SICS Software-Intensive Cyber-Physical Systems (2021) 35:159–183
https://doi.org/10.1007/s00450-021-00427-3

REGULAR PAPER

A new enhanced cyber security framework for medical cyber physical systems

Ishaani Priyadarshini[1] · Raghvendra Kumar[2] · Le Minh Tuan[3,4] · Le Hoang Son[4] · Hoang Viet Long[5,6] · Rohit Sharma[7] · Sakshi Rai[8]

Received: 22 December 2019 / Accepted: 3 March 2021 / Published online: 23 March 2021

Abstract

Medical Cyber-Physical Systems (MCPS) are complex, location-aware, networked systems of medical devices that can be used as a piece of the healing center to give the best medical care to patients. Hence, they integrate human, cyber, and physical elements. Since MCPSs are life-critical and context-aware, they are significant to the healthcare industry, which is prone to data breaches and cyber-attacks. As an emerging research area, MCPS faces several challenges with respect to system reliability, assurance, autonomy and security, and privacy. In this paper, we initially examine the state-of-the-arts of MCPS over the last few decades (1998–2020) and subsequently propose a new framework considering security/privacy for MPCS that incorporates several models that depict various domains of security. An interaction between various models followed with a qualitative assessment of the framework has been carried out to present a detailed description of the proposed framework. It is useful in various healthcare industries like health care services, manufacturing, pharmaceuticals, etc. that utilize smart devices. Additionally, the framework may be applied to enhance security in the Internet of Things (IoT) environment. It may be also useful to deploy efficient workflow operations for patients under the consideration framework. The framework will also lay out the foundation for implementing cybersecurity infrastructures in many healthcare applications.

Keywords Medical cyber-physical systems · Cyber security · Medical control systems · Security and privacy issues · Smart health

✉ Hoang Viet Long
hoangvietlong@tdtu.edu.vn

Ishaani Priyadarshini
ishaanidisha@gmail.com

Raghvendra Kumar
raghvendraagrawal7@gmail.com

Le Minh Tuan
letuan104@gmail.com

Le Hoang Son
sonlh@vnu.edu.vn

Rohit Sharma
rohitapece@gmail.com

Sakshi Rai
sakshirai.sr29@gmail.com

[1] University of Delaware, Newark, DE, USA

[2] Department of Computer Science and Engineering, GIET University, Gunupur, India

[3] Hanoi University of Home Affairs, Hanoi, Vietnam

[4] VNU Information Technology Institute, Vietnam National University, Hanoi, Vietnam

[5] Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[6] Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[7] Department of Electronics & Communication Engineering, Faculty of Engineering and Technology, SRM Institute of Science and Technology, NCR Campus, Delhi - NCR Campus, Delhi - Meerut Road, Modinagar, Ghaziabad, UP, India

[8] Department of Computer Science and Engineering, LNCT University, Bhopal, MP, India

1 Introduction

Rapid developments and progress in the embedded software and network connectivity has led to rapid transformation in medical devices [1]. The healthcare industry is progressively moving away from the usage of stand-alone devices to monitor and treat patients independently. It rapidly moves towards the usage of integrated systems that are able to monitor, evaluate, and treat different parts of patients' physiology concurrently. The integration of embedded software controlling devices, networking abilities of medical devices, and the complex physical elements displayed by patients' bodies, make therapeutic medical device systems, commonly known as Medical Cyber-Physical Systems (MCPS) [2]. MCPS collaborates with cloud computing to construct regional medical information as well as to provide data storage services. *Internet of Things* (IoT) also finds several applications in the healthcare industry like remote health and monitoring, availability and accessibility of hardware, tracking patient inventories, and drug management.

Figure 1 gives an overall idea of Medical Cyber-Physical Systems (MCPS), which incorporates physical devices and physical systems. The physical systems are combined to form an overall system of several systems. This conglomeration of dedicated task-oriented systems bears more functionality and performance than the sum of constituent systems. Cyber-Physical Systems (CPS) are systems that associate the physical world with the virtual world of information processing. The physical world may consist of sensors and actuators. Several constituents in the CPS collaborate to perform some sort of global behavior. These constituents could be software systems, communication technologies, sensors, and actuators, etc. that can interact with the real world. In this research, we focus on the Medical Cyber-Physical System (MCPS), which is a sub-domain of the Cyber-Physical systems. MCPS is the healthcare critical integration of a network of medical devices (components) brought toward high quality in healthcare.

In the past, several research works have been conducted with respect to MCPS. Lee and Sokolsky [98] presented an overview of MCPS in terms of trends in the development and use of high-confidence medical cyber-physical systems. The article is an overall summary of challenges related to MCPS like model-based development, patient modeling, and simulation, user-centric design, security, and privacy, etc. The study is limited, and the authors fail to propose anything novel. Lee et al. [2] summarized some challenges and research prospects for MCPS. The challenges include issues related to device interoperability, decision support, high confidence development, regulatory issues, etc.; however, security and privacy issues have been ignored. Moreover, the article does not propose any solution to overcome the challenges. Jung and Cho [133] highlighted the concept of interoperability for control systems in MCPS. To enable automation of medical devices, software platforms have been considered; yet the study is confined to interoperability only and also does not comment on validation and verification aspects. Min [130] studied MCPS based on Big Data platforms. The idea is to ensure efficiency in processing massive amounts of data, for which a framework was proposed. While the framework incorporates several components, the article lacks necessary theory as well as validation. Kocabas et al. [55] listed some emerging security mechanisms for MCPS based on data acquisition, data aggregation, cloud processing, and actions. They surveyed encryption schemes and evaluates the schemes to enhance security. The proposed method may have computational as well as storage overhead and usability issues. Dey et al. [4] conducted a survey on MCPS and reported the structure of cyber-physical systems, the architecture, emerging trends, evolution of medical devices, big data platforms that support

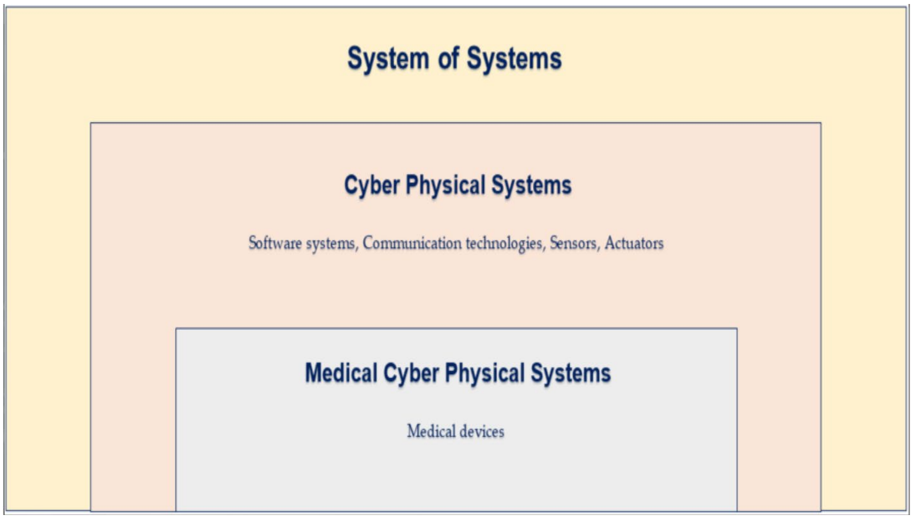

System of Systems
Cyber Physical Systems
Software systems, Communication technologies, Sensors, Actuators
Medical Cyber Physical Systems
Medical devices

Fig. 1 The mapping processes

MCPS, and challenges. The survey fails to identify adequate security issues and potential solutions. Qiu et al. [131] highlight the privacy-preserving issue in MCPS and assert that encryption is robust as long as keys are not compromised. A selective encryption algorithm combined with fragmentation and dispersion to protect the data has been proposed. While the performance of algorithms is evaluated in a smartphone environment, the efficiency of the algorithms varies across platforms. Jimenez et al. [132] presented research on Cyber-Physical Systems and Digital Twins for the healthcare sector. The article incorporates the architecture of MCPS and the impact of Wireless Body Area Networks on healthcare. Moreover, the article states challenges related to high assurance software, regulatory issues, security, and privacy, etc., but fails to provide a conceptual framework or solution for the same. Haideggr et al. [133] presented a research on user requirements and challenges in robotics from the industrial and MCPS perspective. The article highlights medical robot standards and their challenges with respect to safety metrics, performance metrics, boundary metrics, etc. but fails to provide a framework or potential solution for the same. Shishvan et al. [134] proposed the idea of incorporating Artificial Intelligence (AI) into MCPS. The article is a survey depicting machine intelligence algorithms, the types of algorithms available for the healthcare domain, how the data and the decision support output are presented to the end-user, etc. but fails to identify the security issues that may also crop into MCPS devices and systems.

The expanded size and unpredictability of MCPS with respect to existing conventional medical systems have resulted in various formative difficulties (early-stage setbacks) that need to be addressed. In the past few years, researchers have proposed several studies and analyses of MCPS pertaining to the ideas, applications, issues, tradeoffs, etc. that these systems incorporate. However, the research quotient is insufficient, and formal techniques suffer from limitations like interoperability and robustness [122]. Thus, these constraints need to be carefully addressed, and necessary improvements need to be made in terms of framework design [4]. In addition, new administrative methods need to be devised to affirm their use in treating patients [5, 6]. Although a lot of researchers in the past provided an overall idea of the MCPS, they lacked significant *contributions like architecture, applications, and challenges*, which we aim to provide in this research. The novelty of this work is as follows:

1. The article highlights the overall state of the art of MCPS including a general overview, classification, benefits, challenges, and security issues. To the best of our knowledge, this is the first article that underpins the state-of-the-arts of MCPS at such great depth.
2. In this article, we propose a cybersecurity framework along with an interactive model for the proposed framework. Although cybersecurity frameworks like National Institute of Standards and Technology (NIST) Cybersecurity Framework, Center for Internet Security (CIS) controls, etc. exist, the proposed framework would be the first of its kind to underpin IoT devices, MCPS, Trust Model, and Threat Model conjointly, thereby enhancing overall security.
3. One of the drawbacks of the existing frameworks is that although they can be applied to various industries, the evaluation is usually based only on self-assessment using a set of questionnaires. This kind of assessment may be biased and may have certain limitations as it may not cover many aspects of security. Security may never be 100% guaranteed, thus there is no particular way of evaluating a framework, since all frameworks will have some limitations. In our framework, we have included security models based on an extensive survey highlighting various security issues that may crop up in MCPS. We also present how these models in the proposed framework interact with each other. This is followed by a qualitative assessment of the proposed framework to enhance security in MCPS.

The rest of the paper is organized as follows. Section 2 provides an in-depth idea about MCPS including the general overview, classification, benefits, challenges, and security issues. Section 3 highlights the proposed framework, the interaction between various components of the framework, and a qualitative assessment of the same. In Sect. 4, we discuss the conclusion and future work.

2 Medical cyber physical systems

The previous section laid out a general idea about the MCPS highlighting their applications and advantages. Moreover, the prior works pertaining to MCPS have also been mentioned. In this section, we delve into the concept of MCPS by describing its overall structure, classification based on the concept of social insurance, benefits of MCPS and some challenges faced.

2.1 General overview of medical cyber physical systems (MCPS)

Cyber Physical Systems (CPSs) commonly refer to systems in which computing, networking and physical processes are integrated to monitor and evaluate situations. In any CPS, embedded computers and networks will monitor and control the physical processes, with inbuilt feedback loops that

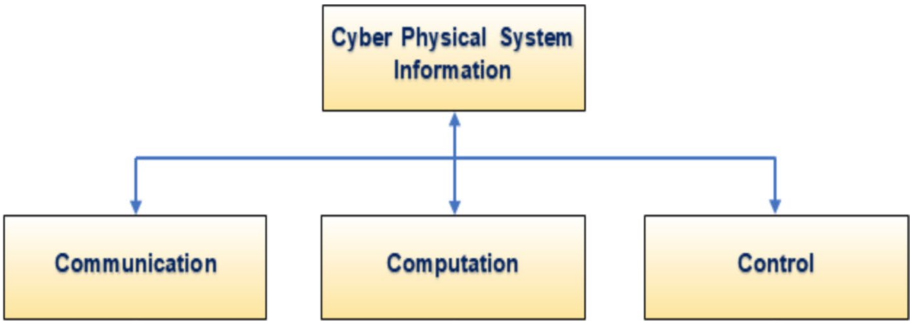


Fig. 2 Capabilities of Cyber Physical System

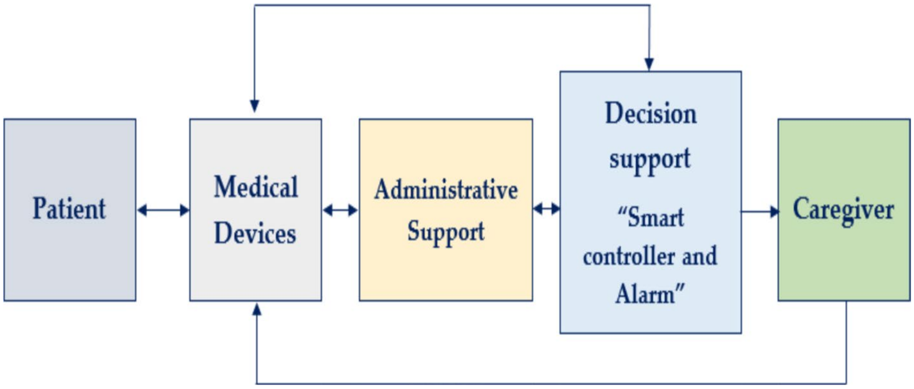


Fig. 3 Core Components Interaction with a medical Device

communicate with physical processes affecting computation and subsequently providing information on the next course of actions to control the physical processes [8–10]. A Cyber Physical System is capable of Communication, Computation and Control (Fig. 2).

The main aim of any CPS is to integrate robotics and sensor systems with information gathered from the other components of the CPS, with all of it being processed with computational knowledge to arrive at the final decision [11]. Thus, they form the core for MCPS and incorporate within them physical and computational capabilities that enable interaction with humans [7].

Like the CPS, the MCPS also consolidates physical procedures with shareware and systems administration as a coordinated entity to create feedback systems (Fig. 3). These devices are not only restricted to the healthcare industry, but also in energy, infrastructure, manufacturing, military, robotics, and transportation [12]. Therefore, versatility, independence, proficiency, usefulness, unwavering quality, security, and the ease of CPSs are paramount for such systems. Hence, drastic improvements are expected to be made due to dynamic and rapid developments of MCPS [13–16].

Owing to the large number of devices involved, Communication and Scheduling are two important tasks for any CPS.

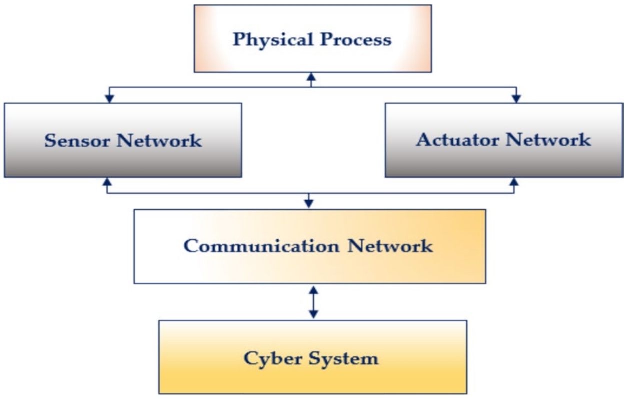


Fig. 4 Overview of the structure of a CPS

Communication: CPS consists of components from the physical world, user interfaces and cyber systems (Fig. 4). The components of *the physical world* ensure that the corresponding devices are monitored and controlled. The *cyber systems* consist of the cutting-edge embedded devices, which process the collected data and disseminate them accordingly. The user interface, communication network and other middle of the road segments such as interconnected sensors, actuators, analog-to-digital converters (ADC), and digital-to-analogue converters (DAC), play an important role in connecting the cyber systems

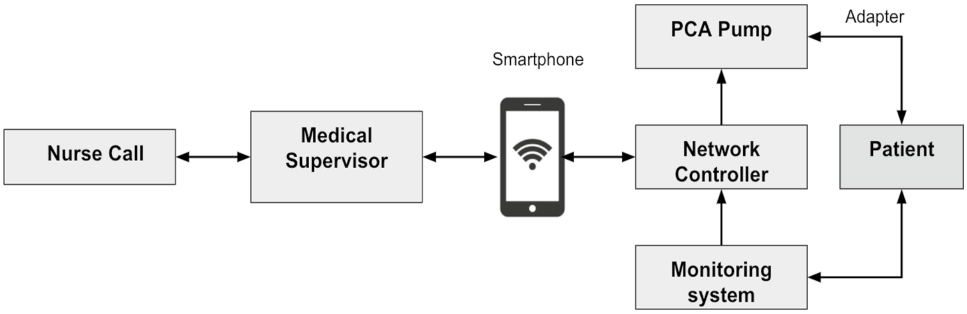


Fig. 5 General structure in MCPS

with the components of the physical world. Sensors and actuators are in charge of transforming the system for the different types of vitality of power, i.e. analogue signal, and vice-versa. ADC and DAC are in charge of changing over proceeds with analog signals to discrete digital signals and the other way around individually [17, 18]. *Scheduling:* Resource scheduling in shared sensors and actuator networks (SANs) is considered an imperative part of any task [19, 20]. Patient information is dealt using a wide array of medical devices that are progressively associated and communicated over the network (Fig. 5). With the purpose of lessen the burden on patients regarding general medical costs, it is important to ensure effective communication scheduling between interoperating therapeutic devices like monitoring system, network controller and Patient Controlled Analgesia (PCA) pump [21, 22]. To study the impacts of the interconnectivity and interoperability of the restorative device and network-empowered control of the patients' wellbeing, a closed-loop clinical situation of medication imbuement is considered through a framework.

Another significant consideration pertaining to the general idea of MCPS is Patient Controlled Analgesia (PCA) that deals with pain-controlled-method patients [23] using a computerized machine to infuse pain controlling drugs into a patient's intravenous line. Figure 6 indicates an outer intravenous Generic Patient Controlled Analgesia (GPCA) in a normal utilization condition. It might be used as a frame of references for demonstrating the uses of engineering techniques for medical devices, and for developing specific implementations of PCA. Patients get the medication from the device through an intravenous needle embedded by the clinician. They are able to self-control endorsed measures of extra medication by squeezing a bolus request button available at the patient's bed [24, 25]. The GPCA likewise has an interface that connects the drug store vault to the doctor's office. In the event that there is a change to the dosage of the medicine, this interface enables the pharmacist to confirm with the doctor that the modified treatment regimen lies within the safe level of consumption for the patient. The GPCA has three essential capacities: (1) Convey medication in light of endorsed timetable and patient solicitations; (2) Counteract perils that may emerge from the use of medication; (3) Screen and advise the clinician of certain outstanding conditions that are experienced by patients [26].

2.2 Classification of MCPS

MCPS is arranged on the basis of classification in Fig. 7**.** The exploration of applications of MCPS in the medical industry is still at its infancy stage. In MCPS, the combination of dynamic client information (for example, the smart feedback system, computerized records of patient information, and inactive client information, related to biosensors and additional smart devices) can support the information procurement for productive decision-making. This blend of

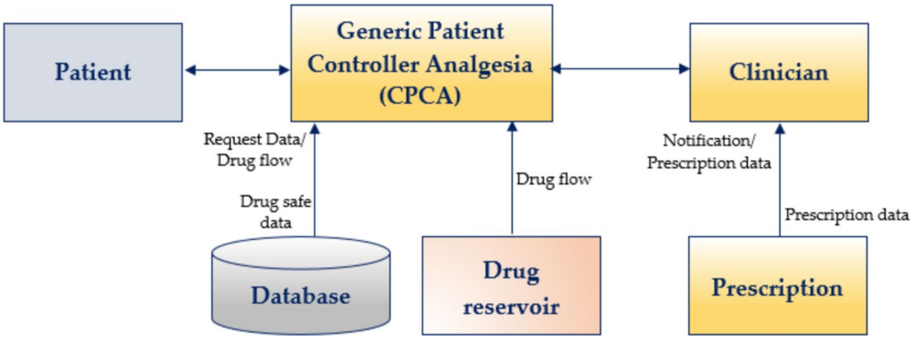
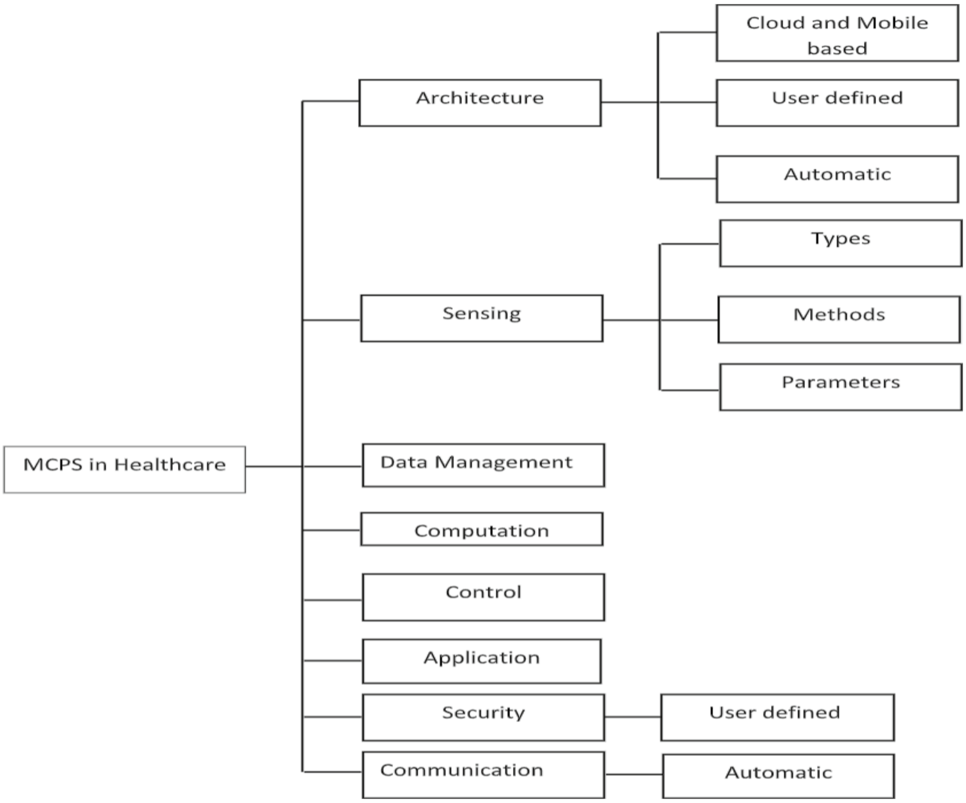


Fig. 6 Illustration of the framework of the GPCA

Fig. 7 Classification of MCPS



information securing and decision taking system is yet to be thoroughly investigated in medical services. Applications in medical services and other social insurance problems would involve a high research premium as it involves multi-dimensional information from a myriad of sources. The chances of using MCPS in human services incorporate the presentation of composing interoperation of self-sufficient and versatile devices. Additionally, it may also incorporate new ideas for overseeing and working restorative physical systems utilizing calculation and control, scaled down implantable smart devices, body area networks, programmable devices and new fabrication methods [31, 32]. In what follows, we highlight some parameters for classification of MCPS (Fig. 7):

1. *Architecture:* The architecture of MCPS systems is very important since the requirement of the quality and the performance of the system. To archive the facility of the system, architecture should be created in light of the application area, client data prerequisites, and system reconciliation. The architecture of MCPS system includes three components: Cloud and Mobile based; User Defined; and Automatic.
2. *Sensing:* Biomedical sensors are in charge of gathering imperative physiological data supplied to the communication system for additional utilization. Sensing is the key for human services as detected qualities are utilized as information parameters of the system. Regular sensing may be difficult for patients, for instance, the blood glucose level (BGL) recognition of diabetic patients requires pricking the finger and gathering tests. To cure this, a non-invasive technique for BGL monitoring utilizing radio-based sensors was utilized [29, 30].
3. *Data Management:* Data Management in MCPS gives a mechanism to control collected data from sensors to satisfy user requirements. Preparing data gives better information collection and communication since sensed data cannot be used in raw format and it requires a large amount of bandwidth and inefficient processing.
4. *Computation:* Performed for two components: modeling and monitoring. Specialists and clinicians need to monitor and screen patients from anytime and anywhere, and they require the capacity to get to required patient data precisely and efficiently. Cloud computing can perform a huge scale of complex computation and communication with the goal that specialists can do without much of a stretch to gather tolerant data from the businesses. It is important to execute methods for diminishing of data bottleneck and figuring of data size to guarantee system proficiency. Cloud computing can give the required computational benefit, and additionally supports superior computing, cell phone reconciliation, and distinctive operating system stage, among others.
5. *Control/Actuation:* Current medical services systems have constrained adequacy in identifying the threshold

value that can be tolerated to be classified as an emergency, and creating an alarm system to alert the relevant approved medical practitioners. In the situation of threshold caution, an alert is created when an imperative sign crosses the threshold value.

6. *Application:* MCPS offers changed applications, for example, medical centers, assisted living, and elderly care. System multifaceted nature relies to a great extent upon the particular application in questions.
7. *Security:* An essential part of the MCPS as patient data is highly confidential and needs to be kept private to ensure compliance with the legal, ethical and moral aspects. In this way, while planning any architecture for medical services applications, additional consideration should be paid to the confidentiality of patient data to guarantee data security.
8. *Communication:* The primary communication is done in two sections: sensing the patient data and interacting with the cloud system. **Major communication** takes place between MCPS and components. Minor communications (or **data communication**) occur through the entire system, for instance, communication of the perception of different stakeholders (e.g. doctors, patients, physicians and pharmacists) that focus on the medical services. The latest improvements in visual communications over wireless multimedia sensor networks (WMSN) can possibly broaden the abilities of the MCPS by permitting extricated and additionally compressed pictures to be imparted in a vitally productive way. This will help with tolerant monitoring and perception, and also an examination of picture data identified with particular physiological parameters. Booking and communication convention are fundamental to effective communication. However, data and communication scheduling are two major problems that should be tackled in MCPS.

2.3 Benefits of MCPS

MCPS is a promising solution for the integration of the physical and cyber world due to several benefits listed below [27, 28]. The benefits listed may often be regarded as salient characteristics of MCPS:

1. *Network Integration:* It is interoperable with Wireless Sensor Networks (WSNs) and Cloud Computing to provide consistent networking benchmarks. It gives network combination qualities, for example, media access control procedures and their impacts on framework elements, middleware and programming that give coordination over networks control over the planning of network transactions and fault tolerances.
2. *Interaction between Human & System:* Displaying and estimating situational alertness from a human view and its ecological changes in parameters are complex for decision making. There is a pressing need for such intricate and dynamic frameworks that can handle such requirements.
3. *Dealing with Uncertainty:* Certainty is the manner, giving verification that a plan is legitimate and reliable. Confirmation may lead to formal verifications or thorough tests in simulations and models. MCPS is intended to have the capacity to advance and work with new and questionable conditions.
4. *Better System Performance:* With the close communication of sensors and cyber foundations, MCPS can give better framework execution as far as feedback and auto remodeling is concerned. Better computational resources and cyber subsystems guarantee the existence of various detecting substances, numerous communication components, advanced programming dialect, and client maintenance which additionally guarantees better framework execution.
5. *Scalability:* MCPS can scale the framework using Cloud Computing. It is intrinsically heterogeneous as consolidating physical elements with computational procedures. The physical area may consolidate mechanical motion control, chemical processes, biological processes and human involvement. The cyber area may join networking framework, programming mechanisms and software designing. MCPS can provide the necessary procedures and devices that help those strategies, which can scale to huge outlines and advance comprehension of complex frameworks.
6. *Autonomy:* MCPS is able to self-govern its own system owing to its sensor cloud alliance. Regularly, it is a closed loop framework, where sensors make estimation of physical flows. These estimations are prepared in the cyber subsystems, which at that point drive actuators and applications that influence the physical procedures. The control systems in the cyber subsystems are versatile and normally prescient.
7. *Flexibility:* A contemporary framework has a considerably higher level of adaptability.
8. *Optimization:* Current biomedical sensors and cloud framework offer vast advancements for optimization of utilizations. This ability opens the pathway to advance its framework in a wider manner.
9. *Fast Response:* MCPS can give speedier acknowledgement time because of quicker preparing and communication capabilities of sensors and cloud framework. Quick reaction time encourages early recognition of remote failure, appropriate use of shared resources, for example, bandwidth. More bandwidth means that more data can be received at the same time, thus, increasing efficiency.

If all bandwidths are used, there is slow response time, but if there is enough bandwidth to receive data, there is faster response time.

2.4 Challenges in MCPS

Developing MCPS obviously requires addressing several challenges. Some of the challenges are listed as follows [33–35]:

1. *High affirmation software:* Software plays an important role in the running of therapeutic devices. Numerous capacities customarily executed in equipment including security interlocks are presently being actualized in software. In this manner, high certainty software improvement is a basic requirement to guarantee the security and capability of MCPS.
2. *Interoperability:* As medical devices and their corresponding interfaces become increasingly interconnected in MCPS, it is imperative to guarantee that the incorporated therapeutic devices are protected, successful, secure and can in the long run be confirmed [36].
3. *Context awareness:* Refers to the ability of the system to respond to user requests based on information related to their environment or context of operations. Medical devices obtain contextual awareness of its operation by communicating with centralized patient records. Medical equipment may also communicate with a common patient to provide real time advisory information. Patient data traded mid-device interoperation may not provide superior comprehension of the condition of patients. However, this system may empower early discovery of infirmities in patients and enable others to be triggered in the case of crises. Given the unpredictability of the human body and varieties of physiological parameters over the patient populace, growing such advanced computational knowledge is a nontrivial job [37]. Push to call buttons, voice dialing capabilities, hands free buttons to call, context aware pill container, context aware hospital bed are some examples that observe patients in context awareness points [38].
4. *Autonomy:* The computational knowledge that MCPS has can be utilized for expanding the autonomy of the framework by empowering the activation of treatments in light of the patient's present health state. Loop closing in this way needs to be done securely and adequately [39].
5. *Security & privacy consequences in patients, data and devices:* Medical data gathered and overseen by MCPSs are extremely basic. Unapproved access or messing with the data can have serious consequences for patients, such as information leak, privacy violation, segregation and mishandling of data, and physical damage. Protecting the security of MCPSs in this manner is a significant component in the development of any MCPS [40]. Vulnerabilities in medical devices pose risks to patients whose privacy depends on proper functioning of devices. While security refers to how personal information is protected, privacy relates to any rights one has for controlling personal information and its uses.
6. *Patient:* an assailant refers to an attacker who penetrates the system illegally. In MCPS, an assailant usually straightforwardly focuses on the patients' wellbeing. This is typically accomplished by focusing on the detecting, handling, correspondence, and treatment conveyance parts of the MCPS [41].
7. *Data leak:* An attacker gets to a patient's data from MCPS in an unapproved way. The result is the loss of patient privacy that would prompt potential separation and manhandling of sensitive data [42].
8. *Device:* An attacker mounts a denial of service (DoS) on MCPS in some frames with the goal that the system cannot play out its errand; thereby constraining device accessibility. Several other attacks like medical hijacking, ransomware attacks, phishing attacks and Trojan attacks may also affect devices. These can likewise bring about loss of privacy in the frameworks that are intended to come up short open as proposed [43, 44].
9. *Communication and Data Scheduling*: The most important issues to make the MCPS efficiently provide services to patients. This relates to major and minor communication, as indicated in Sect. 2.3.

As we clearly see from the above challenges, security and privacy are major problems in MCPS so that we will elaborate them in the following sections.

2.5 Security issues in MCPS

Recent few years have witnessed the issue of restorative device security tended to various classes of therapeutic devices [45], for example, implantable devices [46] and interoperable devices [47]. In majority of these cases, the attention is on specific parts of the MCPS framework to provide specific secure correspondence and viable access control. Some of the tests that focus on the security for MCPS are as follows:

1. *Patient Modeling & Simulation:* Patient models are required for the design of shut circle control, and for the security investigation of situations also. For instance, the shut circle PCA situation requires a model of medication assimilation by the patient's body, as well as the connection between medication dosage and focus and imperative signs displayed by patients, for example, heartbeat rates and respiratory rates [48]. However, complete mod-

els are too perplexing to possibly be utilized as a part of the design and investigation process. Subsequently, the advancement of new deliberation procedures is principal for tending to this test.

2. *User-Centered Design:* Caregiver mistakes in utilizing restorative devices are a noteworthy example of antagonistic occasions [49]. A portion of these mistakes is because of the stress and over-burden that caregivers experience every day. Poor user interface design likewise has been described for a large number of these blunders. In the event that a device is difficult to work, has an illogical user interface, or reacts to user contributions in an unforeseen way, user blunders have a significantly higher probability of occurring. The design and approval of therapeutic devices therefore need to consider user desires and requirements. To utilize show-based design of intelligent restorative devices, models of caregiver conduct should be consolidated. In any case, fusing data about probability of specific activities into caregiver models opens the path for quantitative thinking about device security.
3. *Compositionality:* refers to integration of embedded computer systems and physical processes that the systems interact with. The systems could be embedded devices like intelligent sensors or automation systems. They not only rely on functional requirements but also non-functional requirements such as timing, resource usage and reliability. Interoperable network-empowered restorative devices will ultimately evolve into MCPSs. Compositional thinking is the main thorough approach to guarantee security of such frameworks. It is difficult to anticipate the outcomes of connections between devices and frameworks. For instance, the device giving distinctive medicine to a similar patient may bring about radio impedance in view of the proximity of the devices to one another. Moreover, medication themselves can meddle with each other by influencing physiological reactions in patients [50]. MCPS designers ought to know about these obstructions and guarantee that the framework, giving out treatments, is made mindful of potential meddling in the medications by putting in adequate data settings in place.
4. *Continuous Monitoring and Care:* A standout amongst the most essential needs of medication is to create medical devices that are fit for giving continuous care (i.e. monitoring, choice help, and conveyance of treatment). Such devices are relied upon to diminish health care costs by empowering options, for example, locally situated or mobile care caregivers can have a point by point photo of the patient's well being constantly, empowering them to fine tune the treatment that will be given. Such a framework additionally considers constant notice in case of crises and giving specialists on call precise and complete data about the patient's wellbeing. Continuous care frameworks are being designed to screen plenty of illnesses, for example, cardiovascular maladies [51], neurological issues, gathering meta-physiological state data [52], circadian action monitoring [53] and outrageous condition, therapeutic monitoring [54].

The issue of cyber-security susceptibility related to medical devices requires confining as it comprises a variety of different elements. These incorporate the change from secluded devices to networked devices, the strains this makes on the security and wellbeing; the reasons for the issue not being specialized; and the ensuing conflict amongst direction and produce. Cases of occurrences are given to feature the assorted variety of issues related to cyber-security [55–58].

In what follows, we will explore certain security issues that have been addressed for MCPS over the last few years [4, 26–28, 32–36, 40–43, 47–54, 59–85].

O'Keeffe et al. [26] discussed several key issues related to cybersecurity in medical devices and proposed some arrangements/suggestions. Ray and Cleaveland [27] dealt with integrating security engineering and assurance case development in MCPSs. Sabău-Popa et al. [28] examined the health system with regard to data confidentiality, cybersecurity hazard, and management arrangement. Quadri et al. [32] presented the state-of-the-art provided an overview of various challenges (for example, integration of cloud-computing, programmed testing, and raising of design reflection levels among others). Kanjee and Liu [33] proposed an authentication framework for CPS. Chen et al. [34] proposed a novel run-time predictive safety checking technique that leverages a maximal model coupled with online preparing of a computational virtual subject (CVS) set. Majhi, Patra and Dhal [35] discussed the state of the specialty of CPSs and its utilities. Kruse et al. [36] tried to identify cybersecurity trends, including ransomware, and identify possible arrangements.

García-Valls et al. [40] presented the system based on remote patient observing. Pawlick and Zhu [41] proposed a concept of strategic trust that uses game theory to capture adversarial and strategic nature of CPS security. Cecil [42] discussed IoT based CPSs using two case studies in the areas of manufacturing and medicine. Nithya, Sangeetha and Prethi [43] attempted to summarize the role of CPS in the healthcare and medical field focusing on the architecture development of MCPS, and the key challenges for securing MCPS, as well as examinations on the best way to secure medical data to improve the human lives.

Malathi et al. [47] designed a system that will alert the stakeholders involved by sending notifications to the drug store before a medicine gets expired, whereas Ivanov, Weimer and Lee [48] studied the problem of context-aware detection in the MCPS area. Rushanan et al. [49] and Gunes et al. [50] discussed security threats and privacy issues with respect to Implantable Medical Devices (IMD) and Body Area Networks. Finnegan and McCaffery [51] established confidence in security assurance of medical devices. Sametinger et al. [52] discussed several security challenges in medical devices and prevention techniques like secure update mechanisms, surveillance strategies, malware detection methods, formal methods, etc. AlTawy and Youssef [53] discussed the tradeoff between security, safety, and availability in medical devices. Mashkoor and Sametinger [54] proposed a 'correct by construction' approach in order to monitor and analyze interoperable medical devices with respect to functionality, safety and security level.

Mohan [59] presented cyber threats to devices and constraints of Personal Medical Devices (PMD) and IoTs addressing these cyber threats. Arney et al. [60] presented a way to deal with approving middleware selection for MCPSs using user needs as documented in design columns and clinical requirements. Adyanthaya et al. [61] presented the xCPS research and education stage designed to be representative of CPS with industrial-size complexity.

The healthcare industry is lucrative for attackers since it contains sensitive patient records. Data may be stolen from EMRs, patient accounting systems and other information systems. The following are some of the security issues that are common in MCPS:

1. *Ransomware:* is malicious software that is capable of blocking access to a computer system unless a sum of money is paid. It may prevent organizations from accessing certain parts of the system; thus, affecting patient records. The risk of losing valuable data may impact the overall productivity.
2. *Distributed denial-of-service* (DDoS): attack aims at making online services unavailable by overwhelming it with traffic from multiple sources. DDoS attacks may deny access to users, prevent patients outside from accessing the websites and prevent doctors and hospital staff from sending or receiving emails.
3. *Social engineering attacks*: like phishing are used to steal information using credentials, such attacks may lead to data breaches and patient records may get compromised. Healthcare sector is among most at risk from social engineering. Hackers may gain sensitive data by means of phishing, spoofing, dumpster diving etc.
4. *Malware*: a software program that intends to damage or disrupt computer systems. Medical devices are vulnerable and may connect to a number of sensors and monitors; thereby, making an entry to hospital networks to affect sensitive medical records. The health information incorporating sensitive data may be compromised.
5. *Web based attacks*: like SQL injection and cross site scripting target healthcare websites due to doctors and staff inside healthcare organizations demanding web applications for fast access to medical records, test results and other critical data.
6. *Cyber physical attacks*: affect the physical systems and have the capability to do serious physical damage to medical equipment and interfere with patient care. Some of the Cyber Physical Attacks that MCPS are prone to are as follows:

- *Telesurgery*: incorporates a surgeon at a given location to perform operation at another location. A teleoperated robot, Raven II was hacked with the intention to reveal the vulnerabilities, which may be in the form of malicious commands sent by operator to the robot, modifying the intention of signals from operator to robot arm and hijacking the robot completely [83].
- *Insulin pump hack or Drug Infusion Pumps*: is a recent cyber-security issue in medical devices wherein the device alerts additional doses of diabetes drug to users which could lead to severe consequences [85]. The infusion pumps responsible for delivering nutrients, insulin, hormones, antibiotics, pain relievers, drugs, etc., if compromised, may allow a remote attacker to gain unauthorized access and impact the operation of the pump, as well as varying the dosages.
- *Heart Rate Monitors hack*: is surprisingly easy and requires an oscilloscope, a computer, wireless radio and some free software to perform. It does not require a network, rather uses radio, which may be vulnerable to attacks, as the radio signals are not encrypted. Thus, if the device is tampered, a big shock may be delivered by the device which may be lethal to the patient.

7. *Man-in-the-Middle*: also poses threats to the healthcare industry. Health information may be compromised by attacks on data while it is in the process of being transmitted from one point to another. Sensitive information like patient records may also be altered by the adversary.
8. *Automated applications*: like Bots can be used as malwares to gain access to computer systems in a healthcare organization. Once a boot is in the respective environment, it may access personal data, insurance accounts, vendor accounts, patient data etc.
9. *Account Hijacking*: lead to compromise of sensitive information like Social Security, driver's license and credit card numbers along with medical records and insurance information.
10. *Device malfunctions*: may also be a result of cybersecurity attacks, which may lead to ineffective treatment or severe consequences. For example, if a pacemaker gets hacked, electricity may be sent to the user inappropriately, which may not have positive out-

comes. Moreover, it is difficult to comprehend if the device was hacked or not.

11. *Orangeworm attacks:* are concerned with deploying backdoors in targeted healthcare industries. The malware is installed on medical devices like X-ray and MRI (magnetic resonance imaging) machines in order to copy images for the purpose of cyber espionage [81].

We find that there are several limitations to the existing work ranging from security issues in medical devices to infeasible countermeasures proposed [86–90]. This forms the basis for our proposed work that could address all the security issues of MCPS.

3 Proposed Work

3.1 Dealing with security issues in MCPS

In the previous section, we presented the overall idea of MCPS, its classification based on social insurance, its benefits as well as challenges and various security issues in MCPS also. In this section, we introduce a cyber-security framework considering the issues that arise in MCPS along with Interactive Model.

We have already been familiarized with several possible security issues that pose a risk to MCPS and some possible solutions in Sect. 2.5. However, they do not guarantee complete security for the MCPS environment. Although it is impossible to eradicate all the security issues, there could still be concrete solutions to handle most of the security issues. We present it in the form of the proposed cyber-security framework for the MCPS.

The cyber-security framework for MCPS aims to protect the MCPS infrastructure by managing security risks. Security issues may range from identifying a particular threat to recovery of a system after a security breach has already taken place. There are several cyber-security frameworks based on Tiers and steps [76, 77]. Several other cybersecurity frameworks like the PCI DSS (Payment Card Industry Data Security Standard), COBIT (Control Objectives for Information and Related Technologies) and ISO 27,001 have also been highlighted in the past. While the NIST cyber-security framework fails to address risk level and risk measure [78] and does not comment on maintaining trust, ISMS Cyber-security Framework follows a process centric, product centric etc., assessment framework. HIPAA (Health Insurance Portability and Accountability Act) security framework places an expensive burden on companies that have access to private health data. Thus, there is a need to introduce a framework that would take care of the risk, threat and trust related issues, and is also flexible.

Keeping in view the fact that the NIST model lacks risk modelling, trust modelling and threat modelling, we introduce a new cybersecurity framework for MCPS that takes into account these factors too. The cyber-security framework for MCPS is based on several individual models that collaboratively work towards securing the MCPS infrastructure. Each of these models is responsible for carrying out specific approaches in order to provide resilience to the infrastructure. We accentuate what each of the models is capable of doing and how security measures like identification, defense, risk etc. may be assured by the framework by deploying certain systems and adopting several services. Figure 8 represents our proposed cybersecurity framework for MCPS.

1. ***Identification Model:*** Identification Model is responsible for detecting security issues that might crop up in MCPS. The idea is to comprehend how security issues may affect the infrastructure. MCPS are prone to several security issues ranging from ransomware to device malfunctions. If unidentified, these poses may lead to serious repercussions in form of data tampering, system unavailability, breaches etc. The model may be implemented by managing hard assets, soft assets and policies, as described below. Every component of the infrastructure is taken. The identical model primarily focuses on the following components (Fig. 8):

- *Asset Management:* Hard assets such as servers and networks, soft assets such as data, software and people are the basic components that must be managed and identified. Servers and networks may be managed by applying patches and obtaining detailed system reports to make decisions.
- *Policy management:* Policy management underpins policies, procedures and processes which are essential for managing and monitoring an organization so as to create awareness in the situation of a cyber security risk. Policy management is usually performed by consultation, training the employees, reviewing policies regularly and ensuring consistency.

The identification model aims at detecting security issues at different levels so that attack implications may be avoided. For example, if a malicious packet is detected, port numbers may be blocked, or firewalls may be turned on as per policies so as to disable the network traffic from penetrating the system. Not all security issues may be identified. Advanced malwares with modified signatures may be difficult to identify. Assets may be damaged, for example, server overloads may not allow servers to be up and running for several hours.

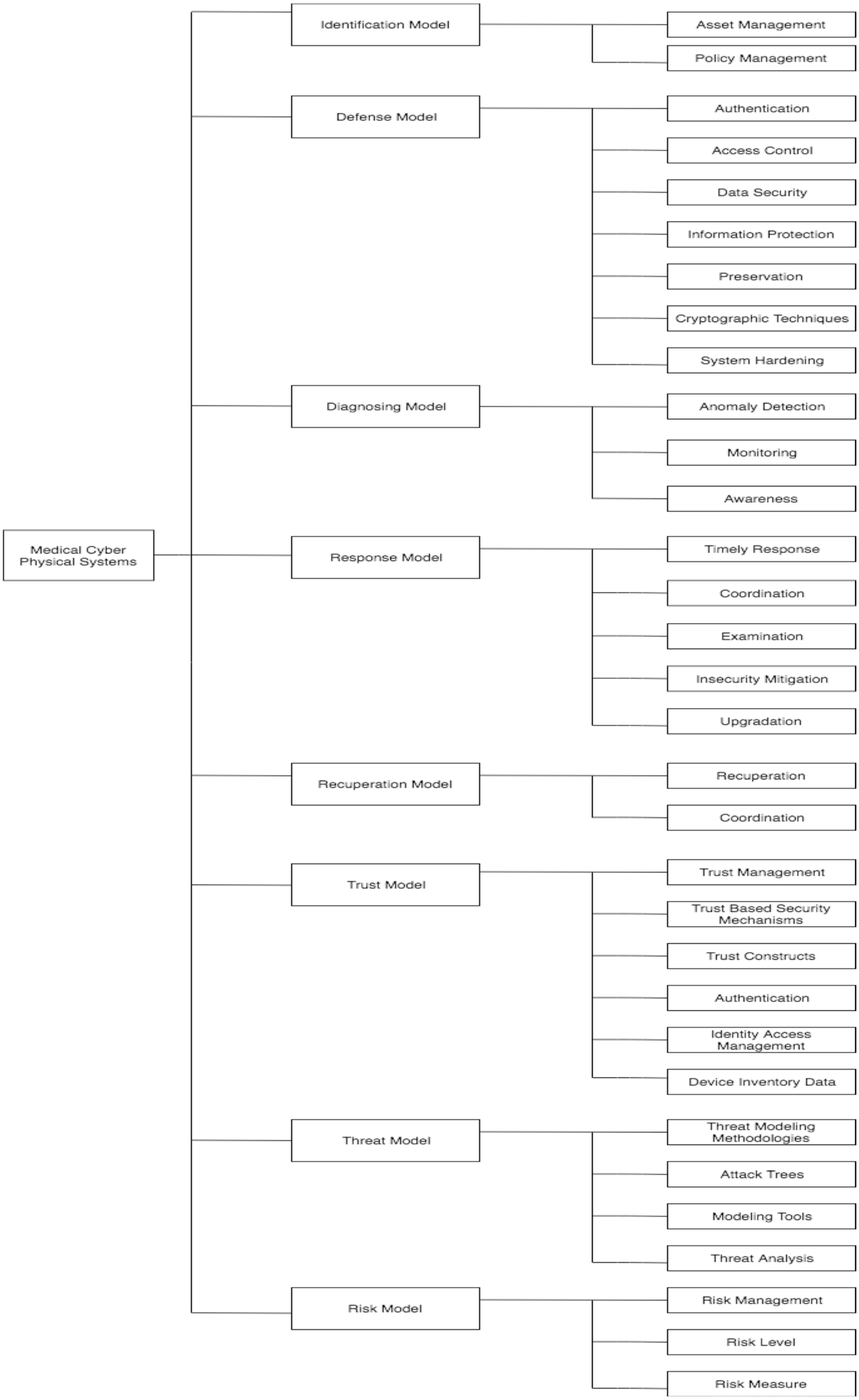


Fig. 8 Proposed cybersecurity framework for Medical Cyber Physical System (MCPS)

2. ***Defense Model:*** To ensure that the MCPS infrastructure is not vandalized by certain security issues like web-based attacks, denial of service attacks etc., it is required that the infrastructure is defended against any system assault. The Defense Model is responsible for introducing defensive techniques in order to protect the MCPS infrastructure.

MCPSs are associated with medical data that are very sensitive; thus, making a protection model very essential. Healthcare industry deals with data ranging from patient's health information to credit card details. The sensitive data may be prone to leakage. Further, medical devices may be prone to hacks and malfunctions. Therefore, a defense model is required to ensure that the system is defended against such attacks. To ensure that medical devices are defended against security issues, several techniques may be adopted like authentication using passwords, access control by defining privileges to users, securing data using backups, protecting information using policies, adopting cryptographic techniques (hashes for passwords) and system hardening mechanisms, which have been explained below. This model is based on the following functions (Fig. 8):

Authentication: Verifying the identity of a person or device. By authenticating user actions and attributes, a system may be defended against fraud and abuse. Authentication may be a single factor like basic username passwords, multifactor like logging into a website and then requesting a one-time password. Emergency authentication is used to provide emergency access to users who has lost or damaged tokens. A token code may be used in the absence of a token and users may rely on two factor authentications for the same.

Access Control: defined as a security technique that ensures who can view or use resources in a computing environment. It deals with selective restriction of access to a resource. MCPS involves interaction with a large number of entities and devices over a network. This means that the information associated with MCPSs are not constant, but moving across several assets such as servers, devices, and network elements. Therefore, the assets must be accessed only by authorized users keeping in view of the sensitivity of the data as well as other sensitive functions of the system. Identity and access management systems are a way to control access.

Data Security: MCPS involves a lot of data acquired through sensors. The data are confidential, and it is vital to secure them in order to maintain confidentiality and integrity of MCPS. Access management, developing data security plan, developing strong passwords and regularly backing up data can enhance data security.

Information Protection: information systems and assets pertaining to MCPS must be protected using specific guidelines, policies and standard operating procedures.

Preservation: Preservation of information systems and assets so that they are not able to be tampered with. Migration, encapsulation and replication of data are some ways of preserving it.

Cryptographic techniques: Due to their size and complexity, reasonable cryptography may not be applied to MCPS. However, Lightweight cryptography techniques such as soft block ciphers like blowfish, Data Encryption Standard (DES) or Advanced Encryption Standard (AES) or light encryption techniques such as substitution and permutation could be used in MCPSs to ensure security.

System hardening: Securing a system by hardening it eliminates several security risks. This keeps untrustworthy components at bay and ensures integrity of the system. Security critical applications must be isolated from untrustworthy platforms, so as to increase the safety levels of the MCPSs. Deploying firewalls and intrusion detection systems could harden the system.

The defense model is associated with authentication, access control, data security, information protection, cryptographic techniques and system hardening. All these techniques have the ability to add additional security layers. Using the stated techniques, we may limit data access to adversaries, prevent unauthorized access and promote confidentiality, integrity and availability which form the basis for a secured system. Since the system is equipped with an additional layer of security, it ensures defense. For example, to ensure that the patient records are confidential, one might need authentication to access the data. Passwords and hashes may contribute to that Access rights may be given to individuals based on their responsibilities. Defense models may encounter challenges in the form of many password guesses and attacks as well as root hacks. Cryptographic techniques may be slow to implement.

3. ***Diagnosing Model:*** A diagnosing model is responsible for carrying out functions with the aim of identifying security incidents and events, and these tasks are usually performed in real time. When MCPS are hammered by security incidents and events, it is necessary to recognize the indicators. Unlike the identification model, where the system establishes the identity of the security issue or anomaly, the diagnosing model is concerned with discovering the issues with proper examination. The idea is to not only identify the issue, but to also see what causes it. If the cause of the issue is not known, it may be difficult to fix the issue. Determining the cause ensures that the patches are made in the early phases so that issues may be rectified at the earliest (Fig. 9).

For diagnosis, anomaly detection may be considered by intrusion detection systems. Network and system may be supervised using monitoring tools. Alerts and alarms raised by Intrusion Detection Systems and Intrusion Prevention Systems assist in making one aware of

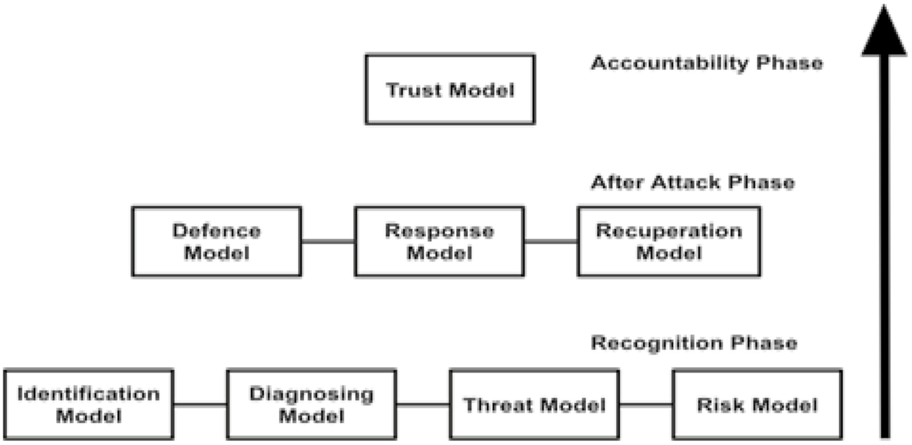


Fig. 9 Interactive Model for the proposed Medical Cybersecurity Framework

abnormalities. The following are responsibilities of a diagnosing model.

Anomaly Detection: Anomaly detection is a promising approach to enhance security levels in MCPS. The idea is to monitor abnormal behavior in real time. The system will be alerted in the occurrence of an abnormal event. Intrusion detection systems and Intrusion prevention systems may assist in anomaly detections.
Monitoring: MCPS assets and information systems are monitored from time to time. The current state of the infrastructure is compared to the previous state in order to detect security issues, and also to verify the level of effectiveness of the safeguarding techniques of the security system. Network monitoring tools are effective in monitoring.
Awareness: It is important to be aware of anomalous events. This is ensured by several processes and techniques. When information systems and assets are timely tested, diagnosing security issues becomes easy. Checking for alerts and logs is one way of ensuring awareness.

The diagnosis model is responsible for scrutinizing several cyber physical attacks; we based attacks, device malfunctions as well as hacks. Early detection of security issues ensures that patching is done in the initial stages. For example, if a remote device stops working, one might need to investigate if the issue is with the server or if it is just a device malfunction, so that appropriate measures may be taken. If the server has issues, it might affect the functioning of other devices too.

Diagnosis may not be performed for security issues that the system does not recognize. Since anomaly detection and monitoring are some techniques used in this model, an Intrusion Detection System may fail to recognize traffic.

4. *Response/Feedback Model:* A response/feedback model comes to aid, when a cyber-security event has already taken place in the MCPS. It does not generate responses for MCPS that have been criticized by cyber-attacks since there would be neither an examination nor any patchwork. Effective incident response activities are adopted so as to respond to the security event in a quick and efficient manner. A timely response in form of a response plan that is well coordinated and examined might evade insecurities using technical controls and measures. A patchwork or upgrade followed by the same contributes to the repairmen of the affected system.

The healthcare industry is coordinated between the medical devices, data and the communication network, and all three are susceptible to security attacks like hacks, malwares or device malfunctions. Once the network, device or data has been compromised, it is necessary to respond to such events. Disregarding which may lead to the system becoming further detrimental. For example, we find one of the databases incorporating patient records is affected by malware. A timely and coordinated response would prevent further damage to the system. A response /feedback model has the following functionalities (Fig. 8):

Timely Response: The identified cyber-security events must be responded to in a timely manner. A response plan incorporating the standard operating procedures and processes is responsible for the same. This could lead to a mitigating impact on devices, healthcare systems and patients if cyber-security attacks are responded to in a timely manner. One of the ways to generate timely response could be an incorporation of an effective and appropriate incident plan that ensures flexibility and clarity. Patients should be allowed to timely access their websites and reports.
Coordination: In the event of a cyber-security issue, it is mandatory that the information be communicated throughout the infrastructure. This is in order to carry out a thorough response plan.

Examination: After a cyber-security incident has taken place, alerts and notifications from the system are examined and their aftereffects are comprehended.

Insecurity Mitigation: Insecurities in the form of vulnerabilities and risks, once identified, are eliminated by using proper procedures. Several vulnerabilities may lead to medical devices being susceptible to tampering and modifications which could pose severe risks to patient health. These may be taken care of by technical controls, governance, resilience measures, consolidated reporting, context expertise, regulation, and standards.

Upgradation: Upgradation refers to patchwork. Once the vulnerabilities and security issues have been identified, the system needs to be repaired, so that it is no more vulnerable to the already identified vulnerabilities and risks.

The Response model supports the ability to contain the impact of potential cybersecurity incidents. It is not only concerned with responding to the security issues in a timely manner but also ensures that the system is updated so that it may avert security issues in future. For example, a malware affected database may be patched and upgraded to a point that it becomes immune to the specific malware in future. The timely response may be achieved only after the issue has been identified. Coordination may not be that simple. It ensures resistance to a specific malware but does not guarantee security from other potential malwares.

5. *Recuperation Model:* This model may be used to impart resilience to a system, which is the next important thing after a system has been upgraded. It does not ensure recuperation to affect the strength and flexibility of the system in the sense that the system might be prone to the same security issue again and again. System recuperation may be ensured using certain processes and procedures ranging from hardware repair to use of data recovery software. Once data is recovered, the information is coordinated across the infrastructure by collecting, verifying and storing data.

A recuperation model comes to aid after the MCPS gets impaired due to a cyber-security incident. For example, a specific database if infected with a worm. The patchwork ensures that the database is no longer prone to be affected by the said worm. But the other databases may still be infected by it. Thus, once the patchwork has been done, it is coordinated across all the other databases, so as to impart strength and stability to the entire system. A Recuperation Model is concerned with the following functions as indicated in Fig. 9:

Recuperation: Information systems and assets that have been vandalized by cyber-security incidents need timely recuperation. This is undertaken by several processes and procedures.

Coordination: Once the information systems and assets have been recuperated, the repaired information is coordinated across the entire infrastructure.

The Recuperation Model brings strength and flexibility to the overall system. As the system becomes more and more flexible to avert security issues, it also becomes stable. Considering the example stated above, once all the databases are immune to a given attack, the system is more resilient towards the attack. It may take a lot of time and computation power to ensure stability, flexibility and strength to systems that have a very large number of databases.

6. *Trust Model:* This model is particularly used to identify procedures for responding to threats and defines the extent to which a system can be relied upon. MCPS are used for carrying out sensitive activities which is why ensuring trust is paramount. Trustworthy assets can contribute to the trust model. Public Key cryptography, certificates, multi factor authentication and policies are some ways to ensure trust in MCPS.

The infrastructure, devices, assets and data concerned with MCPSs demand trust due to sensitive operations as well as sensitive data it deals with. While devices here refer to equipment made for a definite purpose, an asset is more of assumptions. In the healthcare domain, both devices and assets have their specific requirements. The trust model is based on transparency and accountability. The security issues hampering trust are in the form of phishing attacks or man in the middle attacks that aim at procuring sensitive data. Once medical devices be hacked, they may have difficulty in exhibiting transparency as they may not behave as initially directed to. Thus, Trust model is necessary to ensure transparency. It consists of the following functionalities (Fig. 9).

Trust Management: Trust management is based on the understanding between multiple parties in order to carry out sensitive transactions (interaction), and it is important to ensure trust between clinicians, patients and staff. Regular checks and verification at every level of interaction may ensure trust.

Trust based Security Mechanisms: Trust based Security Mechanisms can be used to encapsulate an individual's trust in another individual. These could be in the form of legal protections, institutional solutions or technology related.

Trust Constructs: It is based on trusting behavior, intention and beliefs. Trust establishments may be of various types such as interpersonal trust, system trust, dispositional trust and situational trust.

Authentication: Authentication ensures trust by confirming the validity of data or an entity. Two-factor authentication is predominantly used to access personal health records which are incorporated in MCPS.

Identity Access Management: enables authorized entities to access authorized resources. It is used to identify, authenticate and authorize entities to access resources, thereby ensuring trust.

Device Inventory Data: A device inventory refers to a database of all physical assets over the computer network that is incorporating information. The data can be used to ensure trust even if access requests are not authorized.

By ensuring Authentication, Trust Controls and Identity Management techniques, etc., the model safeguards confidentiality, integrity and availability of the overall system. Data may be accessed only by the authorized users. The model also reinforces transparency and accountability. For example, a particular database may be accessed by a specific group of users, some of which may be allowed to read and read, the others only read. Whatever changes are made are reflected in the database and are known to all.

As mentioned above, regular checks and verification at every level of interaction may ensure trust. Thus, trust must be ensured at the very basic level in form of the functionalities listed above. If there is no trust ensured in the basic level, as the levels progress, each level will lose transparency. Some other challenges while establishing a trust model may be in form of unavailability of servers or connection errors.

7. *Threat Model:* The Threat Model has been introduced to optimize security by recognizing the purpose and vulnerabilities of the system in order to define ways to prevent the threat effects. Threat Modeling may be addressed through certain methodologies, tools and analysis, which have been discussed below.

A threat may be malicious and may be capable enough to damage the assets of an infrastructure. MCPS are also prone to security threats like man-in-the-middle attacks and malwares. These threats are capable of infecting systems and abusing sensitive data. Threat model considers the following functions (Fig. 8):

Threat Modeling Methodologies: Threat modeling can be used to identify security requirements, such that it could be implemented in the software systems of MCPS. This leads to software security and reliability. Several threat modeling methodologies exist, some of which include STRIDE, Trike and VAST.

Threat modeling using Attack Trees: Conceptual diagrams illustrating how assets may be vandalized may assist in detecting threats. These are known as attack trees. Threat modeling using attack trees can be performed using attack tree software such as SeaMonster and ADTool.

Threat Modeling Tools: Another way of ensuring threat modeling is using threat modeling tools. Some of the threats modeling tools are Microsoft's free threat modeling tool, MyAppSecurity and securiCAD.

Threat analysis: Defined as the technique of gaining knowledge on the internal and external information threats in order to match against actual cyber-attacks. It can be used to provide the probability of instances and the outcomes of disrupting a system.

The threat model aims at identifying and addressing threats in a MCPS system. Further, security decisions may be made rationally, and attack surface is reduced considerably. A communication channel compromised by man in the middle attack may be studied using threat analysis. Once the security requirements are identified and the system is patched, the attack surface is reduced considering this particular threat. It also increases software reliability. It is difficult to completely evade threat. Since no system can be completely secured, some threats will always exist.

8. ***Risk Model:*** Risk may be defined as threat time's vulnerability time's consequences. It is not only confined to infrastructure disruption but is also concerned with financial losses and reputation of an organization. Risks may be characterized by their level and measure (Fig. 8).

MCPS being involved in sensitive activities involve risk, thereby making it mandatory for a Risk Model to be a part of the framework. Lack of a risk model may lead to risks not being identified at different stages which may lead to drastic effects. There are risk management models, risk management tools like Manufacturer Disclosure Statement (MDS2) and Medical Device Risk Assessment Platform (MDRAP) that can effectively assess risks by analyzing healthcare systems and device manufacturers [79]. Thus, it eliminates threats and vulnerabilities and aims to minimize the unsatisfactory consequences.

Risk Management: There are cyber-security risks involved in the operations, assets and individuals which must be identified. MCPS is susceptible to several attacks, and this could lead to loss of data and resources and may invite several security risks. Hence, it is necessary that any kind of risk must be identified and managed at the very early stage.

Risk Level: Defined as the level of risk calculated as a function of likelihood and consequence. The likelihood could be in the form of a cyber risk, whereas the consequence could be damage to assets, infrastructure, monetary, etc. A cyber-security risk matrix may be used to predict the risk level.

Risk measure: It is a measure applicable to risks. It is the attribute of a risk being measured. It could be defined on the basis of exposure of a cyber risk as well as its uncertainty.

The risk model as mentioned above eliminates threats and vulnerabilities and also minimizes the unsatisfactory consequences. Risks may exist in the form of device hacks, ransomwares, phishing etc. Consider a database containing some information about patients. If there is a security glitch, it may be possible for an adversary to access adjoining databases by means of primary keys or candidate keys. Thus, if the risk is mitigated at the basic stage, it may not be possible for the adversary to access other relevant data. Internet, hospital networks, medical devices may provide features that improve healthcare and increase the ability of health care providers to treat patients but at the same time these features also increase the risk. Also, risk is a relative term, specific to its environment. The models, although responsible for carrying out distinct operations, are associated with each other for carrying out these functions. We can classify the models on the basis of Recognition Phase, After Attack Phase and Accountability Phase (Fig. 9).

We observe that Identify, Diagnose, Threat and Risk belong to the Recognition Phase (Low Level). These models are responsible for identifying insecurities, abnormalities, threats, vulnerabilities and risks. The framework initially tries to identify all the insecurities and then moves a level above by identifying threats and then risks. Since risk is threat time's vulnerability time's consequences, it is easy to identify risks once the threats are identified.

After the Recognition Phase, we have the 'After Attack' Phase (Medium Level) which incorporates the Defense, Response and Recuperation Models, which function only after an attack has been initiated or identified. The goal is to protect the system from insecurities, provide resilience to a system or initiate effective incident response activities.

After the last two phases have been considered for ensuring security in a system, the Trust or Accountability phase (High Level) may be accessed. This phase ensures transparency and accountability due to involvement of trust mechanisms and authentication. As is evident from the figure the models in the framework interact using a bottom up approach, therefore the models in question may be classified as Low Level, Medium Level and High Level as mentioned previously.

The framework proposed is based on collaboration of certain models, each responsible for carrying out specific cyber security functions. We present a comparison of the

Table 1 Comparative analysis of the framework models

Model	Responsibility/ operation	Some attacks to prevent	Level
Identification	Asset management, policy management	Malware, DDoS, phishing, ransomware, data thefts [80], orangeworm [81]	Low level
Defense	Access control, data security, information protection, preservation, cryptographic techniques, system hardening	Ransomware, DDoS, data breach, loss of devices, device malfunction, orangeworm [82], telesurgery hack, drug infusion pump hacks [83]	Medium level
Diagnosing	Anomaly detection, monitoring, awareness	Cyber physical attacks, web based attacks [82, 84], device malfunction like pacemaker hacking, Telesurgery hack [83], insulin pump hack [85], heart rate monitoring hack, drug infusion pump hacks	Low level
Response/ Feedback	Timely response, coordination, examination, insecurity mitigation, upgradation	Ransomware, malwares [86], device malfunction, orangeworm [81], heart rate monitor hack	Medium level
Recuperation	Recuperation, coordination	DDoS, Malware, Ransomware [87]	Medium level
Trust	Trust management, trust based security mechanisms, trust constructs, authentication, identity access management, device inventory data	Phishing, man-in-the-middle [88], telesurgery hack [81, 83], insulin pump hack [85], heart rate monitor hack	High level
Threat	Threat modelling (attack trees, methodologies, tools, analysis)	Phishing, DDoS, bots, ransomware [89], device malfunctions like pacemaker hacking, heart rate monitor hack, drug infusion pump hacks	Low level
Risk	Risk management, risk level, risk measure	Ransomware, phishing, account hijacking [90], orangeworm [81], insulin pump hack	Low level

models on the basis of the issues they address; some associated attacks as well as the levels they depict in Table 1.

Based on the comparative analysis, it is evident that some of the attacks like Distributed Denial of Service (DDoS), Phishing, Ransomware, Malwares, Bots etc. possess the capability to affect multiple aspects of security. As is evident, most of these attacks have already been discussed in Security Issues in MCPSs. Thus, it is found that our framework incorporating several models takes most of the mentioned security issues, highlighting its robustness.

In this section, we have presented a novel framework for MCPS devices from the Cybersecurity point of view. Cybersecurity underpins several concepts like Identification of attacks, Defense, Trust, Risk etc. Based on these concepts we devised a framework incorporating several models, each specific to a particular cyber security aspect. These models incorporate several techniques and strategies. We have addressed the importance of these techniques and suggested various solutions to mitigate certain security issues. The framework is robust enough to handle a lot of security issues and their variations. Table 1 gives the overall idea about the types of security issues each of the models may be capable of handling. It may be deduced that almost all security issues may be classified into one of the models based on the security aspect they violate or affect. Since we have already addressed the mitigation strategies and suggested techniques to evade these issues, it may be inferred that the framework is capable of handling a large number of security issues due to the specific functioning of each of the models. Once the system is vandalized, security issues may proceed to different levels. Each level will have a different approach to handle the issue. The levels are connected, so are the security models. MCPS devices demand a high level of accountability, making the trust model one of the most sought after models. Figure 10 depicts that in order to ensure accountability, a system must be capable of identifying and diagnosing the threat in the recognition phase. An After-Attack phase would ensure proper defense and patch work of the system so that the system is protected from such attacks in future. This would ensure accountability. Therefore, the proposed framework may be beneficial to the healthcare industry as well as patients for ensuring security and accountability. Based on the framework certain security techniques may be deployed which would further make the healthcare systems difficult to vandalize.

3.2 Evaluation methodology

The underlying idea of introducing the MCPS Cybersecurity framework is devising means to ensure that any kind of cyberattack may be classified into one of the models and appropriate steps may be taken to secure the overall system. This contributes to the security aspect of MCPS. As we know, several cybersecurity frameworks have been proposed in the past as far as the industry is concerned. However, quantitative evaluation of the security frameworks has never been highlighted in many of the cybersecurity frameworks proposed before. This is due to two reasons:

1. Security breaches know no bound, and it is impossible to say that a system is 100% secure. Our aim is to introduce models which cover almost all security aspects known to us, so that any security attacks on MCPS may be clas-

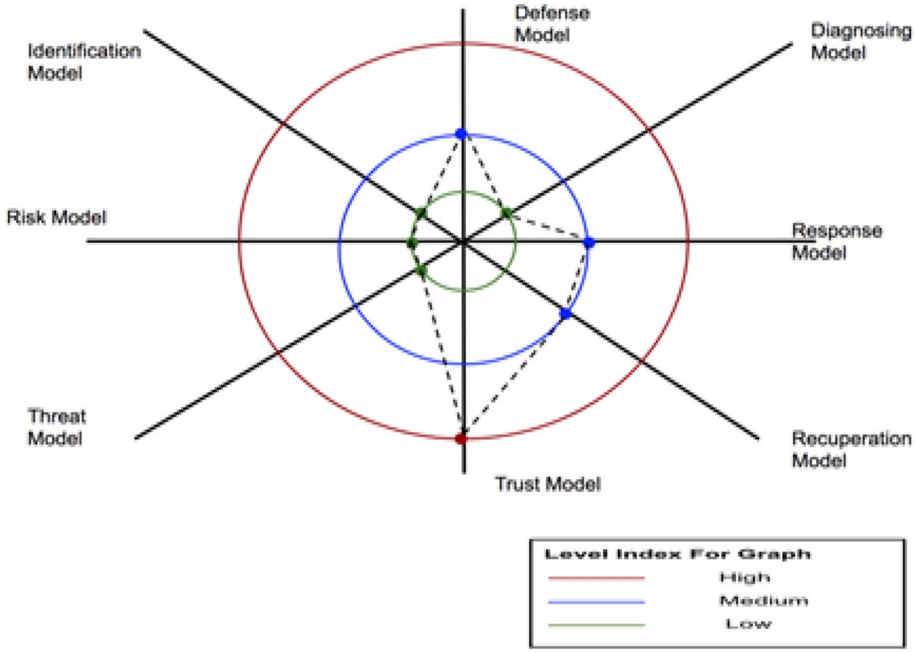


Fig. 10 Graph depicting Qualitative Analysis of the Models

sified into one of the models listed above, for which the evading techniques have also been specified.

2. There is a lack of security metrics, due to which an overall quantitative evaluation for any security framework is impossible. Even though certain parameters like, reliability, number of incidents, cost, risk etc. may be calculated using specific techniques; these tackle only a part of the framework and not the overall of security for a system.

We refer to the interactive model for evaluating the framework non-quantitatively. [123] proposed a security framework for cyber ranges, and assigned qualitative values to the parameters, which was further shown in a plot. [124] proposed a similar framework of unquantified data and used the very same idea to present and evaluate their security framework. The interesting evaluation approach highlights evaluation of frameworks with multiple parameters bearing unquantified values. To evaluate our proposed framework, we will also be considering the same scheme. Consider the following graphical representation (Fig. 10). We have represented each of the models in the cybersecurity framework in the form of axes. The three circles represent low, medium and high. The points correspond to the value (Low, Medium, and High) for each of the models. This unquantified data has been extrapolated from the interactive model (Fig. 9), where we follow a bottom up approach. The Identification Model, Diagnosing Model, Threat Model and Risk Model are the initial stages i.e. the Recognition Phase and therefore are given value Low. The Defense Model, Response Model and Recuperation Model are the mediocre stages i.e. the After Attack Phase, thereby acquiring Medium value. The Trust model or the Accountability phase is subsequently assigned value High. Using the values, we obtain the following plot.

The framework presented has been depicted graphically taking into account the various models as well as the interaction between various levels. We may conclude that:

1. If the points are closer to the center, the model belongs to Recognition Phase or Low Level in bottom up approach, these attacks are easiest to launch.
2. The points that are the farthest belong to the Accountability Phase or High Level in the bottom up approach, these attacks are difficult to launch.
3. The points lying in between the two phases correspond to After Attack Phase or Medium Level in the bottom up approach. These attacks are somewhat easy or difficult to launch.

If an attack is believed to originate from the center, the Recognition Phase Models are the first ones to get affected. This is justified because the initial stages of an attack deal with identification, risks, threats and sometimes even diagnosing. Thus, from a security point of view, these models are the most vulnerable ones. The next phase to get affected after the Recognition Phase is the After Attack Phase which would evidently deal with defending, responding and recuperation. These models are less vulnerable than Recognition Phase Models. The point lying the farthest from the central belongs to the Trust Model. This model is the most difficult to attack and is also a part of the Accountability Phase.

3.3 Comparative Analysis

In this section we present some of the existing cybersecurity frameworks as well as proposed cybersecurity frameworks and perform a comparative analysis against our proposed cybersecurity framework. Table 2 presents the comparative analysis with existing works.

From Table 2, it is evident that conceptual frameworks proposed are not evaluated, and most of the known cybersecurity frameworks perform evaluation using a self-assessment set of questionnaires. While the questionnaires may be a good way to estimate how secure a system is, it might not be completely robust since the assessment would be question specific. In our research, we have performed an in-depth analysis of the security issues that exist in MCPS and considered security models that underpin each of these security issues, thereby enhancing overall security. We also observe that none of the model stress on interaction between the elements of the framework. This is necessary to form an opinion about how damaged a system is so as to easily identify the propagation of the attack. Also, interaction between models acts as a checkpoint in order to assert if a system can be isolated beyond a point so that the attack may not perpetuate further. Finally, the conceptual frameworks proposed in the past do not highlight the trust aspect of security. Accountability is a significant feature when it comes to security. In our proposed framework, we include the trust or accountability component and assert that it may be achieved if all the other models function correctly. The comparative analysis indicates that the proposed framework is superior to Industry standards cybersecurity frameworks as well as proposed conceptual frameworks.

Since the framework is designed for MCPS (and IoT devices), the scalability of the framework would mean the addition of more systems and devices. While the memory and power consumption may increase due to additional devices, there are ways to reduce the memory and power consumption by using IoT platforms, embedded ReRAMs or other embedded memory options [135–138]. One of the best ways to determine real time attacks is by intrusion detection systems [139, 140], which is mentioned in the proposed diagnosing model in the cybersecurity framework. However, cyber-attacks know no bounds and therefore, many zero-day

Table 2 Comparative Analysis of proposed framework with other frameworks

Year and author/ founder	Framework proposed	Methodology/ parameters	Results
Center for internet security (CIS), 2000 [127]	CIS security framework	20 CIS controls (basic, foundational, organizational)	Evaluation based on questionnaires (CIS controls self-assessment tool, or CIS CSAT)
US national institute of standards and technology, 2014 [126]	NIST cybersecurity framework	Identify, protect, detect, respond, recover	Evaluation based on a self-assessment questionnaire
Chan et al., 2017 [125]	Conceptual framework to federate testbeds for cybersecurity	Cross-domain interoperability, elasticity via distributed control, rule-based semantics for interdependency modeling, unified view and control	The framework has not been evaluated by the authors
Powell et al., 2019 [128]	Distributed Energy Resources Cybersecurity Framework	Governance, Cyber-Physical Technical Management, Physical Security	The framework has not been evaluated by the authors
Ilhan and Karaköse, 2019	Cybersecurity framework for industry 4.0	Standards of systems (safety / compliance), industrial control system, network communication (safety / compliance), system inventory record, operations of systems and management (safety / compliance), monitoring and testing	The framework has not been evaluated by the authors
Our proposed framework, 2020	Cybersecurity framework for medical cyber physical systems (MCPS)	Identification model, defense model, diagnosing model, response model, recuperation model, trust model, threat model, risk model	Highlights more security issues threat model and trust model interaction between components evaluation based on qualitative assessment

attacks are detected after two hundred days on an average [141]. Hence there is a need to upgrade the cybersecurity frameworks and systems continuously.

4 Conclusions

In this paper, we have contemplated the growing MCPS technology in the healthcare industry with the general overview of MCPS, classification, benefits, challenges and security issues of the same. A comparative survey has been carried out pertaining to the security issues and prospects for MCPSs over the last few decades (1998–2017). Based on the background study and a comprehensive comparative analysis of the existing literature that has been conducted, we have summarized the advantages and limitations of the existing research that has been done in this area. We proposed a new framework considering both the security/privacy and scheduling mechanism. Bearing in mind the discussed security issues, we have proposed a more concrete method to ensure MCPS security in the form of a cyber security framework based on several securities associated models. It is useful to deploy efficient workflow operations for patients under the considered framework.

The propelled utilization of innovation in medical devices has enhanced the way social insurance is conveyed to patients. Tragically, the expanded unpredictability of medicinal devices poses serious challenges for improvement, affirmation, and administrative endorsement. With an end goal of enhancing the wellbeing of cutting-edge therapeutic devices, organizations such as the FDA have supported the development and investigation of methods to help in the advancement and administrative endorsement of such frameworks. Restorative determination is continuously being developed and upgraded to understand driven counteractive action, forecast, and treatments. Significant developments have been made in recent years in the study and handling of big data, and the advent of data analytics, and both of these will be of great use in the development of MCPS.

The framework has been proposed keeping in mind the various types of security issues that crop up in MCPS. The issues described in Sect. 2.5 may eventually get classified into a model, and necessary steps may be taken to avert it. Several models may be necessary to evade security issues. For instance, Ransomware finds a place in Identification Model, Defense Model, Response Model, Recuperation Model, Threat Model and Risk Model. Orangeworm risk deals with Identification Model, Defense Model, Response Model and Risk Model. Depending on the severity of the situation, one or more techniques may be applied. All the appropriate methodologies falling under these individual models may be applied to protect against Ransomware or Orangeworm.

Since the proposed framework addresses the concerns mentioned above via individual models, more security risks are likely to be covered by the framework, thus strengthening the security infrastructure for these systems. Security breaches know no bound, and malwares are scripted on a daily basis. Several security issues that are related to the ones mentioned in Sect. 2.5 may arise in future. Based on the framework, we have developed the interactive model which ensures transparency by valuing the trust model. MCPS are responsible for performing sensitive tasks which are necessary to ensure accountability. The downside of the framework is that several parameters might have to be considered based on the severity of the issue, the kind of sphere it deals with, etc. There might be an advanced security issue in the future that none of the models in the framework might be capable of averting.

The future work in this area is pertaining to the development of a robust cyber-security system that will provide maximum and comprehensive security coverage to protect the privacy of patients' data in cyberspace. Other areas to work in the near future will be the study of other challenges such as interoperability and administrative difficulties that still pose threats to MCPS [91]. Further, the study and development of advanced data and communication scheduling algorithms based on machine learning [3, 92–124] is our focus.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s00450-021-00427-3.

Funding This research has no funding source.

Compliance with ethical standards

Conflict of interest Authors declare that there is no conflict of interest about the research.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. Lee I, Sokolsky O (2010) Medical cyber physical systems. In: Design automation conference (DAC) 2010, 743–748.
2. Lee I, Sokolsky O, Chen S, Hatcliff J, Jee E, Kim B, Venkatasubramanian KK (2012) Challenges and research directions in medical cyber–physical systems. In: Proceedings of the IEEE 100(1):75–90.
3. Norman G (2016) Drugs and devices: comparison of European and U.S. Approval Processes. JACC 1(5)*:* 399–412. https://doi.org/10.1016/j.jacbts.2016.06.003.
4. Dey N, Ashour AS, Shi F, Fong SJ, Tavares JMR (2018) Medical cyber-physical systems: a survey. J Med Syst 42(4):74

5. Haque SA, Aziz SM, Rahman M (2014) Review of cyber-physical system in healthcare. Int J Distrib Sens Netw 10(4):217–415
6. Williams PA, Woodward AJ (2015) Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices (Auckland, NZ) 9:305
7. Baheti R, Gill H Cyber physical systems. In: IEEE Control Systems Society 2011, 1–6. www.ieeecss.org.
8. Denning T, Fu K, Kohno T (2008) Absence makes the heart grow fonder: new directions for implantable medical device security. In: HotSec 2008
9. Ferguson N, Schneier B, Kohno T (2010) Cryptography engineering: design principles and practical applications. John Wiley & Sons 2010.
10. Halperin D, Heydt-Benjamin TS, Fu K, Kohno T, Maisel WH (2008) Security and privacy for implantable medical devices. IEEE Pervasive Comput 7(1):29–39
11. Lin C, Zeadally S, Chen T, Chang C (2012) Enabling cyber physical systems with wireless sensor networking technologies. Int J Distributed Sensor Netw 1–21, https://doi.org/10.1155/2012/489794.
12. Guerrero-Higueras ÁM, DeCastro-García N, Rodríguez-Lera FJ, Matellán V (2017) Empirical analysis of cyber-attacks to an indoor real time localization system for autonomous robots. Comput Security 70:422–435
13. Mazoit JX, Butscher K, Samii K (2007) Morphine in postoperative patients: pharmacokinetics and pharmacodynamics of metabolites. Anesth Analg 105(7):70–78
14. Hicks RW, Sikirica V, Nelson W, Schein JR, Cousins DD (2008) Medication errors involving patient-controlled analgesia. Am J Health Syst Pharm 65(5):429–440
15. Happ MB (1998) Treatment interference in acutely and critically ill adults. Am J Crit Care 7(3):224
16. Jin Z, Oresko J, Huang S, Cheng AC (2009) HeartToGo: a personalized medicine technology for cardiovascular disease prevention and detection. In: Life science systems and applications workshop, 2009. LiSSA 2009. IEEE/NIH, 80–8
17. Sung M, Marci C, Pentland A (2005) Wearable feedback systems for rehabilitation. J Neuroeng Rehabil 2(1):17
18. Di Rienzo M, Rizzo F, Parati G, Brambilla G, Ferratini M, Castiglioni P (2005) MagIC system: a new textile-based wearable device for biological signal monitoring. applicability in daily life and clinical setting. In: Engineering in medicine and biology society, 2005. IEEE-EMBS 2005. 27th Annual International Conference, 7167–7169.
19. Wood A, Virone G, Doan T, Cao Q, Selavo L, Wu Y, Stankovic J (2006) ALARM-NET: wireless sensor networks for assisted-living and residential monitoring. Univ Virginia Comput Sci Dept Tech Rep 2:17
20. Mundt CW, Montgomery KN, Udoh UE, Barker VN, Thonier GC, Tellier AM, Ruoss SJ (2005) A multiparameter wearable physiologic monitoring system for space and terrestrial applications. IEEE Trans Inf Technol Biomed 9(3):382–391
21. Hughes J, Cybenko G (2014) Three tenets for secure cyber-physical system design and assessment. Cyber Sens Int Soc Opt Photonics 9(7):909–970
22. Penna R, Amaral M, Espíndola D, Botelho S, Duarte N, Pereira CE, Frazzon EM (2014) Visualization tool for cyber-physical maintenance systems. In: Industrial informatics (INDIN), 2014 12th IEEE international conference, July IEEE, 566–571.
23. Larson BR et al. (2013) Open patient-controlled analgesia infusion pump system requirements. Int Workshop Softw Eng Health Care 28–34 https://doi.org/10.1109/SEHC.2013.6602474.
24. Hahanov V, Gharibi W, Kudin AP, Hahanov I, Cristopher N, Yeve T, Priymak A (2014) Cyber physical social systems-future of Ukraine. In Design & Test Symposium (EWDTS) September, IEEE, 1–15.
25. Zhang L (2014) Designing big data driven cyber physical systems based on AADL. In: Systems, man and cybernetics (SMC), 2014 IEEE international conference, October, 3072–3077.
26. O'Keeffe DT, Maraka S, Basu A, Keith-Hynes P, Kudva YC (2015) Cybersecurity in artificial pancreas experiments. Diabetes Technol Ther 17(9):664–666
27. Ray A, Cleaveland R (2015) Security assurance cases for medical cyber-physical systems. IEEE Design Test 32(5):56–65
28. Sabău-Popa D, Bradea I, Boloș M, Delcea C (2015) The information confidentiality and cybersecurity in medical institutions. The Annals of the University of Oradea, 855.
29. Ivanov R, Weimer J, Lee I (2018) Context-aware detection in medical cyber-physical systems. In: Proceedings of the 9th ACM/IEEE international conference on cyber-physical systems, April, IEEE Press, 232–241.
30. Dogaru DI, Dumitrache I (2015) Cyber-physical systems in healthcare networks. In: E-health and bioengineering conference (EHB), November, IEEE, 1–4.
31. Reddy YB (2015) Security and design challenges in cyber-physical systems. In: Information technology-new generations (ITNG), 2015 12th international conference, April, IEEE, 200–205.
32. Quadri I, Bagnato A, Brosse E, Sadovykh A (2015) Modeling methodologies for cyber-physical systems: research field study on inherent and future challenges. ADA USER 36(4):246
33. Kanjee MR, Liu H (2016) Authentication and key relay in medical cyber-physical systems. Security Commun Netw 9(9):874–885
34. Chen S, Sokolsky O, Weimer J, Lee I (2016) Data-driven adaptive safety monitoring using virtual subjects in medical cyber-physical systems: a glucose control case study. J Comput Sci Eng 10(3):75
35. Majhi SK, Patra G, Dhal SK (2016) Cyber physical systems & public utility in India: state of art. Proc Comput Sci 78:777–781
36. Kruse CS, Frederick B, Jacobson T, Monticone DK (2017) Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care 25(1):1–10
37. Meng W, Li W, Xiang Y, Choo KKR (2017) A Bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks. J Netw Comput Appl 78:162–169
38. Bricon-Souf N, Newman C (2007) Context awareness in health care: a review. Int J Med Inform 76(1):2–12
39. Gu L, Zeng D, Guo S, Barnawi A, Xiang Y (2017) Cost efficient resource management in fog computing supported medical cyber-physical system. IEEE Trans Emerging Topics Comput 5(1):108–119
40. García-Valls M, Herrasti N, Jouvray C, Armentia A (2017) Flexible and timely on-line integration of medical services using iLand middleware. ACM Sigbed Rev 14(2):53–60
41. Pawlick J, Zhu Q (2017) Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control. IEEE Trans Inf Forensics Secur 12(12):2906–2919
42. Cecil J (2017) Internet of things (IoT)-based cyber–physical frameworks for advanced manufacturing and medicine. Internet of Things and Data Analytics Handbook, 545–561.
43. Nithya S, Sangeetha M, Prethi KA (2018) Role of cyber physical systems in health care and survey on security of medical data. Int J Pharma Res Health Sci 6(1):75–80
44. Nissim N, Mahler T, Shalom E, Goldenberg I, Hasman G, Makori A, Shahar Y (2018) Know your enemy: characteristics of cyber-attacks on medical imaging devices arXiv preprint arXiv:1801.05583.
45. Croasdell D, Elste J, Hill A (2018) Cyber clinics: re-imagining cybersecurity awareness. In: Proceedings of the 51st Hawaii international conference on system sciences, 4283–4288.

46. Li GC, Chen CL, Chen HC, Lin F, Gu C (2018) Design of a secure and effective medical cyber-physical system for ubiquitous telemonitoring pregnancy. Concurrency Comput 30(2):52–61
47. Malathi S, Priadarsini M, Dharshana M, Agathiya T (2018) Big data and CPS (Cyber Physical System) used in pharmacy to alert on expiration of medicine. Int J Eng Sci, 16946.
48. Ivanov R, Weimer J, Simpao A, Rehman M, Lee I (2015) Early detection of critical pulmonary shunts in infants. In: Proceedings of the ACM/IEEE sixth international conference on cyber-physical systems, April, ACM, 110–119.
49. Rushanan M, Rubin AD, Kune DF, Swanson CM (2014) SoK: security and privacy in implantable medical devices and body area networks. In: Security and privacy (SP), 2014 IEEE symposium IEEE. 524–539.
50. Gunes V, Peter S, Givargis T, Vahid F (2014) A survey on concepts, applications, and challenges in cyber-physical systems. KSII Trans Internet Inform Syst 8(12):4242–4268
51. Finnegan A, McCaffery F (2014) A security argument pattern for medical device assurance cases. In: Software reliability engineering workshops (ISSREW), 2014 IEEE international symposium, IEEE, pp 220–225.
52. Sametinger J, Rozenblit J, Lysecky R, Ott P (2015) Security challenges for medical devices. Commun ACM 58(4):74–82
53. AlTawy R, Youssef AM (2016) Security tradeoffs in cyber physical systems: a case study survey on implantable medical devices. IEEE Access 4:959–979
54. Mashkoor A, Sametinger J (2016) Rigorous modeling and analysis of interoperable medical devices. In: Proceedings of the modeling and simulation in medicine symposium, society for computer simulation international, 5.
55. Kocabas O, Soyata T, Aktas MK (2016) Emerging security mechanisms for medical cyber physical systems. IEEE/ACM Trans Comput Biol Bioinf 13(3):401–416
56. Mackey TK, Nayyar G (2016) Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies. Br Med Bull 118(1):110–126
57. He H, Maple C, Watson T, Tiwari A, Mehnen J, Jin Y, Gabrys B (2016) The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In: Evolutionary computation (CEC), 2016 IEEE congress IEEE, 1015–1021.
58. Carroll N, Richardson I (2016) Software-as-a-medical device: demystifying connected health regulations. J Syst Inform Technol 18(2):186–215
59. Mohan A (2014) Cybersecurity for personal medical devices internet of things. In: Distributed computing in sensor systems (DCOSS), 2014 IEEE international conference, IEEE, 372–374.
60. Arney D, Plourde J, Schrenker R, Mattegunta P, Whitehead SF, Goldman JM (2014) Design pillars for medical cyber-physical system middleware. In: OASIcs-OpenAccess Series in Informatics, SchlossDagstuhl-Leibniz-ZentrumfuerInformatik, 36:124–132.
61. Adyanthaya S, Ara HA, Bastos J, Behrouzian A, Sánchez RM, Van Pinxten J, Frijns R (2017) xCPS: a tool to explore cyber physical systems. ACM SIGBED Rev 14(1):81–95
62. Arney D, Venkatasubramanian KK, Sokolsky O, Lee I (2011) Biomedical devices and systems security. In: Engineering in medicine and biology society, EMBC, 2011 annual international conference of the IEEE, August, IEEE, 2376–2379.
63. Burns AJ, Johnson ME, Honeyman P (2016) A brief chronology of medical device security. Commun ACM 59(10):66–72
64. Celdrán AH, Pérez G, Clemente FJG, Pérez GM (2018) Sustainable securing of medical cyber-physical systems for the healthcare of the future. Sustain Comput 19:138–146
65. Grispos G, Glisson WB, Choo KKR (2017) Medical cyber-physical systems development: a forensics-driven approach. In: Connected health: applications, systems and engineering technologies (CHASE), 2017 IEEE/ACM international conference IEEE, 108–113.
66. Heartfield R, Loukas G, Budimir S, Bezemskij A, Fontaine JR, Filippoupolitis A, Roesch E (2018) A taxonomy of cyber-physical threats and impact in the smart home. Comput Security 78:398–428
67. Li W, Meng W, Su C, Kwok LF (2018) Towards false alarm reduction using fuzzy if-then rules for medical cyber physical systems. IEEE Access 6:6530–6539
68. Lyapustina S, Armstrong K (2018) Regulatory considerations for cybersecurity and data privacy in digital health and medical applications and products. CSC Publishing, 1–8.
69. Mahler T et al. (2018) Know your enemy: characteristics of cyber-attacks on medical imaging devices. Cornell University Library **2018**, 1–6.
70. Hanacek N (2018) NIST cybersecurity framework. https://www.nist.gov/cyberframework
71. Zheng G et al (2017) Ideas and challenges for securing wireless implantable medical devices: a review. IEEE Sens J 17(3):562–576
72. Tyagi A (2016) Cyber physical systems (CPSs)—opportunities and challenges for improving cyber security. Int J Comput Appl 137(14):19–27
73. Jahanian F (2011) The growing imperative and transformative impact of cyber-physical systems. Natl Sci Foundation, 1–53.
74. Wang E et.al. (2010) Security issues and challenges for cyber physical system. In: 2010 International conference on green computing and communications physical and social computing, IEEE/ACM, 733–738.
75. Ofori A, Abdulai J, Katsriku F (2018) Cybercrime and risks for cyber physical systems: a review 1–26, https://doi.org/10.20944/preprints201804.0066.v1.
76. Corpuz M (2010) Limitations of the information security management system assessment approaches in the context of information security policy assessment. Information Security Institute, Queensland University of Technology, 1–3
77. Haufe K, Palacios R, Dzombeta S, Brandis K, Stantchev V (2016) A process framework for information security management. Int J Inform Syst Project Manag, 27–47.
78. Copeland JB Implementing NIST CSF? read this first Retrieved June 19, 2017, from https://www.fairinstitute.org/blog/implementing-nist-csf-read-this-first.
79. Hoyme K, Abrahamson S, Englert P (2017) Medical device risk management and assessment methods. Healthcare Information and Management Systems Society (HIMSS), 1–56.
80. Bradley M (2018) Five typical cyber attack techniques used against business travelers, Retrieved July 23, 2018, From https://www.securitymagazine.com/articles/89255-five-typical-cyber-attack-techniques-used-against-business-travelers
81. Ashford W (2019) Orangeworm cyber attack group targets health sector, Retrieved Jan 2019, From https://www.computerweekly.com/news/252439782/Orangeworm-cyber-attack-group-targeting-health-sector
82. Bezemskij A, Loukas G, Anthony RJ, Gan D (2016) Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle. In: 2016 15th international conference on ubiquitous computing and communications and 2016 international symposium on cyberspace and security (IUCC-CSS), 61–68.
83. Priyadarshini I (2017) Cybersecurity risks in robotics, detecting and mitigating robotic cyber security risks. IGI Global

84. Kruegel C, Vigna G (2003) Anomaly detection of web-based attacks. In: Proceedings of the 10th ACM conference on computer and communications security ACM, 251–261.
85. Goud N (2019) Healthcare alert- Medical devices are more prone to cyber attacks, Retrieved Jan 24, 2019, From https://www.cybersecurity-insiders.com/healthcare-alert-medical-devices-are-more-prone-to-cyber-attacks/
86. Palmer D (2018) What is ransomware? Everything you need to know about one of the biggest menaces on the web, Retrieved August 22, 2018, From https://Www.Zdnet.Com/Article/Ransomware-An-Executive-Guide-To-One-Of-The-Biggest-Menaces-On-The-Web/
87. Voss S (2018) Could you recover from a destructive cyber-attack?—Dell Technologies. Retrieved July 30, 2018, from https://www.delltechnologies.com/en-us/perspectives/could-you-recover-from-a-destructive-cyber-attack
88. Fisher N (2018) 5 identity attacks that exploit your broken authentication, Retrieved March 14, 2018, from https://www.okta.com/security-blog/2018/03/5-identity-attacks-that-exploit-your-broken-authentication/
89. McConnachie L (2018) 10 cyber security threats in 2017 that you can't just ignore [How Vulnerable Are You?]", Retrieved August 27, 2018, from https://purplegriffon.com/blog/10-cyber-security-threats-in-2017.
90. NeSmith B (2018) Avoid These Top Five Cyberattacks, Retrieved May 4, 2018, from https://www.forbes.com/sites/forbestechcouncil/2018/05/04/avoid-these-top-five-cyberattacks/#21265d6c7cc9
91. Ashibani Y, Mahmoud QH (2017) Cyber physical systems security: analysis, challenges and solutions. Comput Security 68:81–97
92. Ali M, Son LH, Khan M, Tung NT (2018) Segmentation of dental X-ray images in medical imaging using neutrosophic orthogonal matrices. Expert Syst Appl 91:434–441
93. Ali M, Son LH, Thanh ND, Van Minh N (2018) A neutrosophic recommender system for medical diagnosis based on algebraic neutrosophic measures. Appl Soft Comput 71:1054–1071
94. Anand M, Cronin E, Sherr M, Blaze M, Ives Z, Lee I (2006) Security challenges in next generation cyber physical systems. Beyond SCADA: Networked Embedded Control for Cyber Physical Systems. 41
95. Haque SA, Aziz SM, Rahman M (2014) Review of cyber-physical system in healthcare. Int J Distrib Sens Netw 10(4):217415
96. Hemanth DJ, Anitha J, Son LH, Mittal M (2018) Diabetic retinopathy diagnosis from retinal images using modified hopfield neural network. J Med Syst 42(12):247
97. Jersey C (2016) ThreatModeler redefines threat modeling by allowing non-security experts to build threat models in minutes, Retrieved July 13, 2016, from https://www.prweb.com/releases/2016/07/prweb13546377.htm.
98. Lee I, Sokolsky O (2010) Medical cyber physical systems. In: Design automation conference (DAC), 2010 47th ACM/IEEE, IEEE, 743–748.
99. Lee I et al (2012) Challenges and research directions in medical cyber–physical systems. Proc IEEE 100(1):75–90
100. Meyer D, Haase J, Eckert M, Klauer B (2016) A threat-model for building and home automation. In: IEEE 14th international conference on industrial informatics (INDIN), 860–866. https://doi.org/10.1109/INDIN.2016.7819280.
101. Ngan RT, Ali M, Son LH (2018) δ-equality of intuitionistic fuzzy sets: a new proximity measure and applications in medical diagnosis. Appl Intell 48(2):499–525
102. Ngan RT, Cuong BC, Tuan TM, Son LH (2018) Medical diagnosis from images with intuitionistic fuzzy distance measures. In: International joint conference on rough sets **2018**, Springer, Cham, 479–490.
103. Ngan TT, Tuan TM, Son LH, Minh NH, Dey N (2016) Decision making based on fuzzy aggregation operators for medical diagnosis from dental X-ray images. J Med Syst 40(12):280
104. Son LH, Phong PH (2016) On the performance evaluation of intuitionistic vector similarity measures for medical diagnosis. J Intell Fuzzy Syst 31(3):1597–1608
105. Son LH, Tuan TM, Fujita H, Dey N, Ashour AS, Ngoc VTN, Chu DT (2018) Dental diagnosis from X-ray images: an expert system based on fuzzy computing. Biomed Signal Process Control 39:64–73
106. Son LH, Thong NT (2015) Intuitionistic fuzzy recommender systems: an effective tool for medical diagnosis. Knowl-Based Syst 74:133–150
107. Son LH, Tuan TM (2016) A cooperative semi-supervised fuzzy clustering framework for dental X-ray image segmentation. Expert Syst Appl 46:380–393
108. Son LH, Tuan TM (2017) Dental segmentation from X-ray images using semi-supervised fuzzy clustering with spatial constraints. Eng Appl Artif Intell 59:186–195
109. Stevens M (2017) Cybersecurity risk: a thorough definition, Retrieved January 10, 2017, from https://www.bitsighttech.com/blog/cybersecurity-risk-thorough-definition.
110. Thanh ND, Ali M, Son LH (2017) A novel clustering algorithm in a neutrosophic recommender system for medical diagnosis. Cognit Comput 9(4):526–544
111. Thanh ND, Son LH, Ali M (2017) Neutrosophic recommender system for medical diagnosis based on algebraic similarity measure and clustering. In: Fuzzy systems (FUZZ-IEEE), 2017 IEEE international conference July, IEEE, 1–6.
112. The European Union Agency for Network and Information Security (ENISA), Risk Management, ISMS Cybersecurity Framework, Retrieved November 20, 2009, from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework.
113. Thong NT, Son LH (2015) HIFCF: An effective hybrid model between picture fuzzy clustering and intuitionistic fuzzy recommender systems for medical diagnosis. Expert Syst Appl 42(7):3682–3701
114. Tuan TM, Ngan TT, Son LH (2016) A novel semi-supervised fuzzy clustering method based on interactive fuzzy satisficing for dental X-ray image segmentation. Appl Intell 45(2):402–428
115. Tuan TM, Duc NT, Van Hai P, Son LH (2017) Dental diagnosis from X-Ray images using fuzzy rule-based systems. Int J Fuzzy Syst Appl (IJFSA) 6(1):1–16
116. Thanh ND, Ali M, Son LH (2017) A novel clustering algorithm in a neutrosophic recommender system for medical diagnosis. Cogn Comput 9:526–544
117. Venkatasubramanian KK, Gupta SKS, Jetley RP, Jones PL (2010) Interoperable medical devices. IEEE Pulse 1(2):16–27
118. Doss S, Nayyar A, Suseendran G, Tanwar S, Khanna A, Thong PH (2018) APD-JFAD: accurate prevention and detection of jelly fish attack in MANET. IEEE Access 6:56954–56965
119. Gonzalez E, Pena R, Avila A, Rosales C, Rodrigues D (2017) A systematic review on recent advances in health systems: deployment architecture for emergency response. J Healthcare Eng 20(17):13–21
120. Fink G, Edgar T, Rice T, MacDonald D, Crawford C (2017) Security and privacy in cyber-physical systems, Foundations, Principles and Applications Intelligent Data-Centric Systems, 129–141.
121. Su L, Ye D (2018) A cooperative detection and compensation mechanism against denial-of-service attack for cyber-physical systems. Inf Sci 444:122–134

122. Lee I, Sokolsky O, Chen S, Hatcliff J, Jee E (2012) Challenges and research directions in medical cyber-physical systems, 2012. Proc IEEE 100(1):75–90
123. Priyadarshini I, Cotton C (2018) Features and architecture of modern cyber range: a qualitative analysis and survey, University of Delaware**.**
124. Priyadarshini I, Cotton C (2019) Some cyber psychological techniques to distinguish human and robot authentication. Advances in Intelligent Systems, Springer.
125. Ramapantulu L, Teo YM, Chang EC (2017). A conceptual framework to federate testbeds for cybersecurity. In: 2017 winter simulation conference (WSC) (pp 457–468). IEEE.
126. Shen L (2014) The NIST cybersecurity framework: overview and potential impacts. Scitech Lawyer 10(4):16
127. Gonzalez CP, Hunting B, Burgess J, Jensen LH CIS critical security controls.
128. Powell C, Hauck K, Sanghvi AD, Hasandka A, Van Natta J, Reynolds TL (2019). Guide to the distributed energy resources cybersecurity framework (No. NREL/TP-5R00–75044). National Renewable Energy Lab (NREL), Golden, CO (United States).
129. Ilhan I, Karaköse M (2019) Cybersecurity framework for requirements of repair, update, and renovation in industry 4.0. In: 2019 1st international informatics and software engineering conference (UBMYK) (pp 1–4). IEEE.
130. Min D (2013) Medical cyber physical systems and bigdata platforms.
131. Qiu H, Qiu M, Liu M, Memmi G (2019) Privacy-preserving health data sharing for medical cyber-physical systems. arXiv preprint arXiv: 1904.08270.
132. Jimenez JI, Jahankhani H, Kendzierskyj S (2020) Health care in the cyberspace: medical cyber-physical system and digital twin challenges. In: Digital twin technologies and smart cities (pp 79–92). Springer, Cham.
133. Haidegger T, Virk GS, Herman C, Bostelman R, Galambos P, Györök G, Rudas IJ (2020) Industrial and medical cyber-physical systems: Tackling user requirements and challenges in robotics. In: Recent advances in intelligent engineering (pp 253–277). Springer, Cham.
134. Shishvan OR, Zois DS, Soyata T (2020) Incorporating artificial intelligence into medical cyber physical systems: a survey. In: Connected Health in Smart Cities (pp 153–178). Springer, Cham.
135. Zhao S, Rengasamy PV, Zhang H, Bhuyan S, Nachiappan NC, Sivasubramaniam A, ... Das C (2019). Understanding energy efficiency in iot app executions. In: 2019 IEEE 39th international conference on distributed computing systems (ICDCS) (pp 742–755). IEEE.
136. Martín-Lopo MM, Boal J, Sánchez-Miralles Á (2020) A literature review of iot energy platforms aimed at end users. Computer Networks, 107101.
137. Ueki M, Takeuchi K, Yamamoto T, Tanabe A, Ikarashi N, Saitoh M, ... Masuzaki K (2015) Low-power embedded ReRAM technology for IoT applications. In: 2015 symposium on VLSI technology (VLSI Technology) (pp T108–T109). IEEE.
138. Mohammad K, Tekeste T, Mohammad B, Saleh H, Qurran M (2019) Embedded memory options for ultra-low power IoT devices. Microelectron J 93:104634
139. Zali Z, Hashemi MR, Saidi H (2012) Real-time attack scenario detection via intrusion detection alert correlation. In: 2012 9th international ISC conference on information security and cryptology (pp 95–102). IEEE.
140. Clotet X, Moyano J, León G (2018) A real-time anomaly-based ids for cyber-attack detection at the industrial process level of critical infrastructures. Int J Crit Infrastruct Prot 23:11–20
141. Irwin, L. (2019, December 17). How long does it take to detect a cyber attack? Retrieved from https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack