International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Alleviating Emerging Cyber Risks in Medical Internet of Things (IoT) Device

GIRISH KOTTE
girish.kotte1@gmail.com

Abstract

The report studies ways to handle growing cyber dangers that affect medical IoT devices in healthcare facilities. It addresses issues in technology and operations, looks into the best cybersecurity approaches and points out the importance of using authentication, monitoring constantly and relying on Zero Trust Architecture. The study finds through secondary data analysis and thematic analysis that certain conforming frameworks help secure sensitive health data, guarantee patient safety and enhance the stability and reliability of medical technology networks.

Keywords: IoT devices, Cybersecurity, healthcare, cyber threat, cyber risks, compliance, security, HIPAA, GDPR, risk-based authentication, 'Zero Trust Architecture (ZTA)'

INTRODUCTION

IoT devices have quickly become part of the healthcare sector, transforming patient monitoring, diagnostics, and the delivery of treatment. The use of wearable monitors, smart infusion devices, and interconnected imaging tools from medical IoT technology has improved both clinical and operational performance. Cybersecurity has become a major concern because technology is now closely linked and relies on data. In this context, using and sending sensitive medical details on networks, these devices are very vulnerable to cyberattacks, including ransomware, data breaches, and unauthorized access. Additionally, data being lost, these attacks can risk patients' health, privacy, and the credibility of healthcare services. The new cyber threats targeting medical IoT networks are getting more complex by using older software, weak encryption, and improperly set up network protocols. The purpose of this paper is to share information on methods to fight these new cyber risks, mentioning measures such as suitable policies and technologies designed for secure medical IoT systems.

Aim

The focus of this report is to study and suggest strategies that can help reduce new cyber threats in medical IoT gadgets.

Objectives

- To determine the complex operative and technical risks associated with implementing 'cybersecurity measures' within the medical IoT device environment
- To examine the workflow of risk-based authentication, continuous monitoring, and authenticated users can increase the protection of healthcare data carried through IoT devices
- To assess the credibility of innovative 'cybersecurity models' and tools for supporting the flexibility, compatibility of linked healthcare environments
- To suggest the best approaches for 'healthcare organizations' to adopt effective 'cybersecurity frameworks' that cooperate with administrative standards

Research Questions

- What are the complex operative and technical risks associated with implementing 'cybersecurity measures' within the medical IoT devices environment?
- How to examining the workflow of risk-based authentication, continuous monitoring, and authenticated users increase the protection of healthcare data carried through IoT devices?
- What is the credibility of innovative 'cybersecurity models' and tools for supporting the flexibility, compatibility of linked healthcare environments?
- How to suggest the best approaches for 'healthcare organizations' to adopt effective 'cybersecurity frameworks' that cooperate with administrative standards?

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

RESEARCH RATIONALE

The application of IoT devices in healthcare supports better patient care by monitoring patients online, diagnosing through data, and providing treatment remotely. In this context, depending on these devices more often leads to serious cybersecurity risks because they often do not have strong security measures against advanced cyber threats. A lot of medical IoT devices use traditional software, do not have enough processing ability for complex encryption, and are connected to different types of networks [1]. The study is important to discover local cybersecurity options that meet functionality, compliance, and security standards. The goal behind this work is to address this major issue by researching methods that can help healthcare systems better manage and lower cyber risks.

LITERATURE REVIEW

Complex operative and technical risks accompany by implementation of 'cybersecurity measures'

Ensuring cybersecurity in medical IoT devices introduces many complex and technical issues, mainly in the changing environment of medicine. The 'IoT devices' have less computing capacity, low power, and unique software from the manufacturer; they are not usually made with built-in security features. Adding strong cybersecurity measures to hospitals with constrained systems can delay healthcare staff, cause devices to fail, and result in security risks for patients [2]. In this context, ensuring security frameworks can be smoothly used in healthcare calls for them to be integrated with systems that are not connected and standardized. As a result, systems are more likely to have misconfigurations, compatibility problems, and operational issues [3]. There is a challenge to upgrade software or change to newer solutions because most hospitals have outdated systems.

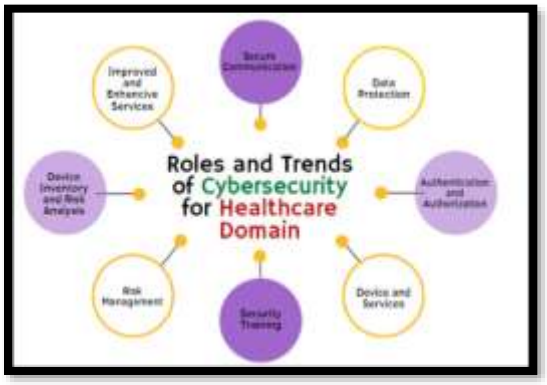

Fig. 1: Functions of cybersecurity in healthcare

Real-time data coming from IoT devices all the time requires extra encryption, reliable authentication, and constant monitoring, which is expensive and calls for teamwork. Following this, to comply with the healthcare regulations 'Health Insurance Portability and Accountability Act (HIPAA)' and 'General Data Protection Regulation (GDPR)', companies must ensure their data is safe [4]. Implementing 'HIPAA' and 'GDPR' is also important to note the involvement of people in these situations. Not all staff may have the right cybersecurity training, which adds to the risks faced by the organization. Ultimately, all systems require cybersecurity, and its use in 'medical IoT' requirements needs to be managed so it does not reduce the system's performance, usability, or regulatory compliance.

Workflow of risk-based authentication, continuous monitoring of healthcare data

The application of a well-structured process of risk authentication, ongoing monitoring, and authenticated access to systems helps shield sensitive healthcare information sent through IoT devices. The process first involves 'risk-based authentication', checking access requests considering factors like the device, location, time, and user activity to give a score for each request[5]. After authentication is completed, 'continuous monitoring' starts to monitor for real-time changes in data flow, user actions, and device behavior. In this way, unusual or risky activities in the network can be spotted, for example, uncommon access records, unusually large data volumes, or links to devices not permitted for use in the network. Automatic alerts or blockages can be issued, which helps quickly respond to the incident if unusual events are spotted.

Furthermore, having authentication limits who can work with essential systems and sensitive medical

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

records. This way, companies can protect themselves from risks caused by employees doing the wrong thing and improperly setting equipment. Ensuring these mechanisms are used together allows medical institutions to safeguard data, comply with the rules 'HIPAA', 'GDPR', and earn people's trust in medical IoT infrastructure[6]. By following this organization, 'IoT hardware' remains safeguarded from threats, preventing major risks and allowing the system to work continuously. Companies need proactive workflows to maintain their sustainability, security, and legal compliance in healthcare while cyber risks change.

Credibility of innovative 'cybersecurity models' and tools for supporting the flexibility

The integrity and value of innovative 'cybersecurity models' and systems are necessary to solve the special issues that connected healthcare systems face because of IoT. The number of IoT devices being used has spiked, allowing for fast monitoring, automating diagnosis, and sharing information smoothly because digital transformation enables healthcare institutions. Additionally, networks being so connected create more risk from cyber attacks because standard firewalls can no longer keep them secure[7]. In this context, because of these risks, newly developed security approaches like 'Zero Trust Architecture (ZTA)', AI that detects unusual activity, and blockchain to protect 'data integrity'[8]. Continuous verification, using many devices, and anticipating cyber threats are the main priorities in cybersecurity models. Being flexible and compatible helps software deal with the mixed nature of healthcare IT infrastructure, where smooth connections and system operations are very important.

Moreover, these models make it possible for policy enforcement to happen automatically, so any breaches are addressed fast without human aid in real time. 'IoT devices' are stronger in protecting themselves against risks or intruders with device identity systems and updated firmware[9]. In order to demonstrate that 'IoT devices' comply with guidelines, healthcare apps also align themselves with the 'HIPAA' and 'GDPR' regulations. Basically, strategic investment in new 'cybersecurity solutions' increases the reliability of healthcare systems, helps maintain safe data transfers, ensures that operations can continue, and improves patient safety.

Best approaches for 'healthcare organizations' to adopt effective 'cybersecurity frameworks'

Organizations can manage emerging cyber risks in medical IoT devices best by following cybersecurity guidelines that can be changed and comply with rules and regulations. The main way is to use a layered security design, which uses endpoint protection, encryption, IDS, and secure access controls to address the latest cyber risks[10]. Since healthcare devices on the Internet include a wide variety of items, security policies must work with different types of devices and be flexible enough to fit operational constraints. It is very important to comply with the 'HIPAA' and the 'GDPR' to add data privacy measures, auditing tools, and response plans of companies into their security routines[11]. 'Security audits' and vulnerability checks should be carried out frequently to uncover and fix weaknesses in a system as soon as possible.

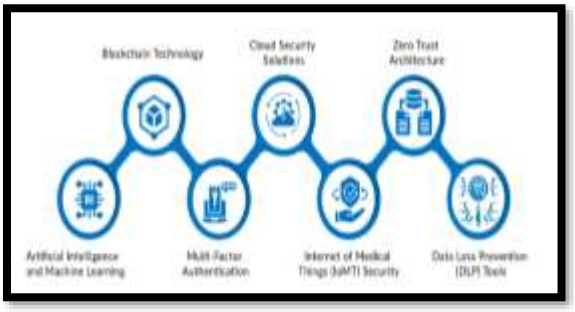

Fig. 2: Cyber-security innovation in healthcare

In this context, the healthcare sector can now identify irregularities at the time of their occurrence with the help of AI and machine learning, which reduces the time needed for response. The organizational staff receive 'cybersecurity training' and a culture of cybersecurity is promoted, and the organization becomes more resilient. Another useful approach is to use 'Zero Trust Architecture', since no device or user is allowed to access anything unless specifically verified [12]. Following the necessary cybersecurity guidelines and policies is necessary to meet regulations and to increase the trust, safety, and dependability of healthcare services with so many IoT devices.

Literature gap

Researchers have discussed the technical and regulatory difficulties of protecting medical IoT, and there is a lack of cybersecurity methods that can combine real-time needs, simplicity, and compliance. There is a limited number of studies investigating the usage of 'Zero Trust' frameworks in varying healthcare environments, mainly in traditional

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

computer systems, and a lower awareness of cybersecurity.

METHODOLOGY

This report follows "***Secondary data sources***" because detailed information from publications, studies, and reports exists about alleviating emerging cyber risks in medical 'Internet of Things (IoT)' devices. The existing report examines this method, and the complex operative and technical risks accompanied by implementing 'cybersecurity measures' within the medical IoT devices environment [13]. Secondary data is a useful data source in this report to analyze the workflow of risk-based authentication, continuous monitoring, and authenticated users can increase the protection of healthcare data carried through IoT devices. The researcher selected "***interpretivism philosophy***" because it aims to use a layered security design that uses endpoint protection, encryption, IDS, and secure access controls to address the latest cyber risks [14]. The interpretive philosophy investigates the credibility of innovative 'cybersecurity models' and tools for supporting the flexibility in the healthcare sector.

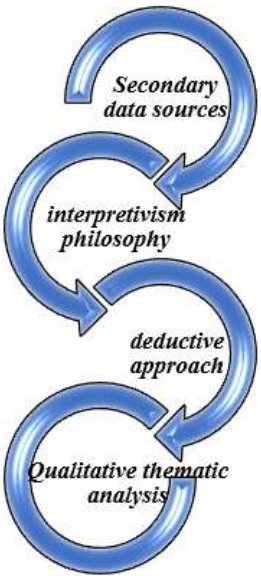

Fig. 3: Methodology

The selected approach has singular significance in medical IoT devices and introduces many complex and technical issues, mainly in the changing environment of medicine. This report applies a ***deductive approach*** to evaluate the best approaches for 'healthcare organizations' to adopt effective 'cybersecurity frameworks' that cooperate with administrative standards. The existing report investigates the technical risks associated with implementing 'cybersecurity measures'. The collected information in this report goes through "***Qualitative thematic analysis***," which enables researchers to increase the trust, safety, and dependability of healthcare services with so many IoT devices [15]. The thematic analysis utilises this method because it offers a comprehensive analysis of the emerging 'cyber risks' in medical 'Internet of Things (IoT)' devices.

DATA ANALYSIS

Theme 1: The complex operative and technical risks associated with implementing 'cybersecurity measures' within the medical IoT devices environment

There are some difficulties in securing medical IoT devices in modern healthcare because there are many challenges at both the operational and technological levels. Most of these devices, such as wearable sensors, infusion pumps, and remote diagnostics, have little processing power, a low battery, and run software unique to the company that is not always secure. In this context, adding good cybersecurity to such limited networks can cause issues with operations, workflow delays, and incompatibility, which could harm patient care [16]. The setup is not always correct, and this leads to more threats from hackers when companies attempt to update older systems with modern security tools. Updating cybersecurity with good intentions in these places can actually create more risks, while the updates clash with the technical capabilities of the network [17]. Additionally, because IoT devices continuously send real-time data, it is important to have strong encryption, 'risk-based authentication', and constant monitoring, which are all difficult and costly to maintain everywhere. As a result, managing these demands is complex, and all IT, medical, and compliance staff must work very closely together. More regulations, such as 'HIPAA' and 'GDPR', make it even more difficult to implement cybersecurity. The incorrect handling of system configuration and data can result in additional vulnerabilities, instead of preventing existing cyber threats, because staff in many healthcare organizations do not receive proper training for cybersecurity [18].

Healthcare providers should develop particular cybersecurity protection for medical IoT considering their individual work procedures and types of technological constraints.

Theme 2: The workflow of risk-based authentication, continuous monitoring, and authenticated users can increase the protection of healthcare data carried through IoT devices

Setting up a specific process involving risk-based authentication, 24/7 monitoring, and validated access for users is necessary to better guard 'IoT medical devices' in the digital healthcare field. The IoT devices are at greater risk from cyber threats, which calls for more advanced cybersecurity while handling personal patient information. This method analyzes things such as device identity, location, time, and behavior of the person trying to access the system. Each login is reviewed by the system to identify possible deceit, which helps prevent unauthorized users, and constant monitoring ensures that real-time data and activity by users are carefully observed after access is given.

An unauthorized entry is registered, important data moves unusually, or someone communicates with a device that has no access, the system can report this right away and may block the process [19]. Such reactions lessen the dangers of cyber-attacks and help make the system more secure without needing input from staff. Using authenticated user procedures increases cybersecurity since only verified individuals can gain access. The healthcare institutions have 'accountability' and 'traceability'; they are able to control both internal threats and operational errors more conveniently [20]. Another advantage of this is that the workflow can comply with 'HIPAA' and 'GDPR', both of which require well-secured data practices. All these steps combine to make a cybersecurity framework that is ready to handle the specific issues found in medical IoT networks.

Theme 3: The credibility of innovative 'cybersecurity models' and tools for supporting the flexibility, compatibility

The use of IoT in healthcare is increasing, so healthcare systems need advanced cybersecurity models that are reliable and can change with technological progress. Standard security techniques are not enough to face the complicated 'cyber attacks' that connect different systems, which underlines the importance of inventing innovative approaches. As a result, 'Zero Trust Architecture (ZTA)', AI-based threat detection, and tools for securing data with blockchain are becoming more common [21]. Real-time observation, constant verification, and automatic policy enforcement increase a network's resilience against new cyber threats. Any security solution must be both flexible and compatible because healthcare systems are always changing and sharing data. IoT models should be innovative, let different kinds of devices to cooperate and maintain compatibility with current medical devices. They work to support audio, video, and file sharing that is secured by encryption, access by legitimate users, and identification with systems that meet the requirements of 'HIPAA' and 'GDPR' [22].

Another reason these approaches are credible is that they carefully detect anything unusual, identify dangers, and defend against attacks without putting critical healthcare activities at risk. Using automatic updates and smart alerts keeps IoT devices safe and usable for different purposes. In this context, using dependable cybersecurity methods, healthcare institutions can create sturdy protection for their digital data, ensure operations keep going, and help patients stay protected. They boost trust towards the institution and help in following regulations and the gradual development of digital healthcare systems [23].

Theme 4: Best approaches for 'healthcare organizations' to adopt effective 'cybersecurity frameworks' with administrative standards

Organizations need to install cybersecurity systems that are advanced from a technical and management standpoint to protect IoT devices in healthcare. Using a variety of security measures, such as protecting endpoints, securely encrypting data, monitoring for breaches (IDS), and role-based control, is very useful. These multiple layers make it harder for advanced cyber threats to harm the critical healthcare systems. Data management frameworks must work with many types of systems and meet mandates such as 'HIPAA' and 'GDPR' because 'IoT devices' may be wearable sensors or smart diagnostic tools [24]. For this reason, privacy protocols, routine reviews, and clear incident response plans must be included to maintain data confidentiality and reliability. The continuation of vulnerability tests and using AI to find threats in real time, so that operations in healthcare remain safe and secure at all times [25].

Providing regular cybersecurity training to staff helps reduce human error, which is a big reason for 'cyber incidents. 'Zero Trust Architecture' is an extra step to support security by verifying access and limiting the number of unprotected access points. Linking administrative requirements to cybersecurity policies

helps an organization obey the law and stay secure using technology. Addressing cybersecurity alongside administrative requirements allows healthcare firms to secure vital patient information, gain confidence from stakeholders, and keep their IoT health services reliable.

FUTURE DIRECTIONS

Experts are planning to use 'edge computing' and 'quantum encryption' in future work to help protect 'medical IoT devices' better. Researchers will also work on making security algorithms so that the algorithms can be used on small healthcare IoT devices. Aiming to test the practical use of 'Zero Trust Architecture', efforts will be taken in clinical environments such as small hospitals with minimal equipment [26]. In addition, research will be done to create guidelines that align worldwide cybersecurity laws with local health care laws. It is planned to increase the involvement of IT workers, healthcare staff, and policy-makers together to guarantee the proper implementation of security practices. They will also work on training and information programs to help everyone become more mindful online.

CONCLUSION

This report points out that many medical IoT devices have old software, problems with hardware and non-standardized systems which leaves them at risk of cyber-attacks. Such risks endanger private health details, affect patient safety and harm the reputation of the institution. A study of secondary data showed that important matters of concern are the difficulties of defense implementation, the need for risk-based verification and consistent supervision and how effective Zero Trust Architecture and artificial intelligence are in fighting threats. Patient care has improved a lot in healthcare because IoT devices allow for regular monitoring, distant diagnosis and immediate treatments. It is concluded that administrative rules must be followed and the plan must consist of audits, encryption, real-time checks and employee training to guarantee the system remains strong and secure. In this context, developers and experts should concentrate on fresh technologies such as edge computing and quantum encryption for more secure IoT systems in medicine.

REFERENCES

[1] Kharroub, S.K., Abualsaud, K. and Guizani, M., (2020). Medical IoT: A comprehensive survey of different encryption and security techniques. *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp.1891-1896.

[2] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A., (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*, pp.1-10.

[3] Nisar, K., Jimson, E.R., Hijazi, M.H.A., Welch, I., Hassan, R., Aman, A.H.M., Sodhro, A.H., Pirbhulal, S. and Khan, S., (2020). A survey on the architecture, application, and security of software defined networking: Challenges and open issues. *Internet of Things*, 12, p.100289.

[4] Kaplan, B., (2020). Phi protection under hipaa: An overall analysis. *Kaplan, B.(with appendix by Monteiro, APL)," PHI Protection under HIPAA: An Overall Analysis," LGPD na Saúde (LGPD Applicable to Health), Dallari, AB, Monaco, GFC, ed., São Paulo: Editora Revista dos Tribunais (Thomsom Reuters)*, *2021*, pp.61-88.

[5] Atlam, H.F., Alenezi, A., Hussein, R.K. and Wills, G.B., (2018). Validation of an adaptive risk-based access control model for the internet of things. *International Journal of Computer Network and Information Security*, 15(1), p.26.

[6] Gade, K.R., (2020). Data Governance and Risk Management: Mitigating Data-Related Threats. *Advances in Computer Sciences,* 3(1).

[7] Tsochev, G., Trifonov, R., Nakov, O., Manolov, S. and Pavlova, G., (2020), October. Cyber security: Threats and challenges. *In 2020 International Conference Automatics and Informatics (ICAI)* (pp. 1-6). IEEE.

[8] Kaul, D., (2019). Blockchain-Powered Cyber-Resilient Microservices: AI-Driven Intrusion Prevention with Zero-Trust Policy Enforcement.

[9] Rizvi, S., Pipetti, R., McIntyre, N., Todd, J. and Williams, I., (2020). Threat model for securing internet of things (IoT) network at device-level. *Internet of Things*, 11, p.100240.

[10] Göksel, U.Ç.T.U., ALKAN, M., Doğru, İ.A. and Dörterler, M., (2019), October. Perimeter network security solutions: A survey. In *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 1-6). IEEE.

[11] Shah, S.M. and Khan, R.A., (2020). Secondary use of electronic health record: Opportunities and challenges. *IEEE access*, 8, pp.136947-136965.
[12] Wells, A., Ajeigbe, K. and Stern, M., (2020). Security Trends in Networking: From Traditional Approaches to Zero Trust Architectures.
[13] Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A., (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, 20, pp.1-10.
[14] Borky, J.M., Bradley, T.H., Borky, J.M. and Bradley, T.H., (2019). Protecting information with cybersecurity. *Effective model-based systems engineering*, pp.345-404.
[15] AlHogail, A., (2018). Improving IoT technology adoption through improving consumer trust. Technologies, 6(3), p.64.
[16] Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. and Dameff, C., (2020). Healthcare challenges in the era of cybersecurity. *Health security*, 18(3), pp.228-231.
[17] Bhuyan, S.S., Kabir, U.Y., Escareno, J.M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D. and Dobalian, A., (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, 44, pp.1-9.
[18] Tabrizchi, H. and Kuchaki Rafsanjani, M., (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), pp.9493-9532.
[19] Yaqoob, T., Abbas, H. and Atiquzzaman, M., (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review. *IEEE Communications Surveys & Tutorials*, 21(4), pp.3723-3768.
[20] Day, R.M., Demski, R.J., Pronovost, P.J., Sutcliffe, K.M., Kasda, E.M., Maragakis, L.L., Paine, L., Sawyer, M.D. and Winner, L., (2018). Operating management system for high reliability: leadership, accountability, learning and innovation in healthcare. *Journal of Patient Safety and Risk Management*, 23(4), pp.155-166.
[21] Mushtaq, S., (2019). Modern Cyber-Attacks and Cloud Security: Strengthening Information Security in Emerging Technologies.
[22] Boppana, V.R., (2019). Cybersecurity Challenges in Cloud Migration for Healthcare. *Available at SSRN 5004949*.
[23] Menear, M., Blanchette, M.A., Demers-Payette, O. and Roy, D., (2019). A framework for value-creating learning health systems. *Health research policy and systems*, *17*, pp.1-13.
[24] Alharbi, R. and Almagwashi, H., (2019), August. The Privacy requirments for wearable IoT devices in healthcare domain. In *2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 18-25). IEEE.
[25] Federici, B., (2019). Safeguarding Digital Infrastructure: Computer Science Approaches to Cybersecurity and Cloud Technology.
[26] Eichelberg, M., Kleber, K. and Kämmerer, M., (2020). Cybersecurity in PACS and medical imaging: an overview. *Journal of Digital Imaging*, 33(6), pp.1527-1542.