

Cloud computing security in health cyber physical systems

Mamoqenelo P. Morolong *

Fungai Bhunu Shava [†]

Attlee M. Gamundani [§]

Namibia University of Science and Technology

Faculty of Computing and Informatics

Department of Computer Science

Windhoek 9000

Namibia

Abstract

The health industry as one of the Critical Infrastructures has rapidly grown in adopting the use of new ubiquitous technologies in advancing its critical services. The industry because of its high need and usage of new technologies is encountering a myriad of challenges including cyber-attacks. Among the technologies adopted by the health industry is the use of cloud computing services for managing Electronic Medical Records (EMR) on the cloud environment. Today's medical devices use sensors that collect data from the diverse environments such as the human heart and such data is sent to the cloud for better analysis, monitoring, or management. However, attackers exploit every single development to advance health or medical services like all the other cyber systems. The scope of this paper is to investigate how cloud computing services adopted in Health Cyber Physical Systems can be secured from the prevalent cybersecurity challenges. The study followed a systematic literature review, where data was collected from online databases with set search constraints such as language, date of publication and specific keywords. This paper presents how cloud computing integrated with the medical cyber physical systems can impeccably securely manage the health systems. More specifically the collection, monitoring, and management of real-time data and as a result of this integration, different cyber-attacks are escalating.

Subject Classification: 68M99.

Keywords: Cloud computing, Cyber security, Cyber physical systems, Health cyber physical systems.

* E-mail: mamqeny10@gmail.com (Corresponding Author)

[†] E-mail: fbshava@nust.na

[§] E-mail: agamundani@nust.na

1. Introduction

The health care sector most often called the “Medical care sector” is one of the sectors that have intensively adopted new technologies into the working environment. A diverse number of new technologies such as Artificial Intelligence, the Internet of Things (IoT) technologies, Cloud Computing, Mobile computing, and others have infiltrated the health care sector with the aim of improving services. As one of the critical services providers, health care needs to protect, enhance, optimize, and secure their services. The health care sector has adopted the use of the cyber physical systems supported by cloud computing to harmoniously achieve its mandate. A lot of research has been conducted demonstrating the implementation and interoperation of the cloud computing in health cyber physical systems [1]. This interoperation is claimed to have proliferated service delivery of the health care industry. Collection of real-time data and processing is required for decision making. Research has been done on cloud computing; cyber physical systems and more specifically on electronic medical or health cyber physical systems; cloud computing security and cyber physical systems security, however, limited research is conducted on the cyber security of cloud computing in health Cyber Physical Systems (CPS)..

It is important to highlight some of the important keywords that will be used in this chapter.

Cyber-security is the general term used to describe the protection of services, cyber-physical infrastructure, communication networks and or people from the cyber-attacks.

Cloud Computing is the term used to define services that make use of the cloud, an interconnected set of remote servers residing on the Internet to process, manipulate, store, distribute, and manage data. IT is referred to as a complex interconnection of on-demand computer systems resources with data storage, computational power, IT resources as services over the internet and software. Examples include Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and Software-as-a-Service (SaaS). Cyber physical systems support both PaaS and IaaS architectures [2].

Cyber physical systems “are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core” [1][3].

1.1 Objectives:

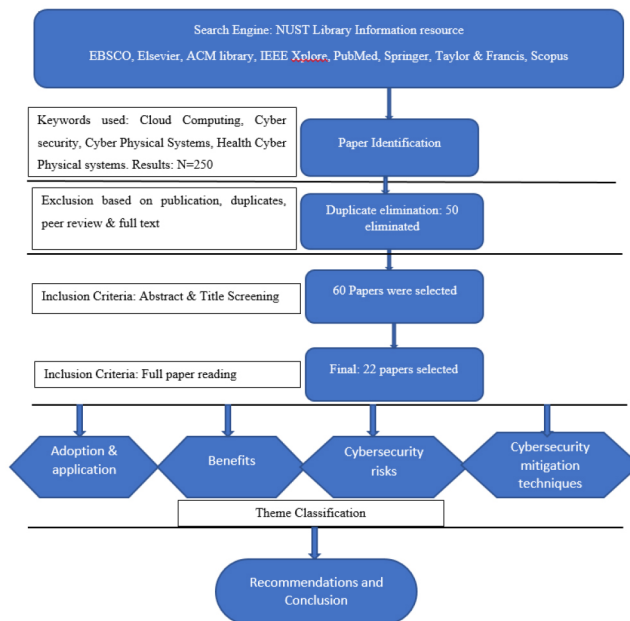
This paper aims to present an assessment of the cyber-security in cloud computing in the health cyber physical systems. To achieve this, the following key aspects are the sub-research objectives:

1. To identify the cyber physical systems for health care service delivery;
2. To investigate the adoption and the application of cloud computing in health care;
3. To investigate the benefits and challenges of cloud computing in health cyber physical systems, and;
4. To analyse the cyber security risks associated with cloud computing adoption in health cyber physical systems.
5. Investigate the cyber security mitigations techniques and tools for cloud computing attacks in cyber physical systems

The paper follows this organisation: section 2 discusses the research methodology, followed by assessing the cloud computing security in the health care cyber infrastructures, then section 3 discusses the adoption and Cloud computing adoption in Health care, benefits, and challenges of cloud computing in Health cyber physical systems follows in section 4. Section 5 looks at the cyber security risks of cloud computing in Health cyber physical systems and the mitigation processes and finally the recommendations and conclusion.

2. Methodology

To attain the objectives of this paper, a systematic literature review was followed. According to [4] A systematic review is an *“evidence-based literature review which goes beyond an ordinary review in rigorously assessing the quality of the literature using methods approved by the body of academic opinion. Systematic Review was used because it is a highly approved academic scoping method within public health in the United Kingdom and abroad”*. In this study we used NUST Library Information Resources as our main database search as it links with more online databases such as Emerald, Scopus, Science Direct, Elsevier, Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), and SAGE, Academic Source Premier, Cambridge Books, Clinical Pharmacology, Ebsco E-books Collection, Health Source: Consumer Edition, Health

**Figure 1****Methodical framework followed**

Source: Nursing/Academic Edition, JSTOR, ProQuest, Springer and Taylor & Francis among others. From the advanced search on NUST Library Information Resources, we parsed the following search strings: ("Cybersecurity*" Or "Cloud Computing") AND ("Cyber Physical Systems*") AND ("Medical*" OR "Health*").

More constraints that include: "Full text" and "Peer reviewed", Dated 2010 – 2022 and English as the preferred language we added. Journal articles, conference proceedings and books were also added to the search string. Elimination of duplicates from the outcome was also performed by checking the titles of the articles. The focus was on papers that were core on cloud computing, cyber physical systems, and cybersecurity. The methodical framework used in this research is shown in Figure 1.

3. Adoption and application of Cloud computing in Health care

The health care sector for a long period especially within the least developed countries has been using the on-premises infrastructure for most of its operations and advanced to Electronic Medical Records (EMR) systems with technology evolutions, however, from 2020 due to the

Covid-19 outbreak, that notion changed. The health care sector is now adopting cloud services for timely service delivery [5]. The Covid-19 pandemic has pushed most of the companies to shift from their normal ways of doing things, hence the health care sector has also adapted to the radical change. This change has been seen from communication; data capturing, processing, and storage; and Doctor to patient relationships.

Cloud computing has successfully integrated various applications ranging from remote processing and storage, big data analytics, on-demand data centres, virtualization of resources and offering various services to end-users; this is made possible by the fact that cloud computing is a distributed system for large scale data processing. In fact, cloud computing emergence is a result of substantial evolution of high-speed networks, together with wide-spread of Service-Oriented Architecture (SOA). SOA enables provision of resources for Machine-to-Machine (M2M) interaction as alluded by [6].

Due to its cost effectiveness, cloud computing is fostering collection of real-time data, storage of data and exchange between medical care organizations [7]. As health care sector is advancing from the traditional way of doing things (paper based) to the more advanced method of using EMR, cloud computing is proven to be cost effective in this regard. Some of the Electronic health services areas include telemedicine services, health information system, personal health record, and EMR and electronic health record. The management of volumes of data from the EMRs is made seamless by cloud computing. As opined by [5] in the health-care sector, the major reason of using Cloud computing is to offer E-health cloud services which range from:

- A. SaaS: On this upper layer, most application software that the user needs from the cloud are run. The end-users or customers have access to myriad of software they have subscribed to using a web browser or an application programming interface (API). The beauty of this service especially to health sector is that, end-users need not worry about any software upgrades and maintenance [8], examples include Clinical Information Systems.
- B. PaaS: Offers applications implemented on the cloud with operative system support [5].
- C. IaaS: This is the layer that provides infrastructure and operating systems for companies that do not have enough capital to secure hardware. It is one of the beneficial services in the context of least

developed countries as they do not need to invest much on hardware. Customers pay according to how much they consume [8].

- D. DSaaS: is a lower layer, this is one of the services that provides storage. It is beneficial for companies that do not have enough muscle to host massive volumes of data on their physical and limited storage [5].

In their research paper, [9] interrogated the cloud computing application in health information systems and pointed out the following applications:

- I. Healthcare information system as a Service
- II. Telemedicine as a Service
- III. Personal Health Record (PHR) as a Service
- IV. Clinical Decision Support System (CDSS) as a Service
- V. Biological SaaS

As indicated by [7] there are a couple of applications of Cloud computing in health care including: 1) Emergency Medical Services (EMS) which when integrated with cloud computing enables retrieval of data from EMR. 2) Emergency Personal Healthcare Record (EPHR) which provides paramedics access to continuously required and updated data from different sources. The other application is discussed in section 3.1.

3.1 Wireless Body Sensor networks (WBAN)

As harangued by [7], the use of Body Sensor Networks (BSN) forms part of the WBAN as demonstrated in Figure 2. The BSN consists of

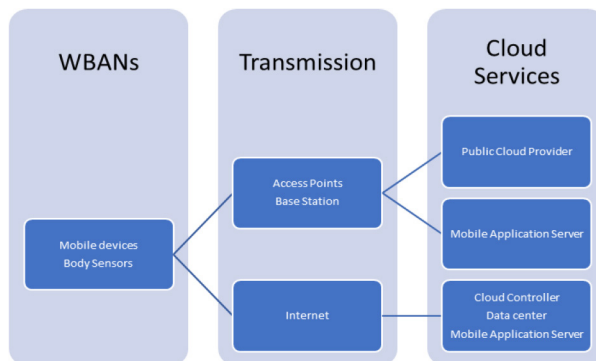


Figure 2
WBAN and mobile cloud computing

sensors attached or implanted in the human body to accumulate real-time data and sends that to the cloud storage or wirelessly transmitted to external healthcare processing units doctors for monitoring and scrutiny of such data. [10] implemented a Wireless Sensor Network integrated with Cloud architecture for e-healthcare application. The architecture shows how cloud computing can be used to form a distributed systems of different hospitals, pharmaceutical labs and blood banks to facilitate shared patient information. This architecture could be adopted during pandemics to share and avoid duplicate patient information.

4. Benefits of cloud computing in health/medical cyber physical systems

As opined [3] cyber-physical systems are systems that provide feedback that have been broadly utilised in health care, automation, communication, smart building, transportation, energy, robotics and physical security . Often, CPS has been considered as an engineering vernacular, however; have been considered as the computer science and mathematics over time. It focuses on algorithmic capabilities, dynamics and data transformation processes. It additionally supports the storage and communication aptitudes coupled with monitoring and control components of the physical world.

CPS have computational and processing capabilities; they directly communicate with hardware components or devices. They collect and process vast amounts of data from the environment using IoT devices and needs space to store collected data.

CPS architecture has four layers according to [2] namely: application, support, network and perceptual layers, however, [11] mentions only three layers namely: application, transmission and perceptual layers; that is the support and network layer are combined; 1) Application layer is the closer to the user mainly meant for decision making and analysis of data and information. 2) Transmission layer (combines network and transport layers) is concerned with transmission of data from the perception and application layer. This layer makes use of protocols such as Zigbee and wireless networks. It also ensures data routing, make use of Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) and firewalls. At the Perception layer environmental real-time data is collected through the use of sensing devices such as the actuators, sensors and Radio Frequency Identifications (RFIDs). The structure of a cyber-physical system is shown in Figure 3 inspired by the presentation done by [12].

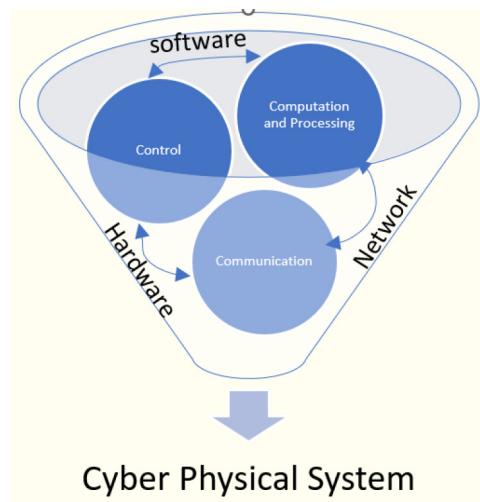
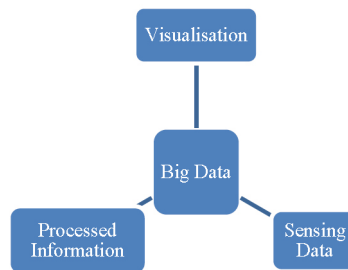


Figure 3
Cyber Physical System Structure

Medical Cyber Physical Systems (MCPS) or Health CPS are merely the CPS used in the health or medical sector to advance the medical processes. In the contemporary era, due to the burgeoning of the IoT technologies, CPS usage in the health sector has escalated significantly where most of the CPS are embedded with IoT devices to collect data from the human bodies, doctor to patient monitoring, data monitoring and management using big data analytics. This establishes that Medical CPS need to have optimal computing speed, huge storage capacity and high processing speed. However, MCPS lack in storage capacity, processing power and speed; due to these challenges, that's where integration of cloud computing comes in. As opined by [6], Cloud computing is beneficial in CPS because it assists with virtualization that enables health sectors to avoid costly computing/processing costs as well as lowering the cost of hardware or any computing devices that maybe needed by the medical sectors.

By mapping the needs of the health sector to the cloud computing services, it is obviously costly for a medical institution to invest in hardware, software and other resources needed to advance the medical services, hence, the escalated cloud computing adoption in health sector. The work of [1] discusses in detail the taxonomy of CPS in health sector; the discussion points out application [1], architecture [2], sensing [2], data management [4], computation [5], communication [6], security [7], and

**Figure 4****Cloud Computing Integration in MCPS**

control/actuation [8] to be major components of a medical CPS. These elements tally well with the structure in

Figure 4 and justifies the notion of [2] that CPS are resource limited, thus an introduction of Cloud Cyber Physical Systems (CCPS).

Figure 4 demonstrates the integration of cloud computing in MCPS.

5. The cyber security risks of cloud computing integration in health cyber physical systems

Due to the rapid change and adoption of IoT devices and cloud computing in health cyber physical systems, a plethora of new cyber security risks have been recorded to date as opposed to the traditional computing systems. Inadequate security for CPS can have adverse effects consequently because sensitive and confidential information about the physical environment is often collected by the CPSs. Consequently, security loss leads to loss of privacy, costs associated with operational disturbance and prospective physical destruction [2].

MCPS as discussed in the previous section are connected to the human bodies to collect data such as heart beat, pulse, blood pressure and are used to monitor old age people etc., with this example, if any harm happens to the MCPS or perhaps there is some misconfigurations; it means adverse effects to the people connected to it, hence, the need to investigate the security of cloud medical cyber physical systems. [13] Elucidate some of the requirements of medical cloud cyber physical systems as:

1. **Security:** The signals and data collected need to be protected.

2. **Privacy:** It is vital that significant collected medical data managed by CPS is not tempered with as it may consequently result in abuse, physical harm and loss of privacy to the patients [10].
3. **Data Integrity:** Data tempering of the collected data must be avoided in all cost.
4. **Data Access Control:** Only authorized persons should have access to the data.
5. **Availability:** The medical services should be available almost all the time when required.
6. **Interoperability:** In MCPS, integration of MCPS with other medical devices is essential and they need to be integrated safely and securely.

The requirements of MCPC are not limited to those discussed above, there are other security requirements such as confidentiality, non-repudiation and authentication as discussed by [11].

[2] Utters that the integration of cloud computing in health cyber physical systems have opened a door to attacks such as Denial of Service

Table 1
Cyber-attacks at different layers of the CMCPs

CMCPs	Cyber security attacks at different layers of the CMCPs		
	Application Layer	Transmission Layer	Perceptual Layer
Objectives	Analysis of Data and decision making	Transmission of data	Collection of Data
Target: Security	Privacy Security Authentication Safety	Confidentiality Integrity Availability Authentication	Confidentiality Privacy Authentication
Threat / attack	Internet Control of Message Protocol (ICMP) flooding, Malicious Code injection, Botnets, malware, Buffer overflow	Denial of Service/ Distributed DOS, User Datagram Protocol (UDP) flood, Man-in-the-middle attack, Repudiation Replay	Eaves dropping Port scan Passive reply

(DoS) and Distributed Denial of Service (DDoS) attacks [12], phishing and Man in the Middle attacks. On the same note [14] alludes that some of the recent attacks encountered on the medical cyber physical systems include malicious code injection attacks, fake data injection attacks and code reuse attacks,. Furthermore, their research shows that there have been several Denial-of-service attacks on cloud CPS thus affecting availability goal since they intensify resource utilization and cause harmful disruptions. While on the same note of security attacks, [11] conducted a study on the security issues of CPS where they identified a plethora of the attacks as summarized in Table 1. In addition to these other studies, [3] discuss a list of prevailing attacks to cyber physical systems as: Stuxnet, insider, Distributed Denial of Services, phishing attack and man-in-the-middle attack. The MCPS are no different from other CPS hence they inherit similar attacks and combines them with cloud security attacks which are discussed by [2].

[15] Identified vital security challenges towards health sector and inherent vulnerabilities, from which Medical cyber physical systems vulnerability was identified as a key challenge. The vulnerabilities identified were therefore: 1) MCPS limited capability, 2) The dependency on the health care network exacerbates the cyber security risks to health care systems and 3) Vulnerable IoT devices introduce cyber threats to the MCPS. Due to the Covid-19 pandemic, most of the health workers have been working remotely and as it has been discussed in the previous sections, remote working is made possible by integration of cloud computing where services and required data are housed in cloud servers. The adoption of remote working in health sector as opined by [15] has stretched the medical sector attack surface. On the very same note, [16] justifies that the integration of cloud computing and physical systems have brought about a lot of cyber-attacks; their research point out that unauthorized access and virus are the most reported attacks.

6. Cyber security Mitigations techniques and tools for Cloud Computing attacks in Medical cyber physical systems

Owing to the integration of IoT and cloud computing, it is evident that the rate of cyber-attacks targeting the health sector is rapidly increasing, as such there is a need to investigate the suitable mitigation techniques. [15] Carried out a comprehensive study which outlined multiple security measures to be taken to safeguard the general health sector. From the study by [15] securing of endpoint devices and securing

the remote work environment is emphasised; thus, all the technologies need to be secured, using measures such as perimeter firewalls and antiviruses. At the same time, used technologies and devices should comply with Health Insurance Portability and Accountability Act (HIPAA).

Additionally, knowing that if the end devices are not well protected, they can be a gateway to denial of services attacks; [17] also suggest the use of remote access control, firewall, Host Intrusion Detection Systems (HIDS) and Host Intrusion Prevention Systems (HIPS). Suggestions of [15] on remote access security include use of Multifactor authentication (MFA) and remote access monitoring. [11] Denotes that MFA is a crucial requirement in CPS because of its ability to condense false positives, and to obfuscate the authentication attacks. This is possible because instead of breaking a single factor, several factors should be broken. Subsequently, access to resources or sensitive information is limited to authorized entities and personnel (devices/users) only.

Owing to cloud computing adoption, [18] suggest the use of encryption, access management [19] and IDS and firewalls to counteract the privacy issues. However, this depends on the type of cloud computing used as the internal Cloud Computing enables the deployment of any security solutions that is seen fit by the IT department, on the other hand external Cloud Computing security solely depends on Cloud Service Provider, while other Cloud Service providers do not give the client the liberty to choose the security solutions of their choice and lastly while other Cloud Service Providers let their clients implement their own security measures. Regarding the type of firewall to use [11] alludes that honey pots and deception techniques are the key deception mechanisms that are commonly applied to cyber physical systems.

[15] suggest raising security awareness, it holds water to assert that humans are perceived the weakest link in security. However, the perimeter security is not enough as most of the phishing attacks that have been recorded as escalating in health sector because of unaware or uneducated employees. Further suggestions include implementing cyber security training programs and continuous cyber security campaigns. [11] Also supports the implementation of periodic cyber security awareness training; this must be performed depending on the level and knowledge of employees. Employees should be made aware of the importance of security and how to spot suspicious activities as well as the reporting mechanisms to follow.

Due to the fact that CPS are forming part of the health sector network, it is significant to segregate the network to isolate the traffic as well as to apply cryptographic security and encryption to achieve privacy and security [15]. One of the encryption mechanisms recommended by [11] and [15] is the homomorphic encryption as it enables the computation and analysis of encrypted data on the cloud. It solves the problem of traditional encryption algorithms which would require an encryption key every time an encrypted file or system was analysed.

[20] Presents a Cyber Physical Enhanced Secured wireless sensor network (WSNs) integrated cloud computing for u-life care (CPeSC3) architecture for health care monitoring and decision support system. The architecture has multiple modules but of interest in this study is the security module. To achieve security [20] applied concatenation between "source sensor node" and "random number" to protect against attacks and applied encryption to anonymise the source node against attacks to achieve identity privacy. *"In order to provide protection against en-route attacks from traffic analysis or fabrication during transfer from one node to another, a secure communication model can be built which can help to establish hybrid key (asymmetric key and symmetric keyed hash function) scheme. On this basis, asymmetric key (between the sensor node and the base station) is used only for hiding the sensor node identity (anonymity) while the symmetric keyed hash function is used to protect the whole actual sensed data"* alludes [20].

There are a myriad of mitigation techniques that can be applied and they can be found on the papers of [15] and [11]. In addition to the proposed solutions on literature, [21] proposes utilising machine learning to detect threats in CPS. It is very significant that any medical institution that intends to adopt the use of IoT technology, Cloud Computing and cyber physical systems follow a comprehensive business continuity plan and establish the internal cyber security policies as well as to adhere to the national and international policies relating to health care sector and data protection.

7. Recommendations

The study has revealed the need to reduce the cyber-attack surface as a means of ensuring confidentiality, integrity, availability, and accountability within the electronic health systems. Multiple solutions to be implemented for the cybersecurity of cloud computing in MCPS as has been discussed. To ensure endpoint security, antiviruses, firewalls, HIDS, HIPS, MFA, encryption, and security awareness are recommended in

compliance with HIPAA requirements. Implementation of defence-in-depth mechanism offers a comprehensive security solution. Thus, to achieve the next generation medical CPS, next generation security should be implemented which includes the use of block chain to achieve accountability and predictive models such as machine learning and neural networks to ensure robust and resilient medical infrastructure. This is to be implemented with a robust security awareness program to strengthen human security in the value chain. Lastly, we recommend implementation of Virtual Private Networks to ensure secure communication from endpoints to servers and vice versa.

8. Conclusion

From the study it is obvious that cloud computing has brought some advantages in the health or medical sector, despite these advantages the integration of cloud computing in the health sector has raised numerous security concerns which amongst other include the choice of either private or public Cloud infrastructure. On top of that privacy and trust issues are other major security concerns [11][8][22][2]. In addition, the integration of sensors, RFID and in general IoT technology in medical CPS opened a backdoor to more attacks especially malware in its different facets such as adware and ransomware.

The study probed the applications of cloud computing in health care, the benefits of cloud computing in health cyber physical systems, cyber security of cloud computing in health cyber physical systems. The study concludes that cloud computing is broadly integrated in the health sector. This integration has enabled most of the health services and with the adoption of small embedded sensing devices that form Body Area Network (BAN) [10] patient data processing and real-time medical data capturing is possible. The study also perused the mitigation techniques suggested by different researchers. The techniques include the use of encryption, network segregation, use of next generation firewalls and IDS/IPS as well as security awareness.

Conflict of Interest

The authors declare no conflict of interest.

References

- [1] S. A. Haque, S. M. Aziz, and M. Rahman, "Review of cyber-physical system in healthcare," *Int. J. Distrib. Sens. Networks*, vol. 2014 (2014), doi: 10.1155/2014/217415.
- [2] Y. Borse and M. Saleh, "Cloud based Cyber Physical Systems Security Issues: A Survey," *Int. J. Comput. Appl.*, vol. 177, no. 9, pp. 38–40 (2019), doi: 10.5120/ijca2019919474.
- [3] M. M. Nair, A. K. Tyagi, and R. Goyal, "Medical Cyber Physical Systems and Its Issues," *Procedia Comput. Sci.*, vol. 165, no. 2019, pp. 647–655 (2019), doi: 10.1016/j.procs.2020.01.059.
- [4] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure," *IEEE Access*, vol. 6, pp. 25167–25177 (2018) doi: 10.1109/ACCESS.2018.2817560.
- [5] M. Masrom and A. Rahimli, "A review of cloud computing technology solution for healthcare system," *Res. J. Appl. Sci. Eng. Technol.*, vol. 8, no. 20, pp. 2150–2153 (2014) doi: 10.19026/rjaset.8.1212.
- [6] R. Chaâri et al., "Cyber-physical systems clouds: A survey," *Comput. Networks*, vol. 108, no. November 2017, pp. 260–278 (2016) doi: 10.1016/j.comnet.2016.08.017.
- [7] A. HA and G. A., "Cloud Computing and Healthcare Services," *J. Biosens. Bioelectron.*, vol. 7, no. 3 (2016) doi: 10.4172/2155-6210.1000220.
- [8] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "EHealth Cloud Security Challenges: A Survey," *J. Healthc. Eng.*, vol. 2019 (2019) doi: 10.1155/2019/7516035.
- [9] H. Moghaddasi and A. Tabatabaei Tabrizi, "Applications of Cloud Computing in Health Systems," *Glob. J. Health Sci.*, vol. 9, no. 6, p. 33 (2016) doi: 10.5539/gjhs.v9n6p33.
- [10] N. Dey, A. S. Ashour, and S. J. Fong, "Medical cyber-physical systems : A survey," pp. 1–13 (2018).
- [11] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocess. Microsyst.*, vol. 77 (2020), doi: 10.1016/j.micpro.2020.103201.
- [12] I. Priyadarshini et al., "A new enhanced cyber security framework for medical cyber physical systems," *Software-Intensive Cyber-Physical*

- Syst., vol. 35, no. 3–4, pp. 159–183 (2021), doi: 10.1007/s00450-021-00427-3.
- [13] P. V. Devi and V. Kalaichelvi, “Security Issues in Medical Cyber Physical Systems (MCPS)-A survey,” *Int. J. Pure Appl. Math.*, vol. 117, no. 20 Special Issue, pp. 319–324 (2017).
 - [14] B. Yildiz and E. H. Younes Gejam, “Cyber-Physical Systems and Cyber Security: A Bibliometric Analysis,” *OPUS J. Soc. Res.*, vol. 19, no. 45, pp. 1–1 (2022), doi: 10.26466/opusjsr.1063227.
 - [15] Y. He, A. Aliyu, M. Evans, and C. Luo, “Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review,” *J. Med. Internet Res.*, vol. 23, no. 4, pp. 1–18 (2021), doi: 10.2196/21747.
 - [16] Y. B. Reddy, “Cloud-based cyber physical systems: Design challenges and security needs,” *Proc. - 2014 10th Int. Conf. Mob. Ad-Hoc Sens. Networks, MSN 2014*, no. October 2015, pp. 315–322 (2014), doi: 10.1109/MSN.2014.50.
 - [17] N. S. Abouzakhar, A. Jones, and O. Angelopoulou, “Internet of Things Security : A Review of Risks and Threats to Healthcare Sector,” pp. 12–17 (2017), doi: 10.1109/iThings-GreenCom-CPSCo-SmartData.2017.62.
 - [18] A. Atianashie Miracle and C. C. Adaobi, “Cloud Computing in Health Care: Opportunities, Issues, and Applications: a Systematic Evaluation,” no. July (2021).
 - [19] H. Qiu, M. Qiu, M. Liu, and G. Memmi, “Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0,” *IEEE J. Biomed. Heal. Informatics, Biomed. Heal. Informatics, IEEE J. of, IEEE J. Biomed. Heal. Inform.*, vol. 24, no. 9, pp. 2499–2505 (2020), doi: 10.1109/JBHI.2020.2973467.
 - [20] J. Wang, H. Abid, S. Lee, L. Shu, and F. Xia, “A secured health care application architecture for cyber-physical systems,” *Control Eng. Appl. Informatics*, vol. 13, no. 3, pp. 101–108 (2011).
 - [21] P. Perrone, F. Flammini, and R. Setola, “Machine learning for threat recognition in critical cyber-physical systems,” *Proc. 2021 IEEE Int. Conf. Cyber Secur. Resilience, CSR 2021*, pp. 298–303 (2021), doi: 10.1109/CSR51186.2021.9527979.
 - [22] J. Al-Jaroodi, N. Mohamed, and E. Abukhousa, “Health 4.0: On the Way to Realizing the Healthcare of the Future,” *IEEE Access*, vol. 8, pp. 211189–211210 (2020), doi: 10.1109/ACCESS.2020.3038858.