is to help security personnel to react timely and in the right way to an alarm and to increase trust in their detection model. They explain this is especially necessary for the healthcare domain since there are too few security experts [74].

20 of the papers compare several anomaly-based approaches to one another and assess the advantages and disadvantages of the approaches in the context of MCPS. E.g., Newaz et al. developed HealthGuard, which utilizes four ML-based detection techniques (Artificial Neural Network, Decision Tree, Random Forest, k-Nearest Neighbor) [89]. The researchers compare the algorithms in terms of accuracy, precision, recall, and F1-score (test accuracy considering precision and recall). 14 researchers combine different anomaly-based approaches to a new, amalgamated approach. While most state how their approach improves the anomaly detection, Kintzlinger et al. emphasize that their proposition of a combination of ML algorithms and statistical methods performs worse than the use of statistical methods alone [77].

Another repeatedly seized approach is Federated Learning (17) which researchers use to address the challenges of healthcare data privacy (e.g., Otoum et al. [92], Thapa et al. [117], Ferrag et al. [54]). It is a machine learning technique that has recently attracted much attention – not only in medical applications – because it protects data privacy. Other ML approaches often store data centrally without taking privacy-preserving measures. This turns these central data stores themselves into lucrative targets. In contrast, Federated Learning establishes a global learning platform that combines the knowledge of locally available models. The process of training an algorithm runs over separate decentralized models. Local datasets are used without revealing private data. Federated learning can thus preserve the training dataset on the devices so that the patient's data is not needed for training

on the server side [93]. While several researchers include one network segment or a whole hospital in a local model, Gupta et al. propose a digital twin for each patient and train their local model on it. The advantage is that all collected data belong to a single patient, and the researchers can correlate more parameters [59].

Specification-based detection approaches are the second largest group, though by a large margin (9). We present three examples in the following: To detect maliciously acting devices instead of attacks, Mitchell and Chen devise a behavior specification-based approach. They define behavior rules and derive attack states from there. Subsequently, the researchers develop state machines. The authors promise this approach could detect unknown attacks while keeping the overhead and false positive rate low [130]. Refining this work, Abdulhammed et al. create a hardware approach (Field Programmable Gate Array (FPGA) chip) that employs behavior rules to detect anomalies [127]. Their approaches address the resource constraints of MCPS. Fang et al. also observed and analyzed the behavior of the monitored devices. They suggest a combined approach of fuzzy core vector machine and rough set (RS) as preprocessor (peculiarity: RS acts as a filter for apparent abnormal behavior) [129].

Exclusively signature-based approaches propose only four researchers in their publications. Meng et al. and Zhang et al. are two examples: Meng et al. cover the topic of decentralized detection for privacy reasons and outline a decentralized signature-based detection approach [25]. Zhang et al. combine the open source IDS *Snort* and the vulnerability scanner *Nessus* for an attack intention prediction [137].

Although signature-based detection may seem to be the least pursued approach, some researchers include it in a more general security strategy, combine it with another method (hybrid), or use it as a means of comparison. Dupont et al. wrote a protocol dissector for the IDS Forescout SilentDefense [140]. Magomedov recommends a signature-based approach for identified DICOM vulnerabilities [6]. Nguyen et al. designed a secure logger for medical devices with some detection capabilities. It consists of a dongle attached to the medical device that sends data to a remote cloud. The detection component focuses on packet or sequence tampering. Contrarily, the researchers consider compromised medical devices or devices sending compromised logs out of scope [145]. Radoglou-Grammatikis et al. compare their ML-based approach to Suricata loaded with attack signatures of Cisco Talos for the IEC 60 870-5-104 protocol. The signature-based approach performs better than most anomaly-based solutions presented in their work [97].

B. RQ 2–DATA COLLECTION AND PROCESSING LOCATIONS

Researchers choose different locations and thus varying data sources for their IDSs. We differentiated between the device, network, and cloud/cloudlet locations and combinations of two out of those (figure 1). It is essential to state that we chose the location network if network traffic was seized, the location device if data was collected and processed on the device (e.g., log data), and the cloud if data was collected in or from cloud services.

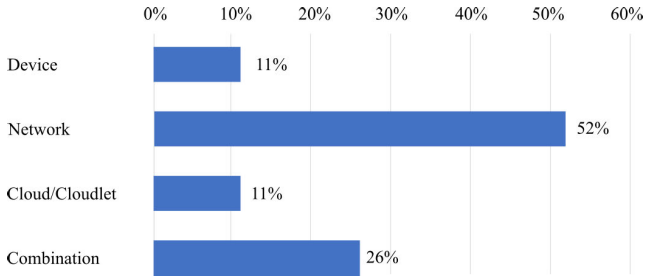

FIGURE 1. The chosen data collection location for the different IDS approaches. In total, 117 papers were analyzed. "Combination" consists of a mixture of two locations, where device and network make up 12%, device and cloud 4%, and network and cloud 10%.

Most researchers select the network as the sole location for their approach (52%). While a majority chooses a classical IP-based NIDS approach, some utilize particular circumstances of the healthcare sector or a specific MCPS. For instance, Gao and Thamilarasu propose a gateway device for an IMD and its programmer device. It acts as a man-in-the-middle and is supposed to detect attacks between those devices [56]. Mahler et al. developed an IDS specifically for a CT device. It intercepts traffic between the host pc and the device (on the can bus) [82].

The location cloud(-let) was chosen by eleven percent of researchers. This was often the case if researchers gathered health data from a manufacturer's cloud. Examples are Gupta et al. [59] and Newaz et al. [89], who correlate different vital signs of patients. The approach of Gupta et al. stood out since they took the first steps in matching network data and health data. From this, they assess the monitored user's behavior to detect abnormalities [58].

Similarly, eleven percent of researchers opted for a pure on-device approach. To meet the special requirements of the healthcare sector, many researchers focus on lower resource constraints while preserving the patients' privacy. A particular advantage of the location device is that researchers can benefit from the special conditions of hospitals and clinics. E.g., Ardito et al. tailor their approach to an electrocardiography (ECG) device and use its user interface to display warnings in case of an anomaly. Then, feedback is requested from the treating physician. In this way, the physician is warned as quickly as possible in dangerous situations, and in the event of a false positive result, the effects can be limited [34]. A disadvantage of the location is that to implement a HIDS on a medical device, most researchers rely on device-specific knowledge or access to source code. This limits the transferability and scalability of the approach in many cases.

Adding combinations of the locations device & network (12%) and device & cloud (4%), the number of researchers who combine the on-device approach with another

location (16%) is higher than the number of researchers who use a pure on-device approach (11%). Thereby, in total, 27% of researchers decided to include device-specific information in their detection approach. Astillo et al. present one example of a combination of device and cloud. In their federated learning approach, they collect the data directly from the Continuous Glucose Monitor and process it on the controller unit of the MCPS. To share the knowledge between similar setups (other diabetes management control systems), only a submodel is generated on the device and subsequently fused to a central model on a cloud server [44]. The approach of Mitchell and Chen is a combination of host-based and network-based detection. Every node in the network acquires a set of behavior rules and can monitor the behavior of its trusted peers. So every medical device is monitored while it is also part of the detection approach [130]. Meng et al. suggest to perform the detection on every node individually and recommend a blockchain as an exchange platform for necessary signatures and a list of blocked nodes. As every node could add signatures to the chain in this scenario, the authors propose a centralized trust management scheme [25].

Besides the aforementioned categories, we could also observe that some researchers neglect the location choice of data collection. Instead, they base their detection approach on existing datasets (further elaboration in section IV-E) in computing platforms and simulation environments such as Matlab and Simulink. In this case, the dataset dictates the collection location. Examples are: Akram et al. [36] and Begli et al. [138]. Others combine the toolboxes with different simulators or platforms. Chen et al. employ Matlab and a cloudlet mesh simulator to calculate and evaluate the optimal number of collaborating IDSs in their cloudlet mesh approach [139]. In contrast, other researchers embed the proposed detection approach in a holistic security concept for a realistic hospital environment and even consider hospital network specifics. One example is Lakka et al., who describe an incident management approach, complementing their swarm-based detection with signature-based detection and consolidating the data in a hospital SIEM. A layered model outlines what information is collected where, sent where, and processed where [143]. Khan et al. also consider how their approach could be rapidly deployed in many hospitals. To this end, they have developed a framework for deploying their approach as Infrastructure as a Service in the cloud and as Software as a Service in a hospital network [75].

C. RQ 3–INCLUDED FEATURES AND CHARACTERISTICS OF THE LEVERAGED DATA

In contrast to the IDS locations, we observed a higher variety in the examined features (figure 2). The majority of researchers base the detection on non-medical contextual information (50%), i.e., analyze technical data and transfer gained IDS-insights from other sectors to the medical sector. One often-used approach is the analysis of the network packet's contents. The medical sector is particularly interesting for ML-based detection approaches because of the resource constraints and the data masses generated by MCPS. Therefore, often observed research focuses are feature selection and hyperparameter tuning (e.g., Akshay et al. [37], Schneble and Thamilarasu [108]).

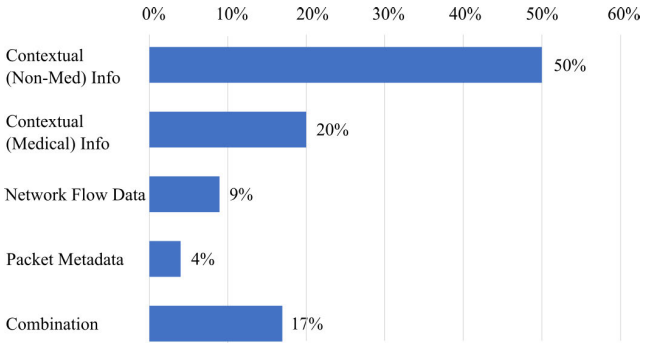

FIGURE 2. The type of data from which the features and characteristics were obtained. In total, 114 papers were applicable for the evaluation. "Combination" consists of a mixture of two data types, where network flow data and contextual (non-medical) data make up 13%, metadata and contextual information 3%, and metadata and network flow data 1%.

Remarkable is the high count of papers using contextual medical information from which researchers derive indicators of an intrusion. 20% of papers base their detection approach solely on such information. Mitchell and Chen were the first to incorporate medical context and correlations for attack detection (e.g., one proposed rule for conspicuous behavior is if the pulse is above a certain threshold during an analgesic request of the patient) [29]. Siniosoglu et al. utilize medical data such as ECG and arterial blood pressure [44]. Newaz et al. relate health values from different devices and interpret the results. They hypothesize that an attack usually targets one device at a time and that a deteriorating state of health should simultaneously affect various measured health values. If only single values deviate, they infer that this data must have been manipulated. E.g., if the patient's oxygen level drops due to health reasons, her heart rate would naturally also decrease. So if only one of the values changes, the IDS will detect an anomaly and raise the alarm [59]. Hady et al. propose a packet comprehension functionality: Their models recognize the heart rate, respiration rate, systolic blood pressure, diastolic blood pressure, blood oxygen, and more from captured network traffic [61].

Others utilize network flow data (9%) or packet metadata (4%) and claim that this is more suitable than inspecting all packets. Besides the already mentioned data masses in the health sector, some researchers give additional reasons. Fernandez et al. argue, for example, that their primary motivation for using network flows is the more and more encrypted data sent over the network, due to which inspecting packets would be pointless [53].

Several researchers combine two types of features in their detection approach to identify attacks (17%). One example is the expansion from the field of disease classification to attack detection on medical data, as Haque et al. pledge their approach can do both [66]. Siniosoglou et al. leverage

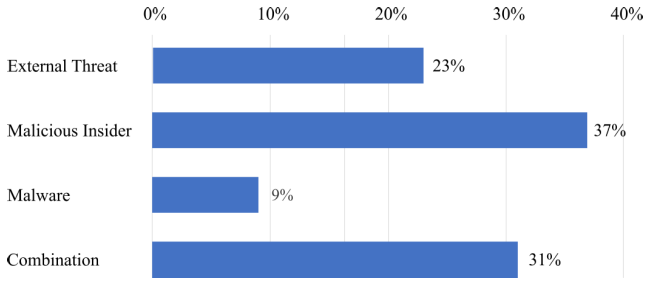

FIGURE 3. The detection approaches focused on different attack scenarios. In total, 113 papers were analyzed. Combinations consist of approaches promising to detect external and internal threats (25%), external and malware threats (3%), and internal and malware threats (3%).

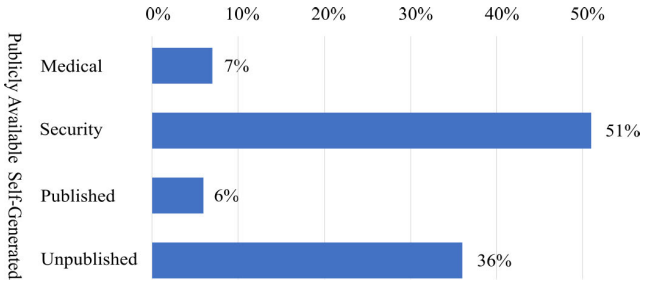

FIGURE 4. The four categories of datasets and -sources encountered in the reviewed publications. In total, 108 papers were analyzed.

this approach and propose two supplementary models: one model to detect intrusions from network flow data and one model to detect anomalies from healthcare data [112]. Sehatbaksh et al. and Rao et al. follow entirely different approaches. The former propose to use the electromagnetic (EM) signals generated by the monitored medical devices during operation to distinguish between normal and malware-infected MCPS [109]. The latter suggest monitoring system operations. They hypothesize that a malware infection is identifiable by monitoring processes and other system parameters (especially the execution time) of a medical device [100].

D. RQ 4–ADVERSARIAL FOCUS

Many researchers limit the applicability of their work by making assumptions about attack types, targets, and locations, among other things. We have investigated which defense scenarios the detection approaches focus on. Here, we differentiated between external threat actors, malicious insiders, attack scenarios utilizing malware, and approaches focusing on detecting more than one attack scenario (figure 3).

Most researchers concentrate on insider scenarios (37%) or the combination of internal as well as external threats (25%). 23% focused on the sole detection of external threats. 9% of the researchers centralize the detection of malware infections. It is essential to state that we also included such papers in the category of insiders that do not explicitly mention such a specific attack scenario as a limitation, but require an attacker to have access to the network or a device (e.g., the attacker is able to spoof a mac address or the drug dosage is monitored for manipulations). So an external attacker that has already compromised an MCPS and can be detected as late as he laterally moves in the network or interferes with the normal function of the MCPS, is considered an insider in our classification scheme. The behavior-based approach of Fang et al. contrasts this scheme, as it promises to defend against external attackers. The model that they call *detecting illegal behavior (DIB)* focuses on the detection of maliciously acting accounts and devices (e.g., accounts that have been taken over through shoulder-surfing attacks) [129]. As it is technically impossible to differentiate between such a compromised account and a real insider sending malicious commands, we decided to follow our definition. While most other behavior-based detection approaches concentrate on the detection of insiders, Mitchell and Chen additionally claim to be able to detect malware, as they estimate malware to change the behavior of an infected device as well [130].

E. RQ 5–DATASETS USED FOR VALIDATION

Researchers need data to train and test detection approaches (especially if they are ML-based). There is an additional benefit when multiple researchers use the same dataset, as the different detection methods become comparable. Choosing a dataset fitting the task is crucial since datasets are generated for specific purposes. We have organized the used datasets and -sources into two categories, each with two subcategories, as shown in figure 4. The first category includes approaches that utilize publicly available datasets. Here we differentiate between security and medical datasets. The second category deals with publications that have created their data themselves. While datasets from some approaches are available to the community, many remain unpublished.

1) PUBLICLY AVAILABLE DATASETS

In non-health domains, researchers usually train and test novel IDSs utilizing publicly available security datasets. Our analysis shows that 51% of the researchers also follow this approach. Figure 5 presents the different datasets. 8% of the researchers in this group utilize the KDDcup-99 dataset. This dataset was developed for the KDD-cup competition in the year 1999, whose goal was to develop an NIDS [146]. Several problems, such as redundant records, have been reported, and the successor, the NSL-KDD dataset, was released in 2009 [147]. 18% of the researchers in this group use this dataset. Both datasets contain several IT protocols such as HTTP, SMTP, and FTP. Among others, Khan et al. bemoan the deficiencies of missing the latest attack vectors in the NSL-KDD dataset [74]. The Canadian Institute for Cybersecurity (CIC) published several datasets promising to have more recent attacks resembling real-world data. Their top priority varies from dataset to dataset. In the 2017 data set, they provided realistic background traffic and simulated the behavior of 25 users [148]. In the 2018 dataset, they focused on insider attacks and provided system logs of every machine [149]. Most researchers relying on CIC

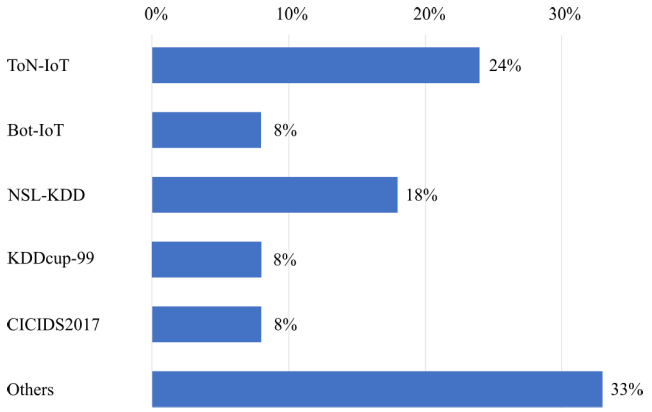

FIGURE 5. The different publicly available network traffic datasets used. During our analysis, we encountered 18 different datasets that were used 72 times. Some research groups used more than one dataset and were therefore assigned to more than one category.

datasets in the examined works use the CIC IDS 2017 dataset (8%). It consists of raw packets in PCAP files as well as labeled flows [148]. However, none of the presented datasets comprise IoT or MCPS protocols. The University of New South Wales (UNSW) fill the gap with their datasets ToN-IoT [150] and Bot-IoT [151]. In these datasets, a real-world network environment containing both IT and IoT devices was mimicked. Besides the network traffic, the researchers from UNSW provide Windows and Linux audit traces and telemetry data for the IoT services. Their IoT testbed consisted of various devices, among others: a fridge, a garage door opener, a thermostat, a GPS tracker, a motion sensor, and a weather station [150]. MCPS, however, have not been included. The ToN-IoT dataset, by 24%, is the most used dataset, while the Bot-IoT dataset is employed by 8% of the researchers that rely on publicly available datasets.

Some researchers employ the medical sector only as motivation and ignore the discrepancy between real network traffic in hospitals and the datasets they choose to support their detection approach. Others point to the absence of MCPS traffic in the dataset and handle the inadequacy differently. For instance, Schneble and Thamilarasu explain that in the context of MCPS, two aspects are crucial to keeping the detection latency low: Feature selection and reducing the amount of data processed by the IDS. Hence, to test the effectiveness of their feature ranking and selection algorithm, they consult the MNIST digit recognition dataset. This dataset contains 60,000 handwritten digits. They choose this dataset, among other reasons, because of the large feature space and the easy access to the data [108]. In contrast, Ferrag et al. explicitly determine the MNIST dataset unsuitable for training and testing IDSs in the context of medical devices [13]. Hameed et al. state that their approach is only applicable for detecting MCPS in a real environment if it is properly adapted prior to deployment [63]. Tabassum et al. use the datasets KDDcup-99 and NSL-KDD and merge their self-generated IoT traffic to cope with the missing IoT traffic in named datasets. However, they do not explain which MCPS they employed for the generation [114].

Some researchers harness medical datasets containing patient and medical data to identify attacks from those datasets (7%). The most commonly used dataset is the MIMIC III dataset, which contains health-related data of forty thousand patients who received intensive care in a hospital in Israel [152]. 25% of the researchers in this group used this dataset. While the researchers found the specifics of the medical data particularly valuable for attack detection, the drawback is that none of these freely available medical datasets contain attacks. Therefore, alternative ways must be found here as well. One idea given by Siniosoglou et al. is to use two distinct datasets to train their neural network: A publicly available medical dataset, and the UNSW-NB intrusion detection dataset for network flow data [112].

2) SELF-GENERATED DATA(SETS)

Many researchers generate their own data(-sets) and work with that data without publishing it afterward (36%). While this results in the fact that subsequent studies cannot be compared to their work, the reasons given are manifold. On the one hand, this data often results from cooperation with hospitals and could reveal real patient data. One example is Boddy et al., who captured network traffic in a UK hospital and depict the complexity of the network infrastructure in a visualization approach [153]. Even if this data could be anonymized, many argue that hospitals prefer to be on the safe side and not risk the exposure of any patient data. On the other hand, the data might be especially suited to an approach or just randomly generated, as in the work of Mitchell and Chen. They generated random data following their devised state machine [130]. This data would have had no benefit for any other researcher, as their states are unique to their approach.

As we already addressed in section IV-B, researchers used computing and simulation environments to test their new attack detection algorithm on existing datasets. Another approach is to utilize simulators and frameworks to model an even more realistic MCPS environment. Among these approaches are those designed for a medical environment and those whose original purpose is different. Two examples of non-medical simulators are presented in the following. Meng et al. operate a publicly available tool to generate attacks on wireless networks. The attacks are not specifically adapted to MCPS environments [25]. Thamilarasu et al. employ Castalia, a simulator for WSN and WBANs, in several papers [26], [56], [116]. Such toolboxes and frameworks originally developed for other purposes have certain limitations regarding MCPS simulation. Therefore, several researchers adapt various open-source medical device simulators to their needs or implement their own medical device simulators. Astillo et al. operate the UVA/Padova Type 1 diabetes simulator that has been approved by the U.S. Food and Drug Administration (FDA) in their testbed and generated

their test data with it. They also use an extended simulator version to induce artificial attacks [44]. Sehatbakhsh et al. leverage open-source code to deploy a syringe pump on various architectures. They found a buffer-overflow vulnerability in the syringe pump's source code that they were able to exploit [109]. Raiyat Aliabadi et al. employ OpenAPS, an open source Smart Artificial Pancreas [132]. They use fault injection as the source for unknown attacks.

Recent research efforts concentrate on the standardization of medical device inter-connectivity to address the heterogeneity of network protocols used by medical devices in hospitals mentioned in section I This is not only an IT security challenge. One project that has already made some progress is the community implementation of an integrated clinical environment, OpenICE. It provides a framework for the integration of medical devices into an integrated clinical environment (ICE). The developers even promise to be able to connect legacy devices to their ecosystem. For that, they developed adapters for those devices and a novel network protocol [154]. Some security researchers propose IDSs for networks based on OpenICE. Li et al. use OpenICE to simulate future medical devices and accomplish a data flow analysis in an OpenICE network [131]. Fernandez et al. analyze network flows of malware outbreaks in such environments [53].

To mimic real-world hospital conditions even better, many researchers employ actual medical devices in a testbed. Figure 6 shows the different devices. While the medical devices most used are blood pressure sensors (12%) a clear favorite could not be determined. Various research groups cover multiple devices. A protruding example is the testbed of Fang et al. which contains 21 different medical devices and a malicious access point to capture network traffic. From the device behavior, they derive 21 behavior rules. Instead of attacking the devices, they define operation rules for each device and specify some operation rules as normal and the remaining as abnormal behavior [129]. This way, no real attacks are conducted. Instead, some behavior is defined as malicious. The detection system of Kintzlinger et al. is explicitly designed for attacks directed at programmer devices for implantable cardioverter defibrillators. They cooperated with two cardiology experts from a university medical center to create malicious programmings [77]. Yan et al. analyzed a medical shoe with 99 sensors attached. It is designed to detect the instability and balance of patients. The researchers statistically correlate the data of the different sensors in a shoe and, thereupon, identify attacks using anomaly detection [123].

Similar to Fang et al. before, we observed that many research endeavors were conducted utilizing household IoT devices rather than medical devices for data collection [129]. One example is Gupta et al., who built a conjoined testbed consisting of medical devices such as pulse oximeters and smart home devices like a fridge and a door sensor [58].

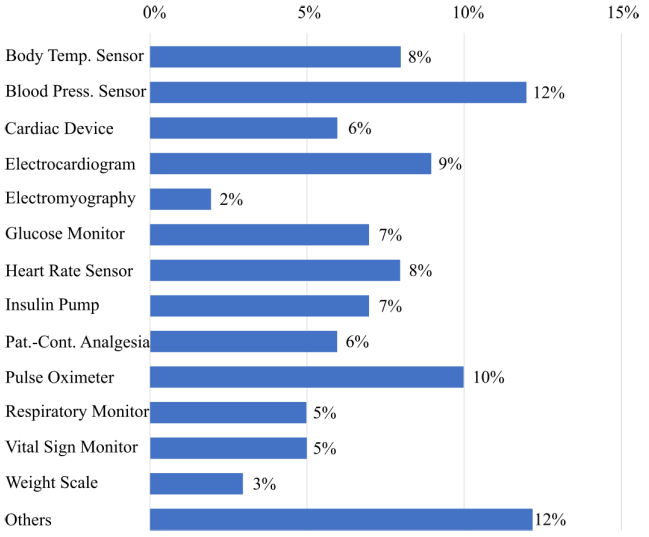

FIGURE 6. The different medical devices deployed in the testbeds of researchers. A total of 23 devices were used in 86 cases. Since several research groups analyzed more than one device, the percentages refer to the number of cases used (86) and not to the count of individual devices (23).

The same phenomenon occurs in the field of malware detection. Since there is little to no research on MCPS-specific malware, those researchers investigating malware outbreaks in clinical environments fall back on existing malware samples. Some utilize IT malware (e.g. Chowdhury et al. [52]), others use malicious android APK packages and explain that there are many mobile devices using android in hospitals [40].

Only six percent of research groups publish their generated datasets of MCPS-specific traffic. Nguyen-An et al. create an IoT traffic generator named IoTTGen. Their focus is smart home IoT as well as biomedical IoT. They analyze the behavior of smart homes and medical devices to build templates for those devices. The generator also allows adding new devices, if the traffic patterns are known. To generate anomalous packets, they extract attack traffic traces from the Bot-IoT dataset and inject them into their generated data. Since the Bot-IoT dataset does not contain MCPS-specific attacks, this generator cannot generate such attacks either. And since one finding in this work is that significant differences between the traffic of smart home devices and medical devices exist [155], it stands to reason that traces of attacks will differ as well.

Three dataset developers have focused on specific protocols or technologies. Radoglou-Grammatikis et al. present a IEC 60 870-5-104 protocol dataset. It contains protocol-specific attacks. They use the IEC Testserver to deploy their MCPS devices without specifying what devices were modeled in detail [97]. Zubair et al. provide a Bluetooth-enabled medical device dataset. They record Bluetooth network traffic and generate flow data from such devices - explicitly excluding the collection of patients' exact health data. The attacks performed during the data recording are also

Bluetooth-protocol-specific [126]. Hussain et al. focused on Message Queuing Telemetry Transport (MQTT) traffic and developed a tool for generating MQTT-based MCPS Traffic. The result is provided as an open-source dataset [70].

Two self-generated and published MCPS datasets have already been reused by other researchers: Ahmed et al. operate the Libelium Mysignals healthcare kit to generate their dataset. This kit provides a platform for the development of medical devices and eHealth applications. The researchers use three available health sensors in their testbed. Just their attacks are not medical protocol specific. Their ECU-IoHT dataset provides the recorded network packets in PCAP format, and network flows recorded using Argus [35].

Hady et al. record their testbed's network traffic, consisting of several small medical devices, and extract traffic flows and patient data from it. This recording is published under the name WUSTL-EHMS dataset. Among their carried-out attacks is the manipulation of medical data. Thereby, they directly integrated attacks on medical network traffic in their dataset, even if those are limited to spoofing and data modification from a MITM position [61]. In addition, their WUSTL-EHMS dataset is the dataset from the category of self-generated and published datasets in our survey that has been used most often by other researchers to detect attacks on MCPS (4).

F. RQ 6–ATTACK PREVENTION ENDEAVOURS

Attack detection is often closely associated with attack prevention since attackers and malware act fast, and a manual response often results in data loss or, in the case of the medical sector, patient harm. Therefore, a timely reaction is an often invoked point. Troublesome is that an automatic reaction based on a false positive might also harm a patient. One example is a higher-than-usual drug dosage given to a patient because of a life-threatening condition. If an IDS identifies this as an overdose attack and preventively interrupts medication delivery, the patient might die. Researchers have to consider these exceptional circumstances and come up with sector-specific solutions. Out of the 118 primary studies we reviewed, only 14 studies address attack prevention or mitigation. Others, such as Kumar et al, see the need for attack mitigation but choose to merely alert an administrator if an attack is detected and take no further action to thwart it [78].

Most preventive approaches (9) leverage software-defined networking (SDN). (Férnandez) Maimó et al. propose a decision and reaction module in their approach. It consists of a rule-based decision component and a reaction and notification component. Utilizing network function visualization and SDN, medical devices can be isolated automatically. They emphasize that their approach is not to prevent the actual attack but to reduce the reach of the attack by preventing the attacker or malware from accessing more devices [53]. This strategy is also chosen by most other SDN-based prevention and mitigation approaches.

Others concentrate on preventing a specific attack vector in a specific environment. E.g., Thapa et al. utilize mitigation SDN rules to react to ransomware spread in an ICE [117]. Similarly, Bassene and Gueye focus their work on detecting DDoS attacks against hospital networks. They as well propose the utilization of SDN [49], but unlike the previous, their approach excludes entire subnets to counter this specific attack type.

Radoglou-Grammatikis et al. are part of the few who discuss the potential consequences of automatic preventive measures. They draw attention to the fact that an attack might come from a device still used for legitimate health-related operations. Their notification and response module weighs this risk of causing higher costs for the healthcare organization against the threat of the detected attacks. Eventually, it decides whether to isolate the device via automatically generated and applied firewall rules, or simply to report it to an administrator and ultimately have that administrator make the mitigation decision [97].

One example of a non-SDN-based approach is MedMon. MedMon is placed in a man-in-the-middle position between a controller and a wirelessly-connected medical device. Attack prevention works by jamming the identified malicious wireless connection. Regarding the option of a false positive, MedMon can be operated in different modes. If a valid connection from the controller to the insulin pump in the example of the researchers is jammed, the patient can manually deactivate the jamming [134]. Since insulin delivery does not have to occur within seconds, a patient can usually react to a warning. Therefore, this approach might be suitable for this particular device type. Contrarily, it might not be suitable for medical devices with other preliminary requirements.

Another non-SDN-based, innovative approach by Rao et al. proposes a new resilient design for MCPS. They suggest to employ different operating modes in the MCPS architecture. Threat mitigation is realized by automatically changing the operating mode based on calculated risk values. In 2018, they presented the idea of a so-called multi-modal system in the form of a pacemaker [100], while in 2019, they expanded the idea to an insulin pump [101]. Carreon-Rascon refined it and added self-healing capabilities to the system. In addition to the operational modes and threat mitigation policies, self-healing policies are proposed and linked to the tasks of the different modes. Once the steps of the active mode have been executed, it is possible for the MCPS to switch to the next lower-risk mode and execute the self-healing tasks coupled to this mode [51].

V. DISCUSSION AND IMPLICATIONS

Overall, many good reasons and motivations for intrusion detection in the medical sector have been published. It is clear that the healthcare sector is receiving special attention, and many argue that particular challenges require special solutions. In the following, we use the knowledge gained on the state of research to discuss obstacles and limitations of attack detection for MCPS. By deriving five future research

topics (A-E), we would like to support prospective research projects to take a targeted direction.

A. CAPTURING THE HEALTH SECTOR-SPECIFIC REQUIREMENTS FOR ATTACK DETECTION

The results show that the majority of researchers sees the difficulties of attack detection in the healthcare domain as detecting attacks with a low false positive rate, with as little computing power as possible while preserving patient privacy. The, by far, most popular approach is anomaly detection, while only a few researchers discuss options, how understaffed IT security personnel could handle results containing false positives. Overall, we observed that many researchers assume different conditions and circumstances in MCPS environments. Especially, technical differences between healthcare networks and those in other sectors have received little attention in research to date. Therefore, we identify the need to determine the requirements to which detection approaches in the medical field must adapt.

One main difference is the use of medical device gateways, which connect medical devices to hospital networks. Such a setup could lead to difficulties since, for example, agent-based approaches could not be easily deployed to such architectures. This also applies to innovative approaches that operate by combining local and global predicates. If, for instance, in an intelligent agent-based approach, such an agent can investigate a suspiciously-acting device, how could legacy devices be included without involving all their manufacturers? Furthermore, it is unclear to the research community if medical devices use encryption. As illustrated in section IV-C, some researchers assume that much of the traffic in a hospital is encrypted and propose a flow-based approach in response to this assumption. In contrast, other researchers like Hady et al. derive patient data from captured network traffic and assume that this traffic is sent unencrypted from medical devices to servers [61]. However, performing deep packet inspection (DPI) in the case of encrypted traffic (e.g., by implementing application layer gateways to break up encryption) is aggravated in the MCPS environment, as security engineers cannot easily place certificates on medical devices. Approaches that rely on DPI must take that into account. As a first future research topic, we see the need for a comprehensive study of the unique constraints, technical characteristics, and challenges of hospital networks, along with connected medical devices, in contrast to other IT and OT environments.

B. CREATING MCPS-SPECIFIC ATTACK DETECTION DATASETS

Researchers deal with the scarce information situation differently. Some leverage the diversity typical for the healthcare sector solely for motivational reasons. Others do not place much emphasis on where and how data is collected. Instead, they use existing, often outdated datasets that do not fit the field or their motivation and ignore any differences. Again other researchers find 'creative' ways to replicate individual features of hospital networks and test specific parts of their approach. One example is the debatable use of the MNIST digit-recognition dataset to reenact the high feature dimensionality in the health sector. Either way, detection based on real health-specific protocols is rarely conducted, leading to limited portability of detection approaches from outside the medical domain. Moreover, it leads to uncertainty about whether the supposedly most suitable approach will be the best fit in a real hospital environment. ML-based IDSs must, most certainly, be retrained to prevent an increased false positive rate in a real-world environment. Furthermore, even the more recent datasets (e.g., CIC IDS 2017/2018) are often unsuitable for detecting attacks on medical devices since they do not contain IoT or IIoT traffic. Even if such datasets exist (e.g., TON-IoT or Bot-IoT), they might not be suitable for the health domain, as we saw that MCPS traffic significantly differs from other IoT traffic. There are several health-specific protocols (e.g., HL7 and DICOM [6], [140]), but only exceedingly few of these protocols are part of the datasets examined. Problematically, current adversaries are increasingly attacking application-layer protocols, as discussed by Hussain et al. [70]. Another factor not covered in current datasets is that different real-world attackers would behave differently. While several researchers, among other things, focus on detecting port scans or denial-of-service attacks, APT attackers would act much more stealthy. The first steps of recognizing the differences in the attacker's modus operandi were taken by Mitchell and Chen, who consider this fact with their attacker archetypes (reckless, opportunistic, and random attacker) [130]. Thamilarasu, too, takes the attacker's behavior's impact on the effectiveness of the detection into consideration [116]. However, these researchers use simulations for their distinctive environment. A dataset containing such characteristics has yet to be developed.

In addition to the uncertainty about the transferability to the real world, the lack of fitting datasets limits the comparability of the approaches. When comparing ML-based approaches, it is common to compare performance indicators such as accuracy, precision, and recall. Many of the papers have calculated and reported the corresponding values in their evaluation. However, we have refrained from correlating papers based on these metrics in this paper. On the one hand, this is because often, not the same datasets were used for training and testing of the individual algorithms so that, at most, a small group of algorithms could be compared to each other. On the other hand, often further assumptions were made about attackers, attacks used, or the granularity of the classification (as described in section IV-D). These assumptions limit the applicability of the algorithms to single-use cases and further reduce the comparability to other algorithms. Sharma et al. reacted to this and built a modular framework with a benchmarking suite. This could help future researchers to easily test their new detection algorithms and compare them directly to the work of other researchers [110]. But since this framework represents a novelty, the community

must first accept it. Furthermore, this suite also relies on the existing datasets, and while it takes an important step for comparability, it is not a comprehensive solution to this concern.

We also observed a trend to utilize distributed and federated learning approaches. It is crucial to point out that these models have specific requirements for datasets and that current datasets do not fulfill them.

In conclusion, the lack of appropriate datasets is a major obstacle to developing attack detection in the healthcare sector. From our point of view, an attack detection dataset should include three things to be suitable for the health domain. It should: (a) incorporate health-specific protocols, (b) model different attacker behavior, and (c) be suitable for specific scenarios and techniques, such as distributed and federated learning. The generation of such MCPS-specific datasets has to be addressed in the future. Therefore, we proclaim it as the second future research topic.

C. ADVANCING STANDARDIZATION PROJECTS

In addition to capturing the current state and the characteristics of the healthcare sector and mapping that state into datasets, we see the need to get to the root of the increasing diversity and the individual technology that makes IT security in healthcare so difficult. Therefore, efforts to standardize the sector's digital infrastructure must be intensified. Initiatives such as OpenICE are commendable. However, OpenICE was developed without consideration of security [145]. Additionally, intrusion detection in OpenICE-based networks will not be easily transferable to real hospital networks, as the network protocols are unique to the OpenICE environment.

The urgent need for standardization also applies to the device level. While it seems unsurprising to find the majority of researchers choosing the network as the data collection location (corresponding to the insights into the heterogeneity of medical devices discussed in section I), many researchers are examining single medical devices and designing specially adopted host-based detection approaches. This suggests that despite the hurdles in this area, many researchers would like to take advantage of the insights that device data can provide. One example of the many possibilities is the implemented feedback reaction to a detected anomaly by Ardito et al. [34] discussed above. However, the heterogeneity of devices currently means that a separate solution is required for each type of device. That is why most researchers propose an HIDS focused on a single or few device types (e.g., a smart artificial pancreas [132], a smart-connected-pacemaker [100], or a diabetes management control system [44]). The transferability of these approaches to the real world and, in particular, scalability are problems that are often not addressed by researchers. Therefore, manufacturers should also incorporate security considerations into the development of devices. Device and log data has to be made accessible to security experts in a standardized way. We ascertain advancing standardization ventures, therefore, as the third future research topic. As explained, this applies to both the device level and the network level.

D. CONNECTING TECHNICAL AND MEDICAL DATA FOR ATTACK DETECTION

In addition to the technical aspects of healthcare networks, some researchers explored the potential of medical context in various forms for intrusion detection. The promised benefits were manifold. E.g., in the case of a syringe pump, medical context could provide insights into a too-high dose for a patient and thereby recognize not only technically novel attacks and malicious insiders but also simple mistakes of health personnel. However, any initial attacker efforts or intrusion attempts might go unnoticed in these approaches. An attacker is only discovered if a device is already compromised and she tries to manipulate the care process. We have presented initial approaches for combined detection based on network traffic and medical data. However, detection has taken place independently and based on unrelated data sources. The genuine and thorough integration of the medical context with the detection based on technical features and, thus, creating a holistic approach is the fourth future research topic.

E. DRIVING RISK-AWARE ATTACK PREVENTION

During this survey, we observed that automatic intrusion prevention in the medical sector is an area that is handled even more carefully than in other sectors. The reason lies in the high stakes at risk: Lives depend on the system's proper functioning. While in other domains, a quick shutdown of a system that is most likely compromised may be just the right response in the risk assessment, an MCPS might still provide life-sustaining measures despite a compromise. Thus, the reaction must be weighed quite differently in this domain. As presented in section IV-F, there are very few research groups that address prevention and mitigation at all. The vast majority of them use the isolation capabilities that their SDN approach provides. While this does not necessarily mitigate the attack, it can stop potential lateral movement. Especially in the context of malware (esp. ransomware), this can be very valuable. However, the implications for the further functioning of isolated medical devices are rarely considered. Other endeavors propose individual solutions for single medical devices. While these preventive approaches are often innovative, they are tailored to the specific device type, and their risk assessment is not (easily) transferable to other devices. A plausible example is the IDS for an insulin pump, which notifies its user in case of an anomaly. The user can override the preventive measures and thus correct a false detection if necessary. This procedure would be fatal in the case of a pacemaker, for example, because here, it is important to react very promptly to anomalies. If the user is consulted first, it is questionable whether she can respond in a timely manner (or at all).

Since attackers and malware make no distinction between hospitals and other targets, these considerations and

difficulties must not lead to a neglect of prevention. Just as in other fields, a quick but well-thought-out response in the event of an attack is essential in the medical field. Hence, a fundamental discussion about intrusion prevention in the medical domain, the sector-specific requirements, and how it can succeed despite the high risks has to be conducted. We conclude that this is the fifth future research topic.

VI. CONCLUSION

Already in 2012, Clark and Fu denounced two challenges in the context of the security of medical devices: "(1) computer security researchers seldom have access to real medical devices for experimentation, and (2) the computer security community is largely disjoint from the biomedical engineering community." [156] These challenges persist to this day.

In this paper, we conducted a structured literature review by following the guidelines of Kitchenham et al. We found the synonyms for MCPS to be manifold and many of the security terms to be used in other respects in the medical domain. Most researchers focused on an anomaly-based detection approach at the network layer. The detection of malicious insiders was the primary focus. Several researchers used publicly available datasets for training and testing their algorithms. Others criticized the lack of suitable datasets and developed testbeds consisting of various medical devices. While some medical devices were used by multiple research groups, we observed no clear preference. Based on the results, we identified five research gaps. We discussed why it is necessary to examine the special conditions of hospital networks, the MCPS deployed within them, and the contrasts to other IT and OT environments. Furthermore, we see an urgent need for the creation of MCPS-specific datasets. Only with these sets researchers can attribute to the requirements and the unique possibilities of the healthcare domain. Alongside this, we see the need to support and expand MCPS standardization projects. Moreover, the medical domain offers an excellent opportunity to fortify attack detection based on technical features with medical context, thereby creating a holistic approach. Last but not least, a fundamental discussion should be held about the challenges of intrusion prevention in the medical domain and how it can succeed despite the high risks. We are confident that by countering these challenges, IT security in hospitals can be enhanced, and patients' lives can be protected.

REFERENCES

[1] P. Bischoff. (2021). *Ransomware Attacks on us Healthcare Organizations Cost $20.8 BN in 2020*. Comparitech. Accessed: Oct. 25, 2022. [Online]. Available: https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

[2] B. Filkins, "Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon," *SANS Inst.*, vol. 42, pp. 1–18, Jan. 2014.

[3] I. Gartner. (2021). *Gartner Predicts by 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans*. Accessed: Oct. 25, 2022. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

[4] L. Coventry, D. Branley-Bell, E. Sillence, S. Magalini, P. Mari, A. Magkanaraki, and K. Anastasopoulou, "Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour," in *Proc. Int. Conf. Hum.-Comput. Interact.* Cham, Switzerland: Springer, 2020, pp. 105–122.

[5] *ENISA Threat Landscape 2021*, Eur. Union Agency Cybersecur., Athens, Greece, 2021.

[6] S. G. Magomedov, "Software for analyzing security for healthcare organizations," in *Futuristic Trends in Network and Communication Technologies* (Communications in Computer and Information Science), P. K. Singh, G. Veselov, V. Vyatkin, A. Pljonkin, J. M. Dodero, and Y. Kumar, Eds. Singapore: Springer, 2021, pp. 181–189.

[7] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Softw. Eng.*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987.

[8] I. Gartner. (2022). *Gartner Market Guide for Operational Technology Security*. Accessed: Dec. 8, 2022. [Online]. Available: https://www.forescout.com/gartner-market-guide-for-operational-technology-ot-cybersecurity/

[9] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," *Comput. Commun.*, vol. 160, pp. 697–705, Jul. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366420312044

[10] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, Aug. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864817302900

[11] J. P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing Internet of Medical Things systems: Limitations, issues and recommendations," *Future Gener. Comput. Syst.*, vol. 105, pp. 581–606, Apr. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X19305680

[12] T. Tervoort, M. T. De Oliveira, W. Pieters, P. Van Gelder, S. D. Olabarriaga, and H. Marquering, "Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: A scoping review," *IEEE Access*, vol. 8, pp. 84352–84361, 2020.

[13] M. A. Ferrag, L. Shu, and K.-K.-R. Choo, "Fighting COVID-19 and future pandemics with the Internet of Things: Security and privacy perspectives," *IEEE/CAA J. Automa. Sinica*, vol. 8, no. 9, pp. 1477–1499, Sep. 2021.

[14] N. M. Thomasian and E. Y. Adashi, "Cybersecurity in the Internet of Medical Things," *Health Policy Technol.*, vol. 10, no. 3, Sep. 2021, Art. no. 100549. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2211883721000721

[15] S. S. Hameed, W. H. Hassan, L. A. Latiff, and F. Ghabban, "A systematic review of security and privacy issues in the Internet of Medical Things; the role of machine learning approaches," *Peer J. Comput. Sci.*, vol. 7, p. e414, Mar. 2021. [Online]. Available: https://peerj.com/articles/cs-414

[16] Y. Rbah, M. Mahfoudi, Y. Balboul, M. Fattah, S. Mazer, M. Elbekkali, and B. Bernoussi, "Machine learning and deep learning methods for intrusion detection systems in IoMT: A survey," in *Proc. 2nd Int. Conf. Innov. Res. Appl. Sci., Eng. Technol. (IRASET)*, Mar. 2022, pp. 1–9.

[17] F. Pelekoudas-Oikonomou, G. Zachos, M. Papaioannou, M. de Ree, J. C. Ribeiro, G. Mantas, and J. Rodriguez, "Blockchain-based security mechanisms for IoMT edge networks in IoMT-based healthcare monitoring systems," *Sensors*, vol. 22, no. 7, p. 2449, Mar. 2022.

[18] C. Eliash, I. Lazar, and N. Nissim, "SEC-C-U: The security of intensive care unit medical devices and their ecosystems," *IEEE Access*, vol. 8, pp. 64193–64224, 2020.

[19] M. Kintzlinger and N. Nissim, "Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems," *J. Biomed. Informat.*, vol. 95, Jul. 2019, Art. no. 103233. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1532046419301522

[20] P. Ghosal, D. Das, and I. Das, "Extensive survey on cloud-based IoT-healthcare and security using machine learning," in *Proc. 4th Int. Conf. Res. Comput. Intell. Commun. Netw. (ICRCICN)*, Nov. 2018, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/8718717/

[21] S. M. W. Umba, A. M. Abu-Mahfouz, T. D. Ramotsoela, and G. P. Hancke, "A review of artificial intelligence based intrusion detection for software-defined wireless sensor networks," in *Proc. IEEE 28th Int. Symp. Ind. Electron. (ISIE)*, Jun. 2019, pp. 1277–1282.

[22] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.

[23] B. Kitchenham et al., "Guidelines for performing systematic literature reviews in software engineering version 2.3," *Engineering*, vol. 45, no. 4ve, p. 1051, 2007.

[24] G. Thamilarasu and Z. Ma, "Autonomous mobile agent based intrusion detection framework in wireless body area networks," in *Proc. IEEE 16th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2015, pp. 1–3.

[25] W. Meng, W. Li, and L. Zhu, "Enhancing medical smartphone networks via blockchain-based trust management against insider attacks," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1377–1386, Nov. 2020.

[26] A. Odesile and G. Thamilarasu, "Distributed intrusion detection using mobile agents in wireless body area networks," in *Proc. 7th Int. Conf. Emerg. Secur. Technol. (EST)*, Sep. 2017, pp. 144–149.

[27] P. Kamble and A. Gawade, "Digitalization of healthcare with IoT and cryptographic encryption against DOS attacks," in *Proc. Int. Conf. Contemp. Comput. Informat. (IC3I)*, Dec. 2019, pp. 69–73.

[28] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[29] R. Mitchell and I.-R. Chen, "Behavior rule based intrusion detection for supporting secure medical cyber physical systems," in *Proc. 21st Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2012, pp. 1–7.

[30] M. Athinaiou, H. Mouratidis, T. Fotis, and M. Pavlidis, "A conceptual redesign of a modelling language for cyber resiliency of healthcare systems," in *Computer Security* (Lecture Notes in Computer Science), S. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, C. Kalloniatis, J. Mylopoulos, A. Antón, S. Gritzalis, F. Pallas, J. Pohle, A. Sasse, W. Meng, S. Furnell, and J. Garcia-Alfaro, Eds. Cham, Switzerland: Springer, 2020, pp. 140–158.

[31] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured IoMT framework based on swarm-neural network," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1969–1976, May 2022.

[32] C. Greer, M. Burns, D. Wollman, and E. Griffor, "Cyber-physical systems and Internet of Things," *NIST Special Publication*, vol. 1900, p. 202, 2019.

[33] J. Cohen, "Weighted Kappa: Nominal scale agreement provision for scaled disagreement or partial credit," *Psychol. Bull.*, vol. 70, no. 4, p. 213, 1968.

[34] C. Ardito, T. Di Noia, E. Di Sciascio, D. Lofù, A. Pazienza, and F. Vitulano, "User feedback to improve the performance of a cyber-attack detection artificial intelligence system in the e-health domain," in *Human-Computer Interaction—INTERACT*, vol. 12936, C. Ardito, R. Lanzilotti, A. Malizia, H. Petrie, A. Piccinno, G. Desolda, and K. Inkpen, Eds. Cham, Switzerland: Springer, 2021, pp. 295–299.

[35] M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, and P. Haskell-Dowland, "ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things," *Ad Hoc Netw.*, vol. 122, Nov. 2021, Art. no. 102621. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870521001475

[36] F. Akram, D. Liu, P. Zhao, N. Kryvinska, S. Abbas, and M. Rizwan, "Trustworthy intrusion detection in E-Healthcare systems," *Frontiers Public Health*, vol. 9, Dec. 2021, Art. no. 788347. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8678532/

[37] M. Akshay Kumaar, D. Samiayya, P. M. D. R. Vincent, K. Srinivasan, C.-Y. Chang, and H. Ganesh, "A hybrid framework for intrusion detection in healthcare systems using deep learning," *Frontiers Public Health*, vol. 9, Jan. 2022, Art. no. 824898. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8790147/

[38] A. Alamleh, O. S. Albahri, A. A. Zaidan, A. S. Albahri, A. H. Alamoodi, B. B. Zaidan, S. Qahtan, H. A. Alsatar, M. S. Al-Samarraay, and A. N. Jasim, "Federated learning for IoMT applications: A standardization and benchmarking framework of intrusion detection systems," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 878–887, Feb. 2023.

[39] M. A. Almaiah, A. Ali, F. Hajjej, M. F. Pasha, and M. A. Alohali, "A lightweight hybrid deep learning privacy preserving model for FC-based industrial Internet of Medical Things," *Sensors*, vol. 22, no. 6, p. 2112, Mar. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/6/2112

[40] A. S. Alotaibi, "Biserial Miyaguchi–Preneel blockchain-based Ruzicka-indexed deep perceptive learning for malware detection in IoMT," *Sensors*, vol. 21, no. 21, p. 7119, Oct. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/21/7119

[41] I. Alrashdi, A. Alqazzaz, R. Alharthi, E. Aloufi, M. A. Zohdy, and H. Ming, "FBAD: Fog-based attack detection for IoT healthcare in smart cities," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2019, pp. 0515–0522.

[42] A. Arfaoui, A. Kribeche, S. M. Senouci, and M. Hamdi, "Game-based adaptive anomaly detection in wireless body area networks," *Comput. Netw.*, vol. 163, Nov. 2019, Art. no. 106870. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1389128619300015

[43] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "FIDChain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications," *Healthcare*, vol. 10, no. 6, p. 1110, Jun. 2022.

[44] P. V. Astillo, D. G. Duguma, H. Park, J. Kim, B. Kim, and I. You, "Federated intelligence of anomaly detection agent in IoTMD-enabled diabetes management control system," *Future Gener. Comput. Syst.*, vol. 128, pp. 395–405, Mar. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21004192

[45] J. B. Awotunde, K. M. Abiodun, E. A. Adeniyi, S. O. Folorunso, and R. G. Jimoh, "A deep learning-based intrusion detection technique for a secured IoMT system," in *Informatics and Intelligent Applications* (Communications in Computer and Information Science), S. Misra, J. Oluranti, R. Damasevicius, and R. Maskeliunas, Eds. Cham, Switzerland: Springer, 2022, pp. 50–62.

[46] S.-A. Ayoub, A.-G. Mohammed Ali, and B. Narhimene, "Enhanced intrusion detection system for remote healthcare," in *Advances Computing Systems and Applications* (Lecture Notes in Networks and Systems), M. R. Senouci, S. Y. Boulahia, and M. A. Benatia, Eds. Cham, Switzerland: Springer, 2022, pp. 323–333.

[47] V. B. Balasubramanyn, G. Thamilarasu, and R. Sridhar, "Security solution for data integrity inwireless biosensor networks," in *Proc. 27th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, 2007, p. 79.

[48] A. Basharat, M. M. B. Mohamad, and A. Khan, "Machine learning techniques for intrusion detection in smart healthcare systems: A comparative analysis," in *Proc. 4th Int. Conf. Smart Sensors Appl. (ICSSA)*, Jul. 2022, pp. 29–33.

[49] A. Bassene and B. Gueye, "DeepDDoS: A deep-learning model for detecting software defined healthcare IoT networks attacks," in *Ubiquitous Networking* (Lecture Notes in Computer Science), H. Elbiaze, E. Sabir, F. Falcone, M. Sadik, S. Lasaulce, and J. B. Othman, Eds. Cham, Switzerland: Springer, 2021, pp. 201–209.

[50] H. Cai, T. Yun, J. Hester, and K. K. Venkatasubramanian, "Deploying data-driven security solutions on resource-constrained wearable IoT systems," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Jun. 2017, pp. 199–204.

[51] A. S. Carreon-Rascon and J. W. Rozenblit, "Towards requirements for self-healing as a means of mitigating cyber-intrusions in medical devices," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2022, pp. 1500–1505.

[52] M. Chowdhury, S. Jahan, R. Islam, and J. Gao, "Malware detection for healthcare data security," in *Security Privacy in Communication Networks* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), R. Beyah, B. Chang, Y. Li, and S. Zhu, Eds. Cham, Switzerland: Springer, 2018, pp. 407–416.

[53] L. F. Maimó, A. H. Celdrán, Á. P. Gómez, F. G. Clemente, J. Weimer, and I. Lee, "Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments," *Sensors*, vol. 19, no. 5, p. 1114, Mar. 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/5/1114

[54] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the Internet of Things: Concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9562531/

[55] M. Fouda, R. Ksantini, and W. Elmedany, "A novel intrusion detection system for Internet of Healthcare Things based on deep subclasses dispersion information," *IEEE Internet Things J.*, early access, Dec. 20, 2022, doi: 10.1109/JIOT.2022.3230694.

[56] S. Gao and G. Thamilarasu, "Machine-learning classifiers for security in connected medical devices," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, Jul. 2017, pp. 1–5. [Online]. Available: http://ieeexplore.ieee.org/document/8038507/

[57] A. Ghourabi, "A security model based on LightGBM and transformer to protect healthcare systems from cyberattacks," *IEEE Access*, vol. 10, pp. 48890–48903, 2022.

[58] D. Gupta, M. Gupta, S. Bhatt, and A. S. Tosun, "Detecting anomalous user behavior in remote patient monitoring," in *Proc. IEEE 22nd Int. Conf. Inf. Reuse Integr. Data Sci. (IRI)*, Aug. 2021, pp. 33–40.

[59] D. Gupta, O. Kayode, S. Bhatt, M. Gupta, and A. Saman Tosun, "Hierarchical federated learning based anomaly detection using digital twins for smart healthcare," 2021, *arXiv:2111.12241*.

[60] K. Gupta, D. K. Sharma, K. Datta Gupta, and A. Kumar, "A tree classifier based network intrusion detection model for Internet of Medical Things," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108158. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790622004049

[61] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion detection system for healthcare systems using medical and network data: A comparison study," *IEEE Access*, vol. 8, pp. 106576–106584, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9109651/

[62] M. Hajder, J. Kolbusz, P. Hajder, M. Nycz, and M. Liput, "Data security platform model in networked medical IT systems based on statistical classifiers and ANN," *Proc. Comput. Sci.*, vol. 176, pp. 3682–3691, 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1877050920319104

[63] S. S. Hameed, W. H. Hassan, and L. A. Latiff, "An efficient fog-based attack detection using ensemble of MOA-WMA for Internet of Medical Things," in *Innovative Systems for Intelligent Health Informatics* (Lecture Notes on Data Engineering and Communications Technologies), F. Saeed, F. Mohammed, and A. Al-Nahari, Eds. Cham, Switzerland: Springer, 2021, pp. 774–785.

[64] S. S. Hameed, A. Selamat, L. A. Latiff, S. A. Razak, O. Krejcar, H. Fujita, M. N. A. Sharif, and S. Omatu, "A hybrid lightweight system for early attack detection in the IoMT fog," *Sensors*, vol. 21, no. 24, p. 8289, Dec. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/24/8289

[65] S. S. Hameed, A. Selamat, L. A. Latiff, S. A. Razak, and O. Krejcar, "WHTE: Weighted Hoeffding tree ensemble for network attack detection at Fog-IoMT," in *Advances and Trends in Artificial Intelligence Theory and Practices in Artificial Intelligence* (Lecture Notes in Computer Science), H. Fujita, P. Fournier-Viger, M. Ali, and Y. Wang, Eds. Cham, Switzerland: Springer, 2022, pp. 485–496.

[66] N. I. Haque, A. A. Khalil, M. A. Rahman, M. H. Amini, and S. I. Ahamed, "BIOCAD: Bio-inspired optimization for classification and anomaly detection in digital healthcare systems," in *Proc. IEEE Int. Conf. Digit. Health (ICDH)*, Sep. 2021, pp. 48–58.

[67] N. I. Haque, M. A. Rahman, and S. I. Ahamed, "DeepCAD: A stand-alone deep neural network-based framework for classification and anomaly detection in smart healthcare systems," in *Proc. IEEE Int. Conf. Digit. Health (ICDH)*, Jul. 2022, pp. 218–227.

[68] D. He, Q. Qiao, Y. Gao, J. Zheng, S. Chan, J. Li, and N. Guizani, "Intrusion detection based on stacked autoencoder for connected healthcare systems," *IEEE Netw.*, vol. 33, no. 6, pp. 64–69, Nov. 2019.

[69] X. Hei, X. Du, S. Lin, I. Lee, and O. Sokolsky, "Patient infusion pattern based access control schemes for wireless insulin pump system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 11, pp. 3108–3121, Nov. 2015.

[70] F. Hussain, S. G. Abbas, G. A. Shah, I. M. Pires, U. U. Fayyaz, F. Shahzad, N. M. Garcia, and E. Zdravevski, "A framework for malicious traffic detection in IoT healthcare environment," *Sensors*, vol. 21, no. 9, p. 3025, Apr. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/9/3025

[71] O. Igbe, I. Darwish, and T. Saadawi, "Distributed network intrusion detection systems: An artificial immune system approach," in *Proc. IEEE 1st Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, Jun. 2016, pp. 101–106.

[72] M. J. Iqbal, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C.-W. Lin, "RThreatDroid: A ransomware detection approach to secure IoT based healthcare systems," *IEEE Trans. Netw. Sci. Eng.*, early access, Jul. 5, 2022, doi: 10.1109/TNSE.2022.3188597.

[73] A. Karthick Kumar, K. Vadivukkarasi, R. Dayana, and P. Malarvezhi, "BotNet attacks detection using embedded feature selection methods for secure IOMT environment," in *Pervasive Computing and Social Networking* (Lecture Notes in Networks and Systems), G. Ranganathan, R. Bestak, and X. Fernando, Eds. Singapore: Springer, 2023, pp. 585–599.

[74] I. A. Khan, N. Moustafa, I. Razzak, M. Tanveer, D. Pi, Y. Pan, and B. S. Ali, "XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks," *Future Gener. Comput. Syst.*, vol. 127, pp. 181–193, Feb. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21003563

[75] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. U. Rehman, "A secure ensemble learning-based fog-cloud approach for cyberattack detection in IoMT," *IEEE Trans. Ind. Informat.*, early access, Jan. 17, 2023, doi: 10.1109/TII.2022.3231424.

[76] I. F. Kilincer, F. Ertam, A. Sengur, R.-S. Tan, and U. R. Acharya, "Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization," *Biocybern. Biomed. Eng.*, vol. 43, no. 1, pp. 30–41, Jan. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0208521622001012

[77] M. Kintzlinger, A. Cohen, N. Nissim, M. Rav-Acha, V. Khalameizer, Y. Elovici, Y. Shahar, and A. Katz, "CardiWall: A trusted firewall for the detection of malicious clinical programming of cardiac implantable electronic devices," *IEEE Access*, vol. 8, pp. 48123–48140, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9025056/

[78] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, Jan. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366420320090

[79] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, A. K. M. N. Islam, and M. Shorfuzzaman, "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8065–8073, Nov. 2022.

[80] P. Kumar, R. Kumar, S. Garg, K. Kaur, Y. Zhang, and M. Guizani, "A secure data dissemination scheme for IoT-based E-health systems using AI and blockchain," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2022, pp. 1397–1403.

[81] W. Li, W. Meng, C. Su, and L. F. Kwok, "Towards false alarm reduction using fuzzy if-then rules for medical cyber physical systems," *IEEE Access*, vol. 6, pp. 6530–6539, 2018.

[82] T. Mahler, E. Shalom, Y. Elovici, and Y. Shahar, "A dual-layer context-based architecture for the detection of anomalous instructions sent to medical devices," *Artif. Intell. Med.*, vol. 123, Jan. 2022, Art. no. 102229. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0933365721002220

[83] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, "Effective attack detection in Internet of Medical Things smart environment using a deep belief neural network," *IEEE Access*, vol. 8, pp. 77396–77404, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9057709/

[84] A. Mishra and P. Bagade, "Digital forensics for medical Internet of Things," in *Proc. IEEE Globecom Workshops*, Dec. 2022, pp. 1074–1079.

[85] R. A. Mohammed and K. M. A. Alheeti, "Intrusion detection system for healthcare based on convolutional neural networks," in *Proc. Iraqi Int. Conf. Commun. Inf. Technol. (IICCIT)*, Sep. 2022, pp. 216–221.

[86] N. Mowla, I. Doh, and K. Chae, "Evolving neural network intrusion detection system for MCPS," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 1040–1045.

[87] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "UbeHealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities," *IEEE Access*, vol. 6, pp. 32258–32285, 2018.

[88] J. Nayak, S. K. Meher, A. Souri, B. Naik, and S. Vimal, "Extreme learning machine and Bayesian optimization-driven intelligent framework for IoMT cyber-attack detection," *J. Supercomput.*, vol. 78, no. 13, pp. 14866–14891, Sep. 2022.

[89] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "HealthGuard: A machine learning-based security framework for smart healthcare systems," in *Proc. 6th Int. Conf. Social Netw. Anal., Manage. Secur. (SNAMS)*, Oct. 2019, pp. 389–396.

[90] A. I. Newaz, A. K. Sikder, L. Babun, and A. S. Uluagac, "HEKA: A novel intrusion detection system for attacks to personal medical devices," in *Proc. IEEE CNS*, Jun. 2020, pp. 1–9.

[91] Y. Otoum, Y. Wan, and A. Nayak, "Federated transfer learning-based IDS for the Internet of Medical Things (IoMT)," in *Proc. IEEE Globecom Workshops*, Dec. 2021, pp. 1–6.

[92] S. Otoum, N. Guizani, and H. Mouftah, "Federated reinforcement learning-supported IDS for IoT-steered healthcare systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–6.

[93] Y. Otoum, V. Chamola, and A. Nayak, "Federated and transfer learning-empowered intrusion detection for IoT applications," *IEEE Internet Things Mag.*, vol. 5, no. 3, pp. 50–54, Sep. 2022.

[94] D. Panagoda, C. Malinda, C. Wijetunga, L. Rupasinghe, B. Bandara, and C. Liyanapathirana, "Application of federated learning in health care sector for malware detection and mitigation using software defined networking approach," in *Proc. 2nd Asian Conf. Innov. Technol.*, Aug. 2022, pp. 1–6.

[95] P. K. R. Maddikunta, M. Parimala, S. Koppu, T. R. Gadekallu, C. L. Chowdhary, and M. Alazab, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, Jul. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S014036642030298X

[96] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, T. Lagkas, G. Fragulis, and A. Sarigiannidis, "A self-learning approach for detecting intrusions in healthcare systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–6.

[97] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos, and S. Wan, "Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 2041–2052, Mar. 2022.

[98] S. Rahmadika, P. V. Astillo, G. Choudhary, D. G. Duguma, V. Sharma, and I. You, "Blockchain-based privacy preservation scheme for misbehavior detection in lightweight IoMT devices," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 710–721, Feb. 2023.

[99] N. Ram and D. Kumar, "Effective cyber attack detection in an IoMT-smart system using deep convolutional neural networks and machine learning algorithms," in *Proc. 2nd Int. Conf. Adv. Technol. Intell. Control, Environ., Comput. Commun. Eng. (ICATIECE)*, Dec. 2022, pp. 1–6.

[100] A. Rao, N. Carreon, R. Lysecky, and J. Rozenblit, "Probabilistic threat detection for risk management in cyber-physical medical systems," *IEEE Softw.*, vol. 35, no. 1, pp. 38–43, Jan. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8239935/

[101] A. Rao, N. Carreón, R. Lysecky, J. Rozenblit, and J. Sametinger, "Resilient security of medical cyber-physical systems," in *Database Expert Systems Applications* (Communications in Computer and Information Science), G. Anderst-Kotsis, A. M. Tjoa, I. Khalil, M. Elloumi, A. Mashkoor, J. Sametinger, X. Larrucea, A. Fensel, J. Martinez-Gil, B. Moser, C. Seifert, B. Stein, and M. Granitzer, Eds. Cham, Switzerland: Springer, 2019, pp. 95–100.

[102] V. Ravi, T. D. Pham, and M. Alazab, "Attention-based multidimensional deep learning approach for cross-architecture IoMT malware detection and classification in healthcare cyber-physical systems," *IEEE Trans. Computat. Social Syst.*, early access, Aug. 19, 2022, doi: 10.1109/TCSS.2022.3198123.

[103] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Comput. Biol. Med.*, vol. 150, Nov. 2022, Art. no. 106019.

[104] T. Saba, "Intrusion detection in smart city hospitals using ensemble classifiers," in *Proc. 13th Int. Conf. Develop. eSyst. Eng. (DeSE)*, Dec. 2020, pp. 418–422.

[105] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the Internet of Medical Things-smart environment based on deep recurrent neural network and machine learning algorithms," *IEEE Access*, vol. 9, pp. 161546–161554, 2021.

[106] A. M. Said, A. Yahyaoui, F. Yaakoubi, and T. Abdellatif, "Machine learning based rank attack detection for smart hospital infrastructure," in *Proc. Int. Conf. Smart Homes Health Telematics*. Cham, Switzerland: Springer, 2020, pp. 28–40.

[107] O. Salem and A. Mehaoua, "A secure framework for remote healthcare monitoring using the Internet of Medical Things," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2022, pp. 1233–1238.

[108] W. Schneble and G. Thamilarasu, "Optimal feature selection for intrusion detection in medical cyber-physical systems," in *Proc. 11th Int. Conf. Adv. Comput. (ICoAC)*, Dec. 2019, pp. 238–243.

[109] N. Sehatbakhsh, M. Alam, A. Nazari, A. Zajic, and M. Prvulovic, "Syndrome: Spectral analysis for anomaly detection on medical IoT and embedded devices," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Apr. 2018, pp. 1–8.

[110] R. A. Sharma, I. Sabane, M. Apostolaki, A. Rowe, and V. Sekar, "Lumen: A framework for developing and evaluating ML-based IoT network anomaly detection," in *Proc. 18th Int. Conf. Emerg. Netw. Exp. Technol.*, New York, NY, USA, Nov. 2022, pp. 59–71, doi: 10.1145/3555050.3569129.

[111] P. Singh, G. S. Gaba, A. Kaur, M. Hedabou, and A. Gurtov, "Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT," *IEEE J. Biomed. Health Informat.*, vol. 27, no. 2, pp. 722–731, Feb. 2023.

[112] I. Siniosoglou, P. Sarigiannidis, V. Argyriou, T. Lagkas, S. K. Goudos, and M. Poveda, "Federated intrusion detection in NG-IoT healthcare systems: An adversarial approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–6.

[113] F. Spegni, A. Sabatelli, A. Merlo, L. Pepa, L. Spalazzi, and L. Verderame, "A precision cybersecurity workflow for cyber-physical systems: The IoT healthcare use case," in *Proc. Int. Workshops Comput. Security (ESORICS)* (Lecture Notes in Computer Science), S. Katsikas, F. Cuppens, C. Kalloniatis, J. Mylopoulos, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. M. Vidal, M. A. S. Monge, M. Albanese, B. Katt, S. Pirbhulal, and A. Shukla, Eds. Cham, Switzerland: Springer, 2023, pp. 409–426.

[114] A. Tabassum, A. Erbad, A. Mohamed, and M. Guizani, "Privacy-preserving distributed IDS using incremental learning for IoT health systems," *IEEE Access*, vol. 9, pp. 14271–14283, 2021.

[115] B. Tahir, A. Jolfaei, and M. Tariq, "A novel experience-driven and federated intelligent threat-defense framework in IoMT," *IEEE J. Biomed. Health Informat.*, early access, Jan. 11, 2023, doi: 10.1109/JBHI.2023.3236072.

[116] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for Internet of Medical Things," *IEEE Access*, vol. 8, pp. 181560–181576, 2020.

[117] C. Thapa, K. K. Karmakar, A. H. Celdran, S. Camtepe, V. Varadharajan, and S. Nepal, "FedDICE: A ransomware spread detection in a distributed integrated clinical environment using federated learning and SDN based mitigation," 2021, *arXiv:2106.05434*.

[118] A. A. Toor, M. Usman, F. Younas, A. C. M. Fong, S. A. Khan, and S. Fong, "Mining massive e-health data streams for IoMT enabled healthcare systems," *Sensors*, vol. 20, no. 7, p. 2131, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/7/2131

[119] S. M. W. Umba, A. M. Abu-Mahfouz, and D. Ramotsoela, "Artificial intelligence-driven intrusion detection in software-defined wireless sensor networks: Towards secure IoT-enabled healthcare systems," *Int. J. Environ. Res. Public Health*, vol. 19, no. 9, p. 5367, Apr. 2022.

[120] S. A. Wagan, J. Koo, I. F. Siddiqui, N. M. F. Qureshi, M. Attique, and D. R. Shin, "A fuzzy-based duo-secure multi-modal framework for IoMT anomaly detection," *J. King Saud Univ., Comput. Inf. Sci.*, vol. 35, no. 1, pp. 131–144, Jan. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157822004050

[121] F. Wahab, Y. Zhao, D. Javeed, M. H. Al-Adhaileh, S. A. Almaaytah, W. Khan, M. S. Saeed, and R. Kumar Shah, "An AI-driven hybrid framework for intrusion detection in IoT-enabled E-health," *Comput. Intell. Neurosci.*, vol. 2022, Dec. 2022, Art. no. 6096289.

[122] J. Wang, H. Jin, J. Chen, J. Tan, and K. Zhong, "Anomaly detection in Internet of Medical Things with blockchain from the perspective of deep neural network," *Inf. Sci.*, vol. 617, pp. 133–149, Dec. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025522011835

[123] R. Yan, V. C. Shah, T. Xu, and M. Potkonjak, "Security defenses for vulnerable medical sensor network," in *Proc. IEEE Int. Conf. Healthcare Inform. (ICHI)*, Sep. 2014, pp. 300–309.

[124] B. Zaabar, O. Cheikhrouhou, and M. Abid, "Intrusion detection system for IoMT through blockchain-based federated learning," in *Proc. 15th Int. Conf. Secur. Inf. Netw. (SIN)*, Nov. 2022, pp. 1–8.

[125] G. Zachos, G. Mantas, I. Essop, K. Porfyrakis, J. C. Ribeiro, and J. Rodriguez, "Prototyping an anomaly-based intrusion detection system for Internet of Medical Things networks," in *Proc. IEEE 27th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Nov. 2022, pp. 179–183.

[126] M. Zubair, A. Ghubaish, D. Unal, A. Al-Ali, T. Reimann, G. Alinier, M. Hammoudeh, and J. Qadir, "Secure Bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system," *Sensors*, vol. 22, no. 21, p. 8280, Oct. 2022.

[127] R. Abdulhammed, M. Faezipour, and K. Elleithy, "Malicious behavior monitoring of embedded medical devices," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, May 2017, pp. 1–6.

[128] G. Choudhary, P. V. Astillo, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "Lightweight misbehavior detection management of embedded IoT devices in medical cyber physical systems," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 4, pp. 2496–2510, Dec. 2020.

[129] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, "A practical model based on anomaly detection for protecting medical IoT control services against external attacks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 4260–4269, Jun. 2021.

[130] R. Mitchell and R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, Jan. 2015.

[131] Z. Li, L. Cheng, and Y. Zhang, "Tracking sensitive information and operations in integrated clinical environment," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 13th IEEE Int. Conf. Big Data Sci. Eng.*, Aug. 2019, pp. 192–199.

[132] M. Raiyat Aliabadi, M. Seltzer, M. Vahidi Asl, and R. Ghavamizadeh, "ARTINALI#: An efficient intrusion detection technique for resource-constrained cyber-physical systems," *Int. J. Crit. Infrastruct. Protection*, vol. 33, Jun. 2021, Art. no. 100430. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548221000226

[133] I. You, K. Yim, V. Sharma, G. Choudhary, I. Chen, and J.-H. Cho, "Misbehavior detection of embedded IoT devices in medical cyber physical systems," in *Proc. 3rd IEEE/ACM Int. Conf. Connected Health-Appl., Syst. Eng. Technol.*, Washington, DC, USA, Sep. 2018, pp. 88–93, doi: 10.1145/3278576.3278601.

[134] M. Zhang, A. Raghunathan, and N. K. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.

[135] M. Boujrad, S. Lazaar, and M. Hassine, "Performance assessment of open source IDS for improving IoT architecture security implemented on WBANs," in *Proc. 3rd Int. Conf. Netw., Inf. Syst. Secur.*, Mar. 2020, pp. 1–4, doi: 10.1145/3386723.3387892.

[136] C. Mpungu, C. George, and G. Mapp, "Developing a novel digital forensics readiness framework for wireless medical networks using specialised logging," in *Cybersecurity Age of Smart Societies* (Advanced Sciences and Technologies for Security Applications), H. Jahankhani, Ed. Cham, Switzerland: Springer, 2023, pp. 203–226.

[137] H. Zhang, S. Kang, and Y. Li, "Visual construction algorithm of attack path based on medical sensor networks," in *Proc. IEEE Int. Conf. Saf. Produce Informatization (IICSPI)*, Dec. 2018, pp. 775–779.

[138] M. Begli, F. Derakhshan, and H. Karimipour, "A layered intrusion detection system for critical infrastructure using machine learning," in *Proc. IEEE 7th Int. Conf. Smart Energy Grid Eng. (SEGE)*, Aug. 2019, pp. 120–124.

[139] M. Chen, Y. Qian, J. Chen, K. Hwang, S. Mao, and L. Hu, "Privacy protection and intrusion avoidance for cloudlet-based medical data sharing," *IEEE Trans. Cloud Comput.*, vol. 8, no. 4, pp. 1274–1283, Oct. 2020.

[140] G. Dupont, D. R. D. Santos, E. Costante, J. den Hartog, and S. Etalle, "A matter of life and death: Analyzing the security of healthcare networks," in *ICT Systems Security and Privacy Protection* (Advances in Information and Communication Technology), M. Hölbl, K. Rannenberg, and T. Welzer, Eds. Cham, Switzerland: Springer, 2020, pp. 355–369.

[141] W. Meng, K.-K.-R. Choo, S. Furnell, A. V. Vasilakos, and C. W. Probst, "Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks," *IEEE Trans. Netw. Service Manage.*, vol. 15, no. 2, pp. 761–773, Jun. 2018.

[142] N. Kolokotronis, M. Dareioti, S. Shiaeles, and E. Bellini, "An intelligent platform for threat assessment and cyber-attack mitigation in IoMT ecosystems," in *Proc. IEEE Globecom Workshops*, Dec. 2022, pp. 541–546.

[143] E. Lakka, G. Hatzivasilis, S. Karagiannis, A. Alexopoulos, M. Athanatos, S. Ioannidis, M. Chatzimpyrros, G. Kalogiannis, and G. Spanoudakis, "Incident handling for healthcare organizations and supply-chains," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2022, pp. 1–7.

[144] U. Tariq, I. Ullah, M. Yousuf Uddin, and S. J. Kwon, "An effective self-configurable ransomware prevention technique for IoMT," *Sensors*, vol. 22, no. 21, p. 8516, Nov. 2022.

[145] H. Nguyen, B. Acharya, R. Ivanov, A. Haeberlen, L. T. X. Phan, O. Sokolsky, J. Walker, J. Weimer, W. Hanson, and I. Lee, "Cloud-based secure logger for medical devices," in *Proc. IEEE 1st Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, Jun. 2016, pp. 89–94.

[146] S. D. Hettich and S. Bay, "KDD CUP 1999 data," *UCI KDD Arch.*, vol. 3, no. 1, pp. 1–35, 1999.

[147] M. Tavallaee, E. Bagheri, W. Lu, and A.-A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. 2nd IEEE Symp. Comput. Intell. Secur. Defence Appl.*, Ottawa, ON, Canada, Jul. 2009, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/5356528/

[148] I. Sharafaldin, A. Gharib, A. H. Lashkari, and A. A. Ghorbani, "Towards a reliable intrusion detection benchmark dataset," *Softw. Netw.*, vol. 2018, no. 1, pp. 177–200, 2018.

[149] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, vol. 1, Jan. 2018, pp. 108–116.

[150] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.

[151] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic Botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796, Nov. 2019.

[152] A. E. Johnson, T. J. Pollard, L. Shen, H. L. Li-Wei, M. Feng, M. Ghassemi, B. Moody, P. Szolovits, L. A. Celi, and R. G. Mark, "MIMIC-III, a freely accessible critical care database," *Sci. Data*, vol. 3, no. 1, pp. 1–9, 2016.

[153] A. Boddy, W. Hurst, M. MacKay, and A. El Rhalibi, "A study into detecting anomalous behaviours within healthcare infrastructures," in *Proc. 9th Int. Conf. Develop. eSyst. Eng. (DeSE)*, Sep. 2016, pp. 111–117.

[154] D. Arney, J. Plourde, and J. M. Goldman, "OpenICE medical device interoperability platform overview and requirement analysis," *Biomed. Eng. Biomedizinische Technik*, vol. 63, no. 1, pp. 39–47, Feb. 2018.

[155] H. Nguyen-An, T. Silverston, T. Yamazaki, and T. Miyoshi, "Generating IoT traffic: A case study on anomaly detection," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN*, Jul. 2020, pp. 1–6.

[156] S. S. Clark and K. Fu, "Recent results in computer security for medical devices," in *Wireless Mobile Communication and Healthcare* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), K. S. Nikita, J. C. Lin, D. I. Fotiadis, and M.-T. Arredondo Waldmeyer, Eds. Berlin, Germany: Springer, 2012, pp. 111–118.

SIMON B. WEBER received the B.S. degree in computer science from Heinrich Heine University (HHU) Düsseldorf, in 2019, and the M.S. degree in computer science, in 2020, where he is currently pursuing the Ph.D. degree. His primary focus of study was on IT and network security. His research interests include sector-specific attack detection for critical infrastructure. In addition to his doctorate, he is part of the IT Security Team, University Computing Center.

STEFAN STEIN received the B.S. degree in project engineering from Baden-Württemberg Cooperative State University, in 2017, and the M.S. degree in IT security and forensics from the Wismar University of Applied Sciences, in 2019. Currently, he conducts research as a Doctoral Student with the Brandenburg University of Applied Sciences. In addition, he is also a Security Analyst with Gematik GmbH. His work focuses on IT security in healthcare, including vulnerability scanning, security monitoring, data protection, security incident assessment, and vulnerability and information security management.

MICHAEL PILGERMANN received the Ph.D. degree in information security from the University of South Wales, in 2006. After, he has gained 15 years of professional IT security experience in business and administration. Since 2021, he has been a Professor with the Brandenburg University of Applied Sciences, specializing in IT security. He researches on detection of cyber attacks when operating critical infrastructures.

THOMAS SCHRADER is a Professor of applied computer science, focusing on medical informatics with the Brandenburg University of Applied Sciences. His research interests include data quality in medical data repositories, prospective risk analysis in medical environments, motion analysis, evaluation of hyperspectral images, and e-health.