

Securing Medical Imaging Systems Against Emerging Cyber Threats: A Multi-faceted Approach

Rukminidevi Potlabathini¹, Bhavana Jamalpur¹, Nafis Uddin Khan^{2*}

¹School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana, India, ²Department of Artificial Intelligence and Data Science, Faculty of Science and Technology (IcfaiTech), ICFai Foundation for Higher Education (IFHE), Hyderabad, Telangana, India. *Corresponding Author's Email: nafisuk97@gmail.com, nafisuk@ifheindia.org

Abstract

In today's digital age, the convergence of healthcare and technology has revolutionized medical imaging, facilitating rapid diagnosis and treatment. However, with this advancement comes the pressing need to safeguard sensitive medical data from evolving cyber threats. Motivated by the critical role of medical imaging in patient care and the growing sophistication of cyber-attacks targeting healthcare systems, this article embarks on a comprehensive exploration of cybersecurity in medical imaging. The research commences with the development of a bespoke encryption framework tailored explicitly for DICOM and other medical imaging formats. This framework is meticulously crafted to uphold the highest standards of security while ensuring seamless accessibility for authorized users. Building upon this foundation, the study meticulously evaluates existing cybersecurity measures within the medical imaging domain, pinpointing vulnerabilities ripe for exploitation. Drawing upon the latest encryption techniques, the research proposes robust improvements to bolster the resilience of medical imaging systems against malicious intrusions. Furthermore, this work advances the frontier of cybersecurity in medical imaging by introducing a novel protocol for real-time anomaly detection during image transmission and storage. A comparative survey on various emerging methods developed so far in this area has been explored.

Keywords: Cybersecurity, Cyber Threats, Defense Mechanisms, Healthcare, Medical Imaging.

Introduction

A new age of healthcare innovation has been brought about by the quick integration of medical devices into networked systems, especially in the context of the Internet of Things (1). But along with the advantages of improved communication and simpler procedures, this connectedness has made the healthcare industry vulnerable to hitherto unseen cybersecurity threats. This article explores the important conversation about the security issues that medical imaging systems face, illuminating the constantly changing cyber threat environment and emphasizing the need to strengthen defenses to protect patient data and guarantee the provision of healthcare services. The use of federated learning is investigated to perform safe and privacy-preserving analysis of medical images (2). Federated learning enables the training of machine learning models across different decentralized medical institutions without the need to share raw data. This approach ensures the protection of patient privacy and enhances cybersecurity that has been depicted in Figure 1.

The article presented provides a thorough review of the complex cybersecurity issues that medical imaging systems face, emphasizing the growing complexity of cyber threats and the vulnerabilities present in medical equipment that are networked (3). It highlights the revolutionary effect of contemporary imaging technologies in transforming healthcare, enabling early illness identification and enhancing patient care via sophisticated diagnostic capabilities. It also draws attention to the dangers and difficulties that come with handling the enormous volumes of digital data that healthcare organizations produce, which makes strong security measures necessary to prevent breaches and protect patient privacy. The past research aims to develop a Network Detection System (NDS) utilizing various machine learning techniques to enhance network security through anomaly detection (4). Central to the discussion is the emergence of Medical Cyber-Physical Systems (MCPS), which integrate embedded software, networking capabilities and physiological elements

This is an Open Access article distributed under the terms of the Creative Commons Attribution CC BY license (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted reuse, distribution and reproduction in any medium, provided the original work is properly cited.

(Received 12th March 2026; Accepted 25th August 2026; Published 08th October 2026)

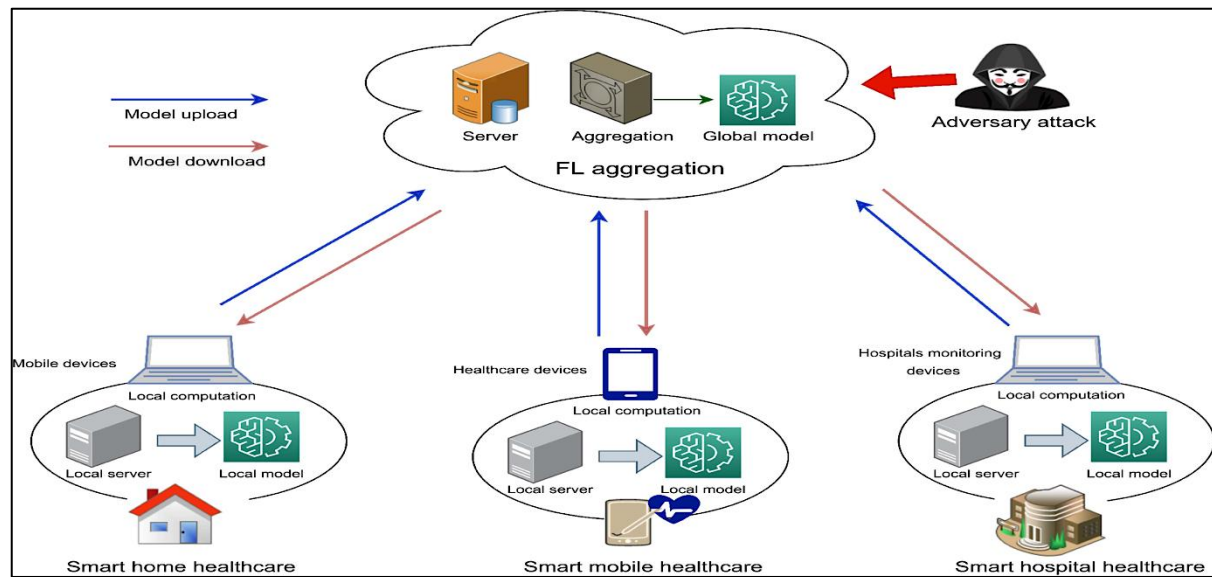


Figure 1: An Overview Architecture of Cyberattack in Healthcare Systems

to enhance monitoring and treatment in healthcare settings (5). While MCPS promise groundbreaking advancements in remote health monitoring and personalized medicine, they also introduce novel security challenges, necessitating comprehensive cybersecurity frameworks to safeguard medical data and devices from malicious exploitation. Furthermore, the integration of cloud computing technologies into healthcare infrastructures presents a viable solution for managing and storing medical data efficiently (6). Cloud-based solutions offer scalability, cost-effectiveness and ubiquitous accessibility, empowering healthcare organizations to optimize resource allocation while entrusting cloud providers with the responsibility of ensuring data security and compliance. But given how widely Internet of things and cloud technologies are being used in healthcare settings, it is imperative that security issues be addressed to reduce the hazards that may be presented by cyberattacks (7). The passage clarifies the security implications of medical equipment that are networked, highlighting the need of intrusion detection systems, access restrictions and encryption protocols to strengthen defenses against changing cyber threats that target medical systems (8).

Against this backdrop, the purpose of this paper is to explore the nuances of cybersecurity in the medical field with a focus on proactive defense tactics, encryption schemes and new security mechanisms that are specifically designed to meet the needs of healthcare organizations. This study

intends to contribute to the development of cybersecurity methods that protect patient data, maintain system integrity and support the core principles of healthcare delivery by analyzing the challenges associated with protecting medical imaging systems. The passages that have been presented provide an in-depth analysis of the complex field of cybersecurity, specifically about medical imaging equipment and the larger healthcare infrastructure (9). These texts highlight the dynamic nature of cyber threats and emphasize how crucial it is to strengthen defenses against hostile intrusions in a time of growing technological complexity and connectedness. Emphasizing real-time big data technologies, anomaly detection methods and machine learning algorithms, the research highlights the need of strengthening security protocols in the face of the increasing number of connected devices. It elucidates the daunting challenge posed by the exponential growth of networked devices, necessitating heightened vigilance and adaptive strategies to safeguard against a spectrum of cyber-attacks (10). Moreover, the excerpts elucidate the escalating risks facing medical imaging systems, where the convergence of technological advancements and healthcare intersects with vulnerabilities ripe for exploitation. From ransom ware attacks to vulnerabilities in network protocols, the discourse underscores the imperative for comprehensive security measures, spanning not only medical imaging systems but the entirety of healthcare IT infrastructure. The

conversation goes beyond medical imaging to include the larger field of networked medical equipment under the Internet of medical things, explaining the revolutionary possibilities as well as the inherent security threats (11-13). These articles navigate the challenges of protecting Internet of medical things devices while using their potential to transform healthcare delivery, from developments in semiconductor technology to the use of AI and block chain (14, 15). A summary of how quickly medical devices are being incorporated into networked systems under the IoT paradigm and the revolutionary effects of contemporary imaging technologies on the practice of medicine and the related cyber security dangers have been discussed.

Cybersecurity Issues and Vulnerabilities

The passage discusses several topics, including the rise in linked devices, Internet of medical things, the use of cloud computing and the need for encryption methods to protect patient data. The text delineates how the integration of medical devices into networks, alongside the adoption of

advanced technologies like AI and block chain, presents both opportunities and challenges, especially in terms of security risks (16). It underscores the critical need for robust security mechanisms to protect against cyber threats, given the sensitivity of patient information and the potential consequences of data breaches in healthcare settings. It also describes how important it is to secure medical imaging systems, such as Picture Archiving and Communication Systems (PACS) and emphasizes the role that Digital Imaging and Communications in Medicine (DICOM) standards play in guaranteeing the security and interoperability of medical data sharing. The passage also recognizes the development of MCPS and the need of resolving privacy and security issues in these systems to protect the confidentiality and integrity of medical data. In addition, it emphasizes how cyber threats are always changing and how crucial it is to develop proactive defense plans and promote stakeholder engagement to successfully reduce risks to vital infrastructure, including healthcare systems (17). Various types of cyber security attacks were shown in Figure 2.

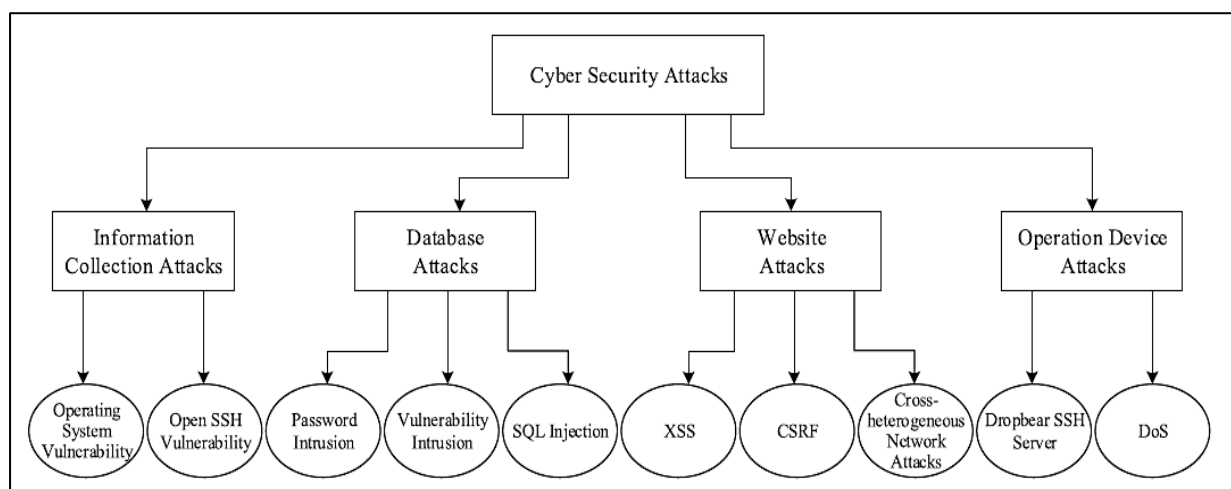


Figure 2: Various Types of Cyber Security Attacks

The significance of studying medical imaging systems within the context of evolving cyber threats and vulnerabilities within interconnected networks cannot be overstated. Over the last several years, the incorporation of medical devices into networks has significantly increased due to innovations like the Internet of medical things and the use of cloud computing. While these developments offer immense potential for improving

patient care and streamlining medical processes, they also introduce significant security risks. One of the primary concerns is the safeguarding of patient data, which is of utmost importance due to its sensitivity and the potential consequences of breaches in healthcare settings (18). Encryption techniques are crucial for protecting this data from unauthorized access or manipulation, especially as medical devices become increasingly interconnec-

ted and reliant on data exchange. Furthermore, the adoption of advanced technologies like artificial intelligence and block chain introduces both opportunities and challenges in terms of security. While AI can enhance diagnostic accuracy and treatment effectiveness, it also opens new attack vectors that malicious actors could exploit. Similarly, block chain holds promise for ensuring the integrity and immutability of medical records, but its implementation must be accompanied by robust security measures to prevent unauthorized access or tampering. Securing medical imaging systems, such as PACS, is of utmost importance in this context. Standards such as DICOM are essential for guaranteeing that medical data can be exchanged securely and effectively. However, it is necessary to implement more safeguards to address emerging security risks. The rise of MCPS highlights the need to prioritize security and privacy measures to safeguard the authenticity and secrecy of medical data (19). The dynamic

nature of cyberattacks that specifically target essential infrastructure, such as healthcare systems, necessitates the implementation of proactive defense mechanisms and the cooperation of all parties involved (20). Healthcare businesses may successfully manage risks and protect patient information from cyber-attacks by keeping updated on developing threats and employing strong security measures. It is crucial to comprehend and tackle the overlap between medical imaging systems and cybersecurity to guarantee the ongoing dependability and safety of healthcare provision in an ever more digital era (21).

Every step of a medical imaging workflow, from image acquisition to image viewing, needs to have security safeguards in place to address cybersecurity concerns. The common vulnerabilities and related mitigation techniques for each component are shown in Table 1.

Table 1: Cybersecurity Vulnerabilities in Acquisition Devices, Communication Networks, PACS Servers, Cloud Repositories and Viewing Workstations at Every Stage of the Imaging Workflow

Imaging Workflow Component	Common Cybersecurity Vulnerabilities	Recommended Security Measures
Acquisition Equipment (CT, MRI, X-ray, Ultrasound, etc.)	a) Outdated operating systems and firmware b) Default passwords c) Unauthorized physical access d) Malware infections via USB devices	a) Regular firmware and software updates b) Change default credentials and enforce strong passwords c) Multi-factor authentication where possible d) Disable unnecessary ports and services e) Restrict USB access and use endpoint protection f) Physical security controls and access logging
Communication Networks	a) Data interception during transmission b) Man-in-the-middle attacks c) Network eavesdropping d) Unauthorized network access	a) Encrypt data in transit using TLS/SSL and VPNs b) Implement secure DICOM communication c) Network segmentation and VLANs d) Firewalls and Intrusion Detection/Prevention Systems e) Continuous network monitoring and traffic analysis
PACS Servers	a) Unauthorized access to patient images b) Weak authentication mechanisms c) Ransomware attacks d) Data tampering or deletion	a) Role-Based Access Control b) Multi-factor authentication c) Encryption of stored data d) Regular security patching and vulnerability assessments e) Backup and disaster recovery plans f) Audit trails and log monitoring

Cloud Repositories	a) Misconfigured cloud storage b) Data breaches c) Unauthorized third-party access d) Insider threats	a) End-to-end encryption for stored and transmitted data b) Secure cloud configurations following HIPAA/GDPR standards c) Identity and Access Management policies d) Data Loss Prevention solutions e) Regular cloud security audits and compliance checks f) Backup and redundancy mechanisms
Viewing Workstations (Radiologist and Clinician Terminals)	a) Malware and phishing attacks b) Unauthorized user access c) Screen data exposure d) Vulnerable software applications	a) Endpoint Detection and Response solutions b) Strong authentication and MFA c) Automatic screen locking and session timeouts d) Application whitelisting e) Regular software updates and patch management f) User cybersecurity awareness training

Note: CT = Computed Tomography, USB = Universal Serial Bus, TLS = Transport Layer Security, SSL = Secure Sockets Layer, VPNs = Virtual Private Networks, DICOM = Digital Imaging and Communications in Medicine, VLANs = Virtual Local Area Networks, PACS = Picture Archiving and Communication Systems, HIPAA = Health Insurance Portability and Accountability Act, GDPR = General Data Protection Regulation, MFA = Multi-Factor Authentication.

The acquisition devices are used to encrypt communications and stored data and authenticate users at each step of the operation, maintaining and keeping an eye on all security changes and actions and then putting backup and disaster recovery plans into place. The risk of data breaches, ransomware attacks, unauthorized access and patient privacy violations in medical imaging systems is greatly decreased by this tiered strategy.

Related Work

The introduction offers a concise summary of the importance of cybersecurity in the healthcare industry, specifically focusing on its relevance to medical imaging. The review article delineates the goals and extent of the study, emphasizing the significance of encryption, anomaly detection and strategic defenses in reducing cyber risks and protecting patient data. In this study, a comprehensive framework is introduced that consists of many layers and integrates intrusion detection, access control and encryption algorithms (22). The purpose of this framework is to enhance the security of medical imaging equipment and data repositories. The framework's comprehensive approach to cybersecurity guarantees all-encompassing protection against a broad spectrum of threats. An overview on various encryption techniques based on latest security

standard protocols is proposed that are intended to improve the security of medical pictures when they are transferred via Internet of medical things networks (23). The algorithm demonstrated robust encryption capabilities while minimizing computational overhead, making it suitable for resource constrained Internet of medical things devices. The effectiveness of leveraging big data analytics and machine learning algorithms to identify patterns of suspicious activity and potential security breaches in medical imaging workflows has been demonstrated (24). By analyzing vast amounts of data from diverse sources, security analytics systems enable proactive threat detection and response. In order to identify unwanted access and unusual activity inside Internet of medical things networks, a comparative narrative assessment of machine learning-based anomaly detection frameworks is suggested (25).

The study examines the important matter of cybersecurity in the field of medical imaging, with a specific emphasis on encryption, anomaly detection and strategic defense methods (26). The methods in this study achieved excellent detection accuracy and minimized false positive rates by using anomaly detection algorithms that were trained on extensive medical imaging datasets. This review seeks to assess the paper's

contribution, relevance and efficacy in addressing the issues encountered by healthcare institutions in safeguarding sensitive medical data. The article offers a thorough examination of the security concerns that exist within the Internet of medical things environment. It emphasizes the potential

dangers of breaches in confidentiality, compromises in integrity and interruptions in availability. Various studies on cyber security in healthcare have been presented as shown in Table 2.

Table 2: Various Studies on Cybersecurity in Healthcare

Methods and Models	Evaluation Approach	Year	References
Utilizing hybrid optimization techniques with cryptographic encryption to enhance the security of medical images in the Internet of Things.	Performance metrics, Security analysis	2020	(26)
Context-sensitive access in IIoT healthcare applications	Usability testing, Security analysis	2018	(27)
Ensuring the security of Internet of Things devices in the era of machine learning and software-defined networking.	Performance metrics, Threat modelling	2018	(28)
A system for synchronizing time in a femtocell network using clusters.	Simulation, Performance metrics	2015	(29)
Image encryption scheme based on Signcryption technique with adaptive Elephant Herding Optimization	Peak Signal to Noise Ratio and Mean square errors.	2019	(30)
An advanced hybrid image watermarking approach is proposed for both medical and non-medical photos, using the DWT and Two-Dimensional SVD.	Security analysis, Performance metrics	2019	(31)
Encryption algorithms in colour images	Security analysis, Performance metrics	2019	(32)
An image encryption technique is developed by combining composite chaos and hyper chaos with DNA coding.	Security analysis, Performance metrics	2020	(33)
Designing a secure picture encryption technique with a unique S-box based on chaos theory.	Security analysis, Performance metrics	2017	(34)
Image encryption approach using combinational permutation techniques	Security analysis, Performance metrics	2006	(35)
Securing the Internet of healthcare	Usability testing, Security analysis	2018	(36)
Security and privacy issues in Internet of Things	Risk assessment, Security analysis	2024	(37)
Ensuring the safety and confidentiality of data in the medical Internet of Things	Literature review, Risk assessment	2018	(38)
The AES technique with CBC mode is used for encrypting images	Performance metrics, Security analysis	2024	(39)

Note: IIoT = Industrial Internet of Things, DWT = Discrete Wavelet Transform, SVD = Singular Value Decomposition, DNA = Deoxyribonucleic Acid, AES = Advanced Encryption Standard, CBC = Cipher Block Chaining.

The literature review part explores the fundamental principles and technologies that form the basis of cybersecurity in medical imaging. It examines the evolution of encryption algorithms and standards, the principles of anomaly detection

and the strategic frameworks for cybersecurity risk management. Key studies and advancements in the field are critically analyzed to provide a comprehensive understanding of current practices and challenges.

Emerging Cybersecurity Challenges in Medical Imaging

This section explores the role of encryption in securing medical imaging data, both at rest and in transit. It discusses various encryption techniques, including symmetric and asymmetric encryption, as well as their applicability and limitations in the healthcare context. Case studies and real-world examples illustrate the implementation of encryption protocols and best practices for ensuring data confidentiality and integrity. Encryption stands out as a fundamental method for safeguarding sensitive medical data in cloud environments. Several frameworks have been developed to address encryption's role in securing medical data. For instance, a steganography-based approach is proposed to conceal medical records, albeit with limitations in embedding capacity (40). Additionally, a convergent encryption algorithm was introduced to minimize data duplication, albeit with potential trade-offs in image quality (41). The Advanced Encryption Standard (AES) algorithm is advocated to encrypt data blocks, ensuring privacy and preventing accidental disclosures (42). Moreover, a study explored a hybrid cryptosystem incorporating visual cryptography and Rivest Shamir Adleman (RSA) algorithm to enhance data security while providing ease of access for authorized users (43). These encryption techniques offer varying degrees of security and efficiency, catering to diverse privacy requirements in medical imaging. A comprehensive survey of emerging cybersecurity challenges in medical imaging is presented (44). While echoing the importance of encryption, this survey extends the discussion to encompass novel strategies such as anomaly detection and strategic defenses. Drawing on recent advancements in cybersecurity technologies, it also offers insights into proactive measures that complement encryption techniques in safeguarding medical imaging data. The paper makes a valuable contribution to the ongoing discussion on cybersecurity in healthcare by tackling current obstacles and suggesting creative remedies.

The research delves into the critical realm of safeguarding medical imaging data against cyber threats (45). The authors highlight encryption measures as a cornerstone strategy to fortify the security posture of medical institutions.

Encryption emerges as a paramount defense mechanism, serving as a robust deterrent against unauthorized access and interception of sensitive patient information. In this study, author emphasize the significance of using advanced encryption methods to guarantee the secrecy and accuracy of medical imaging data. Healthcare firms may enhance their defenses and reduce the dangers of data breaches by using sophisticated encryption techniques (46). Moreover, the authors highlight the crucial need for encryption in healthcare, namely in complying with rigorous regulations like the Health Insurance Portability and Accountability Act (HIPAA). Compliance with regulatory frameworks necessitates the implementation of robust encryption protocols to safeguard patient privacy and uphold data security standards. This study elucidates on the multifaceted benefits of encryption in medical imaging cybersecurity. Beyond protecting against external threats, encryption also fosters trust among patients by assuring them of the confidentiality of their medical data. Moreover, encryption serves as a proactive measure to preemptively mitigate potential risks, thereby enhancing the resilience of healthcare systems against evolving cyber threats.

Anomaly Detection in Medical Imaging Cybersecurity

Anomaly detection is examined as a proactive approach to identifying irregular patterns or behaviors indicative of cyber threats within medical imaging systems. This section evaluates the effectiveness of machine learning algorithms, statistical methods and anomaly detection frameworks in detecting and responding to security breaches. Practical considerations and implementation challenges are discussed, along with recommendations for optimizing anomaly detection strategies. In addition to encryption, anomaly detection systems are essential for recognizing and mitigating cybersecurity risks in medical imaging. Despite the presence of computational burdens, homomorphic encryption as a method for doing calculations on encrypted data is developed (47). Meanwhile, authors advocated for a multi-cloud environment coupled with segmentation and watermarking techniques to ensure data integrity and prevent unauthorized access. The usage of visual cryptography for

securing cloud storage leads to emphasizing its computational efficiency and ability to reduce security risks. Anomaly detection is pivotal for fortifying cybersecurity within medical imaging, with several studies investigating its application. A case study on real-time anomaly detection in MRI image transmission in conjunction with Leveraging Network Intrusion Detection Systems (NIDS) and anomaly detection algorithms, highlights effective measures for detecting and mitigating cybersecurity threats during MRI image transmission, ensuring data integrity and confidentiality (48). A statistical analysis-based approach for anomaly detection in medical imaging workstations is proposed (49). This study employs anomaly score computation and hypothesis testing to detect deviations in user activities, contributing novel insights to workstation security enhancement strategies (49). Through Convolution Neural Networks and Recurrent Neural Networks, the researchers demonstrate robust performance in identifying unauthorized access and data breaches within PACS systems, offering significant advancements in medical imaging cybersecurity (50). Immutable backups and disaster recovery procedures are kept for PACS and cloud-based repositories to guarantee quick restoration of medical images and patient records without having to pay ransom demands. The possibility of ransomware execution is further decreased by endpoint protection, application whitelisting and anti-malware software on viewing workstations. The study shows the effectiveness of supervised and unsupervised algorithms in identifying suspicious network behavior, contributing valuable insights into cybersecurity enhancement.

Strategic Defenses and Risk Management

The concluding part of the document centers on strategic defenses and risk management

procedures designed to strengthen the cybersecurity position of medical imaging settings. The text examines the significance of thorough risk assessments, cybersecurity policies and incident response methods in reducing cyber hazards. The text emphasizes the strategies for promoting cooperation among healthcare stakeholders and adjusting to changing risks. In this systematic study, the use of blockchain technology to enhance security in medical imaging is examined. Their research investigates the capacity of blockchain technology to enhance the reliability and privacy of data in healthcare environments (51). The study provides a thorough evaluation of current research, highlighting the advantages and disadvantages of using blockchain technology to secure medical imaging data. It offers significant insights that may guide future advancements in exploring machine learning techniques specifically designed for enhancing cybersecurity in the field of medical imaging. The researchers examine several approaches in machine learning and investigate how they may be used to identify and reduce cyber dangers in medical imaging systems. The review provides valuable insights into the efficacy of machine learning algorithms in bolstering cybersecurity measures, hence contributing to the protection of patient data and medical imaging (52). A thorough literature study has been performed in the past on strategic defenses against cyber threats in the field of medical imaging. The review examines novel tactics and technology designed to enhance cybersecurity defenses in healthcare systems (53) and an extensive evaluation of anomaly detection systems specifically designed for cybersecurity in the field of medical imaging (54). The research assesses the effectiveness and efficiency of several anomaly detection methods in identifying and reducing cyber risks as shown in Table 3.

Table 3: An Examination of Techniques for Processing Large Datasets to Identify Abnormal Patterns Using Machine Learning

Domain	Finding	ML Techniques	References
Telecommunication and Mobile Network	Analyzing security logs to get information may be a complex task.	Unsupervised Clustering using the Expectation-Maximization technique, Supervised linear classification and the WEKA program.	(55)

Telecommunication and Mobile Network	Current frameworks lack integration of group user profiling, essential for targeted malware detection.	K-means clustering, Markov models	(56)
Telecommunication and Mobile Network	Analyzing streaming data for anomalies using a pipeline based on Pearson correlation.	Pipeline for Pearson correlation	(57)
Network Traffic	High traffic volumes delay threat detection, affecting scalability, accuracy and memory consumption.	DDoS detection based on clustering algorithm	(58)
Network Traffic	Excellent trade-off between attack detection and false-positive rates	Three Classification algorithms and two anomaly detection methods	(59)
Smart Grid	Offline detection methods need extensive training data sets.	Periodic auto-regression with an exogenous variable	(60)
Cloud Environment	The surge in network traffic data overwhelms the current infrastructure, making computations more complex.	Naïve Bayes, Decision Tree, Support Vector Machine	(61)

Note: WEKA = Waikato Environment for Knowledge Analysis.

A recent study highlights the dominance of machine learning models among various anomaly detection techniques, noting the challenge posed by increasing network traffic due to the complex computations required (62). The suggested methodology utilizes Hadoop, HDFS, Map Reduce, cloud architecture and machine learning methods to improve the efficiency of anomaly detection. The accuracy and efficiency of the model were assessed using the WEKA interface, using the Naive Bayes, Decision Tree and Support Vector Machine algorithms. Nevertheless, the incorporation of cloud infrastructure and real-time data streaming was insufficiently resolved. The study addressed the difficulties of identifying abnormalities in real-time data, with a focus on universality and scalability (62). They presented a new method for detecting anomalies online by using entropy and Pearson correlation measurements. To tackle the issues of generality and scalability, large data streaming components were used effectively (63). However, the limits of the data processing include the complexity of the procedures involved and the longer length required for periodic batch processing. It has been noted in the literature that current anomaly detection methods for smart grids were mostly offline and required substantial amounts of energy. Their advocacy focused on the implementation of real-time detection while minimizing energy use (60). Their suggested solution used an in-memory distributed frame-

work that integrated existing architecture (63). This design facilitates scalable live streaming for real-time anomaly detection. However, the framework required a prolonged period of training, resulting in the unsettled scheduling of real-time jobs.

Related Reviews/Surveys and Contributions

Numerous surveys and reviews have scrutinized the landscape of cybersecurity in healthcare (64-66). The recent study highlighted vulnerabilities across software, hardware and network layers, emphasizing the susceptibility of emerging technologies like cloud computing and smart-phone applications (64). A comprehensive study has been performed on implanted medical devices, with a particular focus on security, privacy issues and patient safety (65-66). Similarly, the research provided insights into IoT-enabled health technology, covering network architectures, industry development and privacy/security considerations (67). Several other studies focused on specific aspects of cybersecurity in healthcare, such as authentication taxonomy access control for implantable devices (68) and cyber threats classification (69, 70). Additionally, bibliometric analyses (71) and systematic literature reviews (72) shed light on publication trends, research gaps and security/privacy concerns in Electronic Health Record (EHR) systems (73). Our contribution lies in consolidating and extending

upon existing knowledge. We introduce a comprehensive data flow model tailored to identify and mitigate cyber-attacks in the medical domain. Moreover, we categorize cyber-attacks specific to medical systems, offering insights into their strengths and limitations. We classify medical cybersecurity architectures across different systems, facilitating targeted solutions to cybersecurity challenges. By analyzing the advantages and drawbacks of various architectures, we provide actionable recommendations for securing intelligent medical systems, electronic medical records and healthcare facilities. Furthermore, we present a comparative analysis of cybersecurity architecture capabilities, aiding in the recommendation of suitable solutions. Finally, we offer a comprehensive conclusion encompassing all facets of our survey, along with discussions on prospects in medical imaging cybersecurity.

When it comes to protecting medical imaging equipment from cyberattacks, vulnerabilities like Denial of Service (DoS) and remote code execution present substantial risks. These vulnerabilities may enable malicious individuals to influence crucial system data, such as modifying the amount of medicine for patients. A notable risk involves hackers sending deceptive commands to insulin pumps, potentially leading to fatal insulin overdoses in diabetic patients. Addressing these vulnerabilities is crucial, as shown by several proposed solutions targeting operation device attacks. The article identified and proposed mitigation strategies for backdoors in software systems, focusing specifically on Drop bear SSH vulnerabilities (74). Their findings indicate that it is possible to identify critical decision-making components within the SSH server, thereby reducing the risk of unauthorized access. The work is extended to create an algorithm that can categorize network data to identify malicious activity by solving equations related to traffic parameters (74). A machine learning-driven intrusion detection system is then developed to detect DoS assaults on Wi-Fi networks (75). This method, distinguished by its exceptional accuracy and completeness, does not need any alterations to the protocol. To strengthen the firewall's protection against DoS assaults, FR-Win Firewall was developed, which utilizes fuzzy reasoning to improve its efficacy (76). This sophisticated

firewall system has shown success in the design, implementation and testing stages, providing a strong solution for preventing DoS attacks. A further development was a Markov game framework to address DoS vulnerabilities where the author used a modified Nash Q-learning technique to solve Bellman equations and enhance the security of wireless networks (77). This strategy is efficient; however, it still has difficulties in completely protecting wireless settings. The Shar LK, Tan HB solution uses Software-Defined Networking (SDN) to identify DoS threats by examining typical attack patterns in Open Flow infrastructures. Although this strategy is efficient, it may unintentionally give rise to other categories of DoS assaults (78). The solution to this is depicted by creating a prototype to establish limits and create regulations for Java Server Page (JSP) applications (79). They assessed the prototype using four JSP programs. Although this approach can detect XSS attacks without changing client-driven components, its ability to do so is limited by time-consuming policy investigations. The researchers proposed an innovative server-side approach to identify XSS attacks by using XML Schema Definition (XSD) and XML to enforce schema rules, efficiently identifying harmful JavaScript code (80). Nevertheless, the method's substantial server-side prerequisites may have an adverse effect on the performance of open networks.

To find and validate DOM-based XSS vulnerabilities, DEXTERJS testing platform was introduced (81). This platform can detect previously unknown DOM XSS activities, sometimes known as zero-day vulnerabilities, in both benchmark tests and real-world scenarios. Nevertheless, this method has difficulties in recognizing the initial purpose of the client side, which might potentially include harmful code. A study on Cross-Site Request Forgery (CSRF) vulnerabilities was conducted (82), where they examined several protection strategies to develop a strong defense against CSRF attacks. However, their technique does not have explicit experimental verification, which means that complete protection has not been accomplished and more enhancements are required. Several approaches have been suggested to identify CSRF vulnerabilities in online applications, recommending users to

install a simple extension to get warnings about possible CSRF dangers. Nevertheless, this extension just notifies users without offering direct protection against CSRF. A protective framework for cross-site scripting (XSS) enhances user defenses against XSS assaults and is compatible with many website technologies, including PHP and ASP (83). The efficacy of this schema is constrained by its dependence on anticipated behavioral patterns, resulting in erroneous negative alarms.

A context-sensitive purification technique for protecting against XSS attacks in cloud computing identified different types of online applications and improved the effectiveness of purifiers for web application variables (84). When tested in real-world situations, this technique demonstrates a high rate of correctly identifying positive cases and a low rate of incorrectly identifying negative cases. However, it does not have the capability to interact with Online Social Networks (OSNs). The XSS protection method has been later enhanced for cloud platforms to safeguard virtual machines from XSS attacks. This method does not necessitate any alterations to the web application's browser source code and offers a low occurrence of both false-positive and false-negative results. The improvement in this work, however, does not currently provide support for OSN but efficiently terminates unauthorized sessions in a timely manner (85). It should also be noted that this approach just focuses on identifying reflected CSRF attacks and does not address login CSRF assaults.

Anomaly detection is essential for enhancing cybersecurity measures in the field of medical imaging. This section explores relevant studies that delve into the application of anomaly

detection techniques to enhance the security of medical imaging systems, complementing the insights presented in the paper Enhancing Cybersecurity in Medical Imaging: Encryption, Anomaly Detection and Strategic Defenses.

Various Methods for Cyber-attacks

Securing medical imaging systems against emerging cyber threats presents unique challenges, particularly regarding the vulnerabilities posed by ubiquitous and relatively immature safeguard inherent in medical devices. The proliferation of interconnected medical devices, including imaging systems, introduces significant security risks due to their extensive use and evolving technological landscape. As medical devices continue to evolve, their integration into healthcare networks raises concerns about their susceptibility to cyber-attacks. This equipment, such as medical imaging systems, often lack robust security safeguards, leaving them susceptible to exploitation by malevolent individuals aiming to breach patient data, disrupt healthcare operations, or even jeopardize patient safety. The importance of these security threats is emphasized by the growing interconnectivity of healthcare systems, where hacked devices might act as gateways for larger cyber-attacks that aim at key medical infrastructure (86). Consequently, ensuring the security of medical imaging systems requires a multi-faceted approach that addresses vulnerabilities at various levels, including device hardware, software, network infrastructure and user practices. Existing research and industry efforts have recognized the need to enhance cybersecurity measures for medical devices, including imaging systems as shown in Table 4.

Table 4: Overview of Common Machine Learning and Deep Learning Algorithms in Cybersecurity

Method	Working Principle	Advantages	Disadvantages
Decision Tree	A classification model structured as a tree, trained using information gain from features in training data	Low computational cost, simple to implement	Requires storage of all model information, leading to high space complexity
Support Vector Machine	A hyperplane is identified in feature space to segregate classes, with the objective of maximizing the distance from the closest data points.	Effective for small samples with many features	Challenging to determine the optimal kernel size (k-value)

Naive Bayes Classifier	Determines the class's posterior probability from supplied data using Bayes' theorem	Handles noisy data well, easy implementation, maintains performance with small samples	Assumes feature independence, which is often unrealistic in practical scenarios
Artificial Neural Network	Comprises one or more hidden layers between input and output, storing input data as weights using backpropagation	High accuracy for pattern recognition tasks	Higher computational complexity compared to other methods
K - Means Clustering	Forms clusters among data points based on similarity	Simple to implement, ideal for problems with difficult labeling	Requires domain knowledge to select the initial k-value
Convolutional Neural Network	Extracts features from data through a convolution layer, uses hidden and pooling layers for output prediction	Excellent for image classification and pattern recognition	Computationally intensive, performance drops with small sample sizes
Recurrent Neural Network	Analyzes sequential data by integrating temporal layers	Performs well for sequential data tasks, such as speech and text	Suffers from vanishing or exploding gradient issues
Restricted Boltzmann Machine	An unsupervised model limiting connections within the same layer, between visible and hidden layers	Utilizes a feedback mechanism to extract key features in unsupervised learning	Very high computational cost
Deep Belief Network	Composed of stacked RBMs, performing layer-by-layer training for enhanced performance	Outperforms Restricted Boltzmann Machine by stacking it on each layer's training data	Very high computational cost due to numerous parameters

Even with all these thorough approaches, these studies might not cover every facet of cybersecurity in medical imaging. Although the suggested frameworks and protocols are made to be flexible, their efficacy may differ in various healthcare settings and technological environments due to the size of the field and the quick evolution of cyber threats. As a result, some niche areas or new challenges may not have been thoroughly explored. Generalizing the findings to all medical imaging systems worldwide may not be feasible without considering contextual factors and infrastructure differences (87). Although the research proposes innovative methodologies, their real-world efficacy has yet to be fully validated through extensive empirical testing. Practical implementation and performance evaluation in diverse healthcare contexts are essential to ascertain the scalability and reliability of the proposed solutions. The development and testing of encryption frameworks, anomaly detection

protocols and strategic defenses require significant resources in terms of time, expertise and infrastructure. Limitations in access to such resources may impact the depth and breadth of the study's findings. Given the dynamic nature of cybersecurity threats, the findings of this study may become outdated over time. Continuous monitoring and adaptation to emerging threats are necessary to ensure the relevance and applicability of the proposed solutions in the long term.

Based on the cybersecurity needs and workflow features documented in the literature, a qualitative evaluation was carried out to analyze the consistency of the various cybersecurity frameworks across various medical imaging modalities. Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Ultrasound (US), Mammography, Nuclear Medicine and Digital Radiography (DR) were the six main imaging modalities taken into consideration, as depicted in Table 5.

Table 5: Summary of the Applicability of the Cybersecurity Framework Components Across the Different Imaging Modalities

Security Component	CT	MRI	Ultrasound	Mammography	Nuclear Medicine	Digital Radiography
Device Hardening	✓	✓	✓	✓	✓	✓
Secure Communication	✓	✓	✓	✓	✓	✓
PACS Protection	✓	✓	✓	✓	✓	✓
Cloud Security	✓	✓	✓	✓	✓	✓
Access Control & MFA	✓	✓	✓	✓	✓	✓
Ransomware Protection	✓	✓	✓	✓	✓	✓
Audit Logging	✓	✓	✓	✓	✓	✓

Note: CT = Computed Tomography, MRI = Medical Resonance Imaging, PACS = Picture Archiving and Communication Systems, MFA = Multi-Factor Authentication.

The evaluation offers a cybersecurity architecture that is independent of modality and can safeguard a variety of medical imaging systems while meeting operational needs unique to each modality.

Discussion

While various techniques exist to mitigate privacy and security risks in cloud-based medical imaging, their practical implementation remains complex, especially concerning the management of large datasets. As such, future research should focus on addressing these complexities and aligning security measures with the unique requirements of the healthcare domain. Analyzing the security landscape surrounding medical imaging systems reveals an urgent need for robust anomaly detection mechanisms capable of processing real-time big data. A report by Cisco highlights the exponential growth of Internet protocol (IP) traffic, with a forecast of 2.3 Zettabytes traversing the Internet by 2020, a significant increase from previous years. In addition, the increasing number of non-PC devices, such as smart gadgets, is causing a significant increase in the amount and diversity of data. This presents difficulties for current security analytics systems in promptly identifying and addressing potential risks. The vulnerability of non-PC devices was demonstrated in large-scale attacks targeting prominent organizations via smart home devices in 2016, signaling the critical importance of real-time monitoring (64).

Organizations are allocating significant resources to security expenses as they confront the

increasing challenges posed by cybersecurity threats. According to Gartner, global security expenditure is expected to reach \$96 billion by the end of 2018. This increase is a result of enterprises being more aware of security threats and realizing that current solutions are not effective in preventing assaults. The U.S. Federal Cybersecurity Industry Forecast highlights the need of investing in cybersecurity, predicting that the industry will be worth \$22 billion by 2022. Deep Learning algorithms are becoming more important in the field of cybersecurity due to the rise of new threats. In the next five years, these technologies are expected to replace conventional Security Information and Event Management (SIEM) systems, introducing a new era of security solutions powered by machine learning. Furthermore, data stream processing is recognized as a rapidly growing field of study, providing immediate analysis of constantly moving data streams originating from external sources. Use case examples highlight the need of detecting anomalies in real-time across several domains. In contemporary network traffic situations, IoT infrastructures produce extensive sensor data, requiring immediate monitoring to identify anomalous activity. The increasing availability of mobile cloud services highlights the need of processing data in real-time to guarantee the reliability and protection of confidential information stored in the cloud (65).

Autonomous vehicles present a unique security challenge, with connected devices vulnerable to malicious attacks. Real-time anomaly detection is crucial for detecting abnormalities in car modules

and assuring the safety and dependability of autonomous systems. In healthcare settings, the use of real-time anomaly detection allows for proactive monitoring of patient services, which in turn enables prompt interventions and ultimately leads to improved patient outcomes. Real-time anomaly detection has numerous uses, such as detecting insider trading in financial markets and ensuring the safety of important systems. Organizations may reduce financial risks and protect against possible threats by identifying abnormal trade activity and illegal access attempts in crucial systems. The authors successfully emphasize the requirement of strong security measures to protect patient data by highlighting the significance of access control, identity management and authentication in Internet of medical things networks. Furthermore, the article provides in-depth analyses about the significance of security analytics and public key infrastructure in addressing vulnerability concerns and guaranteeing data encryption. The authors' dedication to improving cybersecurity in healthcare is evident in the use of encryption algorithms specifically designed for medical imaging, such as the Shufe Encryption Algorithm (SEA) and hybrid encryption models. In addition, the examination of previous studies and suggested approaches enhances the study by providing a thorough insight into the present condition of cybersecurity in medical imaging and possible directions for future investigation. The article has a clear and organized framework, with distinct parts that effectively direct the reader through the discourse. The language used is easily comprehensible, making the intricate notions of cybersecurity accessible to a broad spectrum of individuals. Incorporating figures and tables in the article helps to illustrate important ideas and improve the overall clarity of the content (66).

Additional inquiry is necessary to explore the use of blockchain technology to enhance the security and reliability of medical imaging data. The research should prioritize assessing the capacity of block chain technology to provide unchangeable and tamper-resistant storage for medical pictures, while also enabling safe and verifiable access control methods in healthcare settings. Further investigation is needed to examine cooperative cybersecurity frameworks that promote the

exchange of information and cooperation among healthcare institutions, technology suppliers, regulatory agencies and cybersecurity specialists. This may include the creation of established procedures and optimal strategies for exchanging threat information, coordinating incident responses and implementing collective defenses against new cyber threats. Research should further consider the usability and human factors elements of cybersecurity solutions used in medical imaging systems.

This includes investigating user perceptions, acceptance and adoption of security measures, as well as designing intuitive interfaces and training programs to enhance cybersecurity awareness and compliance among healthcare professionals. Given the regulatory landscape surrounding healthcare data security, future research should focus on evaluating the impact of regulatory compliance requirements, such as HIPAA regulations, on the design and implementation of cybersecurity measures in medical imaging systems. This includes assessing the alignment of existing security frameworks and standards with regulatory mandates and identifying areas for improvement. Research should aim to quantify the cybersecurity risks and impacts associated with potential security breaches in medical imaging systems. This involves conducting comprehensive risk assessments, vulnerability analyses and impact assessments to quantify the financial, operational and reputational consequences of cybersecurity incidents in healthcare organizations.

Cybersecurity in medical imaging systems faces threats like information collection attacks, database intrusions, website compromises and operational device breaches. These vulnerabilities allow malicious actors to engage in forgery, data manipulation and breaches, which can severely compromise patient privacy and negatively impact treatment efficacy. Information Collection Attacks: Influenced by the MS17-010 security update and Open SSH vulnerabilities, such attacks can allow full control over medical equipment. The MS17-010 vulnerability is notably prevalent, with methods like API sequences of ransomware and alternative designs focusing on decoupled architecture and usable security being suggested to mitigate this issue. Despite their high detection

capabilities, these methods often inherit poor system performance. OpenSSH vulnerabilities enable attackers to access patient information directly, where cryptographic keys and RSA algorithms are recommended to lower the success rate of these attacks, although challenges remain in optimizing resource use and data transfer rates. Website Attacks: Medical websites, essential for various functions and data transmissions, are susceptible to session hijacking, CSRF and XSS attacks. Proposed solutions include mathematical methods for XSS detection and various CSRF countermeasures, though they often suffer from high resource consumption and limited applicability to the medical domain, leaving systems vulnerable to other attack vectors.

Databases storing patient and hospital information face threats like password intrusions, vulnerability exploits and SQL injections, with the latter being particularly hazardous. There is a critical need for innovative solutions beyond current measures to enhance database security. Operational Device Attacks i.e., Attacks on medical devices, often through the Drop bear SSH server and DoS attacks, involve executing malicious code to alter device operations, potentially endangering patient safety. Future research must focus on CSRF solutions to secure operational devices, improving efficiency and system performance.

The future emphasis should be on developing low-cost, efficient architectures to enhance transmission efficiency and data confidentiality. New detection methods are essential to address backdoors, DoS and ransomware attacks, which currently suffer from poor performance and pose significant risks to patient safety. Enhancing awareness and preventive measures for database security is crucial to mitigate potential attacks from their inception.

Conclusion

The research survey highlights the crucial significance of implementing a comprehensive strategy for cybersecurity in the field of medical imaging. By integrating encryption, anomaly detection and strategic defenses, healthcare organizations can establish robust layers of protection against evolving cyber threats. Through the development of bespoke encryption frameworks and the introduction of novel anomaly

detection protocols, the research demonstrates tangible advancements in securing medical imaging systems. These enhanced security measures not only mitigate current vulnerabilities but also provide a proactive stance against future threats.

This study highlights that a single security method is insufficient to secure medical imaging equipment. Technical, organizational, operational and regulatory controls must all cooperate in a multifaceted, defense-in-depth strategy. Strong encryption for data in transit and at rest, multi-factor authentication, role-based access control, secure communication protocols, network segmentation, endpoint protection, vulnerability management, ongoing monitoring and intrusion detection systems are all crucial technical measures to lessen the possibility and impact of cyberattacks. The security of DICOM-based communication and PACS environments also need special attention because flaws in imaging workflows could jeopardize patient data and clinical operations. When relevant, adherence to laws like HIPAA and GDPR should be seen as part of a larger plan for safeguarding patient privacy, data integrity and system availability rather than just as a compliance duty.

The protocols and frameworks proposed in literature empower healthcare providers to safeguard patient data with confidence. The ability to identify anomalies in real-time allows for quick identification and resolution of possible cyber threats, protecting the security and privacy of medical imaging data. By delving into the realm of advanced persistent threats and devising proactive strategies for risk management, the research equips healthcare organizations with the tools to anticipate and mitigate emerging cybersecurity challenges. By addressing pressing cybersecurity challenges, the research aims to bolster patient outcomes and foster trust in digital healthcare ecosystems. While the study makes substantial strides in enhancing cybersecurity in medical imaging, several avenues for future research and development remain. Continued exploration of emerging threats, refinement of encryption protocols and optimization of anomaly detection algorithms represent areas ripe for further investigation.

The comparative analysis shows that accessibility and efficiency have been greatly enhanced by the growing integration of modalities like CT, MRI, X-ray, ultrasound and nuclear imaging with PACS, cloud platforms, EHRs and Internet-connected medical devices. However, this interconnected ecosystem has also increased the attack surface and made medical imaging infrastructures vulnerable to an increasing number of cyber threats, such as malware, ransomware, unauthorized access, data breaches, denial-of-service attacks, insider threats, adversarial manipulation of medical images and attacks against networked imaging devices.

There are still a few obstacles to overcome despite tremendous progress. New vulnerabilities will continue to be introduced by the quick uptake of cloud-based imaging, telemedicine, Internet of Medical Things devices, AI-assisted diagnostics, remote radiology services and more interconnected healthcare infrastructures. Security implementation is further complicated by the need to sustain continuous clinical services, interoperability requirements, limited cybersecurity budgets, diverse vendor environments and legacy equipment.

In the end, cybersecurity in medical imaging should be seen as both an information-technology duty and a crucial part of patient safety and healthcare quality. Therefore, throughout the whole lifecycle of medical imaging data and systems, a robust medical imaging ecosystem must guaranty the concurrent protection of confidentiality, integrity, availability, authenticity, privacy and clinical dependability.

Future research should prioritize multidisciplinary cooperation among cybersecurity specialists, healthcare practitioners, data scientists and policymakers to effectively tackle the intricate difficulties arising from the convergence of medical imaging and cybersecurity. This cooperative method may expedite the creation of groundbreaking solutions, well-informed rules and exemplary practices for ensuring the security of medical imaging systems and protecting the privacy and reliability of patient data.

Abbreviations

AES: Advanced Encryption Standard, CSRF: Cross-Site Request Forgery, EHR: Electronic Health

Record, HIPAA: Health Insurance Portability and Accountability Act, MCPS: Medical Cyber-Physical Systems, NDS: Network Detection System, PACS: Picture Archiving and Communication Systems, RSA: Rivest Shamir Adleman, SEA: Shufe Encryption Algorithm, XSD: XML schema definition.

Acknowledgement

We would like to thank the International Research Journal of Multidisciplinary Scope for considering our research review article.

Author Contributions

All the authors have equally contributed to the work.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Data Availability

The data are publically accessible, however upon reasonable request, the corresponding author may make the processed data available.

Declaration of Artificial Intelligence (AI) Assistance

The authors declare that Generative AI tools were used only for language refinement and grammatical corrections. Generative AI tools were not used to generate the research ideas, methodology, results, analysis, or conclusions. The authors take full responsibility for the content, accuracy, originality and integrity of the manuscript.

Ethical Approval

Not Applicable.

Funding

None.

References

1. Hareland SA, Kramer M, Siddiqui S, Navers F, Kastanek B. See-saw commander/follower architecture for optimal control, safety and extensibility in a medical system. In 2017 IEEE International Systems Engineering Symposium (ISSE), Vienna, Austria. 2017;1–6. <https://doi.org/10.1109/SysEng.2017.8088261>
2. Ahmad A, Paul A, Rathore M M. An efficient divide-and-conquer approach for big data analytics in

- machine-to-machine communication. *Neurocomputing*. 2016; 174:439–453.
<https://doi.org/10.1016/j.neucom.2015.04.109>
3. Ahmed M, Naser Mahmood A, Hu J. A survey of network anomaly detection techniques. *J Netw Comput Appl*. 2016;60:19–31.
<https://doi.org/10.1016/j.jnca.2015.11.016>
 4. Pai V, Pai K, Manjunatha S, Hirmeti S, Bhat VV. Adaptive network anomaly detection using machine learning approaches. *EURASIP Journal on Information Security*. 2025;29.
<https://doi.org/10.1186/s13635-025-00216-4>
 5. Akoglu L, Tong H, Koutra D. Graph based anomaly detection and description: a survey. *Data Min. Knowledge Discovery*. 2015;29(3):626–88.
<https://doi.org/10.1007/s10618-014-0365-y>
 6. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity Challenges for PACS and Medical Imaging. *Acad Radiol*. 2020;27(8):1126–1139.
<https://doi.org/10.1016/j.acra.2020.03.026>
 7. Badrouchi F, Aymond M, Haerinia S. Cybersecurity Vulnerabilities in Biomedical Devices: A Hierarchical Layered Framework, in *Internet of Things Use Cases for the Healthcare Industry*, Raj, J. M. Chatterjee, A. Kumar and B. Balamurugan, Eds., Cham: Springer International Publishing. 2020;157–84.
https://doi.org/10.1007/978-3-030-37526-3_7
 8. US Food and Drug Administration. FDA warns patients and health care providers about potential cybersecurity concerns with certain Medtronic insulin pumps. 2019.
<https://www.prnewswire.com/news-releases/fda-warns-patients-and-health-care-providers-about-potential-cybersecurity-concerns-with-certain-medtronic-insulin-pumps-300876422.html>
 9. US Food and Drug Administration. Certain Medtronic MiniMed insulin pumps have potential cybersecurity risks: FDA safety communication. 2019.
<https://www.techtarget.com/healthtechsecurity/news/366594612/Certain-Medtronic-Insulin-Pumps-Pose-Healthcare-Cybersecurity-Risks-FDA-Says>
 10. Mirsky Y, Mahler T, Shelef I, Elovici Y. Malicious tampering of 3d medical imagery using deep learning. In *28th USENIX Security Symposium (USENIX Security19)*. 2019;461–78.
<https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky>
 11. Gillum J, Kao J, Larson J. Millions of Americans' medical images and data are available on the Internet. Anyone Can Take a Peek. *ProPublica*. 2019.
<https://www.propublica.org/article>
 12. Cohen IG, Hoffman S, Adashi EY. Your Money or Your Patient's Life? Ransomware and Electronic Health Records. *Ann Intern Med*. 2017;167(8):587–8.
<https://doi.org/10.7326/M17-1312>
 13. Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. *IEEE Commun Surv Tutor*. 2018;20(4):3453–95.
<https://doi.org/10.1109/COMST.2018.2855563>
 14. Alsubaei F, Abuhussein A, Shiva S. Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment, In *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*. 2017;112–120.
<https://doi.org/10.1109/LCN.Workshops.2017.72>
 15. Dimitrov DV. Medical Internet of Things and Big Data in Healthcare. *Healthc Inform Res*. 2016;22(3):156.
<https://doi.org/10.4258/hir.2016.22.3.156>
 16. Ching KW, Singh MM. Wearable Technology Devices Security and Privacy Vulnerability Analysis. *Int J Netw Secur Its Appl*. 2016;8(3):19–30.
<https://doi.org/10.5121/ijnsa.2016.8302>
 17. Mohzary M, Tadisetty S, Ghazinour K. A Privacy Protection Layer for Wearable Devices, In A. Benzekri A, Barbeau M, Gong G, Laborde R and Garcia-Alfaro J, (Eds). *Foundations and Practice of Security. Lecture Notes in Computer Science*. 2020;363–70.
https://doi.org/10.1007/978-3-030-45371-8_24
 18. Robert Vamosi. Hacking the Human Body SCADA System. In *Black Hat USA and DefCon Security Conferences*, Las Vegas. 2011.
<https://infocondb.org/con/black-hat/black-hat-usa-2011>
 19. Pelton J, Singh I. *Smart cities of today and tomorrow*. Cham: Springer International Publishing. 2019.
<https://link.springer.com/book/10.1007/978-3-319-95822-4>
 20. Stremlau T. The financial motivation to keep information secure. *Comput Fraud Secur*. 2020;2:18–9.
[https://doi.org/10.1016/S1361-3723\(20\)30020-8](https://doi.org/10.1016/S1361-3723(20)30020-8)
 21. Li Y, Quevedo DE, Dey S, Shi L. SINR-Based DoS Attack on Remote State Estimation: A Game-Theoretic Approach. *IEEE Trans Control Netw Syst*. 2017;4(3):632–42.
<https://doi.org/10.1109/TCNS.2016.2549640>
 22. HZhang H, Zhang H, Wang X, Yang Z, Zhao Y. Analysis of Requirements for Developing an mHealth-Based Health Management Platform. *JMIR MHealth UHealth*, 2017;5(8):e117.
<https://doi.org/10.2196/mhealth.5890>
 23. Guang Y. An Overview of Current Solutions for Privacy in the Internet of Things. *Front Artif Intell*. 2022;5:812732.
<https://doi.org/10.3389/frai.2022.812732>
 24. Mahler T, Shalom E, Makori A, Elovici Y, Shahrar Y. A Cyber-Security Risk Assessment Methodology for Medical Imaging Devices: The Radiologists' Perspective. *Journal of Digital Imaging*. 2022;35(3):666–77.
<https://doi.org/10.1007/s10278-021-00562-y>
 25. Thakur S, Bhatele M, Waoo A. A review of the Comparative Study of Anomaly Detection Techniques for Enhancing Security in AI-driven Medical Applications. *Next Research*. 2026;9:101744.
<https://doi.org/10.1016/j.nexres.2026.101744>
 26. Elhoseny M, Shankar K, Lakshmanaprabu SK, Maselena A, Arunkumar N. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. *Neural Comput Appl*. 2020;32(15):10979–93.
<https://doi.org/10.1007/s00521-018-3801-x>

27. Al-Turjman F, Alturjman S. Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Application. *IEEE Trans Ind Inform.* 2018;14(6):273-44.
<https://doi.org/10.1109/TII.2018.2808190>
28. Restuccia F, D'Oro S, Melodia T. Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. *IEEE Internet Things J.* 2018;1(1):4829-42.
<https://doi.org/10.1109/JIOT.2018.2846040>
29. Hasan MK, Saeed RA, Alsaqour RA, Ismail AF, Aisha HA, Islam S. Cluster-based time synchronisation scheme for femtocell network. *Int J Mob Commun.* 2015;13(6):567-98.
<https://doi.org/10.1504/IJMC.2015.072063>
30. Shankar K, Elhoseny M, Perumal E, Ilayaraja M, Sathesh Kumar K. An Efficient Image Encryption Scheme Based on Signcryption Technique with Adaptive Elephant Herding Optimization, in *Cybersecurity and Secure Information Systems. Advanced Sciences and Technologies for Security Applications.* Cham: Springer International Publishing. 2019;31-42.
https://doi.org/10.1007/978-3-030-16837-7_3
31. Araghi TK, Manaf AA. An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Future Gener Comput Syst.* 2019;101(C):1223-1246.
<https://doi.org/10.1016/j.future.2019.07.064>
32. Ghadirli H M, Nodehi A, Enayatifar R. An overview of encryption algorithms in color images. *Signal Process.* 2019;164(C):163-185.
<https://doi.org/10.1016/j.sigpro.2019.06.010>
33. Wan Y, Gu S, Du B. A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding. *Entropy.* 2020;22(2):171.
<https://doi.org/10.3390/e22020171>
34. Çavuşoğlu Ü, Kaçar S, Pehlivan I, Zengin A. Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos Solitons Fractals.* 2017;95:92-101.
<https://doi.org/10.1016/j.chaos.2016.12.018>
35. Mitra A, Subba Rao YV, Mahadeva Prasanna SR. Image encryption approach using combinational permutation techniques. *Security analysis Performance.* 2006;1(2):127-31.
https://www.researchgate.net/profile/A-Mitra/publication/228758228_A_new_image_encryption_approach_using_combinational_permutation_techniques/links/5b9cc03b299bf13e603184f2/A-new-image-encryption-approach-using-combinational-permutation-techniques.pdf
36. Mattioli M, Shackelford S J, Myers S, Brady A, Wang Y, Wong S. Securing the Internet of healthcare. *Minnesota Journal of Law, Science & Technology* 2018;405.
<https://www.repository.law.indiana.edu/facpub/2681>
37. Sahu S K, Majumdar K. Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance. *Front Artif Intell.* 2024;7:1397480.
<https://doi.org/10.3389/frai.2024.1397480>
38. Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G. Wang. Security and Privacy in the Medical Internet of Things: A Review. *Secur Commun Netw.* 2018;59786361-9.
<https://doi.org/10.1155/2018/5978636>
39. Haria K, Shah R, Jain V. Mangrulkar R. Enhanced image encryption using AES algorithm with CBC mode: a secure and efficient approach. *Iran Journal of Computer Science.* 2024;7:589-605.
<https://doi.org/10.1007/s42044-024-00191-y>
40. Hassani H, Silva ES. Forecasting with Big Data: A Review. *Ann Data Sci.* 2015;2(1):5-19.
<https://doi.org/10.1007/s40745-015-0029-9>
41. Casas P, D'Alconzo A, Zseby T, Mellia M. Big-DAMA: Big Data Analytics for Network Traffic Monitoring and Analysis. In *ACM SIGCOMM Workshop on Fostering Latin-American Research in Data Communication Networks.* Big-DAMA Publications. 2016;1-3.
<https://doi.org/10.1145/2940116.2940117>
42. Rarhi K, Saha S. Image Encryption in IoT Devices Using DNA and Hyperchaotic Neural Network. *Design Frameworks for Wireless Networks. Lecture Notes in Networks and Systems.* 2020;82:347-75.
https://doi.org/10.1007/978-981-13-9574-1_15
43. Singh MK, G DK. Eds. Effective Big Data Management and Opportunities for Implementation: in *Advances in Data Mining and Database Management.* IGI Global. 2016.
<https://doi.org/10.4018/978-1-5225-0182-4>
44. Chen P, Wald C. Consensus, Frameworks and Best Practices in A Review of Cybersecurity and Privacy Standards in Medical Imaging. *Journal of the American College of Radiology.* 2025;22(10):1124-31.
<https://doi.org/10.1016/j.jacr.2025.06.033>
45. Lata K, Gupta C, Cenkeramaddi L R. A cryptographic framework for secure medical imaging in smart healthcare environments. *Results in Engineering.* 2025;27:106780.
<https://doi.org/10.1016/j.rineng.2025.106780>
46. Vengadapurva AM, Nisha G, Aarth R, Sasikaladevi N. An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security. *Procedia Comput Sci.* 2017;115:643-50.
<https://doi.org/10.1016/j.procs.2017.09.150>
47. Ghazal TM, Hasan MK, Hassan R, Islam S, Abdullah SNHS, Afifi MAM, Kalra D. Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technology.* 2020;63(1s).
<https://solidstatetechnology.us/index.php/JSST/article/view/3096>
48. Cao W, Zhou Y, Chen CL, Xia L. Medical image encryption using edge maps. *Signal Process.* 2017;132:96-109.
<https://doi.org/10.1016/j.sigpro.2016.10.003>
49. Haque SA, Aziz SM, Rahman M. Review of Cyber-Physical System in Healthcar. *Int J Distrib Sens Netw.* 2014;10(4): 217415.
<https://doi.org/10.1155/2014/217415>

50. Burns AJ, Johnson ME, Honeyman P. A brief chronology of medical device security. *Commun ACM*. 2016;59(10):66–72. <https://doi.org/10.1145/2890488>.
51. Wang L and Jones R. Big data analytics for network intrusion detection: A survey. *International Journal of Networks and Communications*. 2017;7(1):24–31. <https://doi.org/10.5923/j.ijnc.20170701.03>
52. Li Y, Zhang P, Ma L. Denial of service attack and defense method on load frequency control system. *J Frankl Inst*. 2019;356(15):8625–45. <https://doi.org/10.1016/j.jfranklin.2019.08.036>
53. Kroll M, Schütze B, Geisbe T, Lipinski HG, Grönemeyer DHW, Filler TJ. Embedded systems for signing medical images using the DICOM standard. *Int Congr Ser*. 2003;1256:849–54. [https://doi.org/10.1016/S0531-5131\(03\)00463-1](https://doi.org/10.1016/S0531-5131(03)00463-1)
54. Chen M, Mao S, Liu Y. Big Data: A Survey. *Mob Netw Appl*. 2014;19(2):171–209. <https://doi.org/10.1007/s11036-013-0489-0>
55. Gonçalves D, Bota J, Correia M. Big Data Analytics for Detecting Host Misbehavior in Large Logs. In 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland. 2015;238–45. <https://doi.org/10.1109/Trustcom.2015.380>
56. McNeil, Shetty S, Guntu D, Barve G. SCREDIT: Scalable Real-time Anomalies Detection and Notification of Targeted Malware in Mobile Devices. *Procedia Comput. Sci*. 2016;83:1219–25. <https://doi.org/10.1016/j.procs.2016.04.254>
57. Rettig L, Khayati M, Cudré-Mauroux, Piorkowski M. Online Anomaly Detection over Big Data Streams, in *Applied Data Science*, M. Braschler, T. Stadelmann and K. Stockinger, Eds., Cham: Springer International Publishing. 2019;289–312. https://doi.org/10.1007/978-3-030-11821-1_16
58. Hameed S, Ali U. HADEC: Hadoop-based live DDoS detection framework. *EURASIP Journal on Information Security*. 2018;11. <https://doi.org/10.1186/s13635-018-0081-z>
59. Lobato AG, Andreoni Lopez M, Cardenas AA, Duarte OC, Pujolle G. A fast and accurate threat detection and prevention architecture using stream processing. *Concurrency and Computation: Practice and Experience*. 2021;34(3):e6561. <https://doi.org/10.1002/cpe.6561>
60. Liu X, Nielsen PS. Regression-based online anomaly detection for smart grid data. *arXiv preprint arXiv:1606.05781*. 2016. <https://arxiv.org/abs/1606.05781>
61. B. Cui and S. He. Anomaly Detection Model Based on Hadoop Platform and Weka Interface. In 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, Japan. 2016;84–9. <https://ui.adsabs.harvard.edu/abs/2016imis.conf...55C/abstract>
62. Nayak S, Patgiri R. A Vision on Intelligent Medical Service for Emergency on 5G and 6G Communication Era. *EAI Endorsed Trans. Internet Things*. 2020;6(22):e2. <https://doi.org/10.4108/eai.17-8-2020.166293>
63. Yaqoob T, Abbas H, Atiquzzaman M. Security Vulnerabilities, Attacks, Countermeasures and Regulations of Networked Medical Devices—A Review. *IEEE Commun Surv Tutor*. 2019;21(4):3723–68. <https://doi.org/10.1109/COMST.2019.2914094>
64. Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, Lymberopoulos D. A Survey on Security Threats and Countermeasures in Internet of Medical Things (Internet of medical things). *Tran Emerg Telecommun Technol*. 2022;33(6):e4049. <https://doi.org/10.1002/ett.4049>
65. Akhtaruzzaman M, Hasan MK, Kabir SR, Abdullah SNHS, Sadeq MJ, Hossain E. HSIC Bottleneck Based Distributed Deep Learning Model for Load Forecasting in Smart Grid With a Comprehensive Survey. *IEEE Access*. 2020;8:222977–3008. <https://doi.org/10.1109/ACCESS.2020.3040083>
66. Hassan R, Qamar F, Hasan MK, Aman AH, Ahmed AS. Internet of Things and its applications: A comprehensive survey. *Symmetry*. 2020;12(10):1674. <https://doi.org/10.3390/sym12101674>
67. Riazul Islam SM, Kwak D, Kabir MH, Hossain M, Kwak KS. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*. 2015;3:678–708. <https://doi.org/10.1109/ACCESS.2015.2437951>
68. Malasri K, Wang L. Securing wireless implantable devices for healthcare: Ideas and challenges. *IEEE Commun. Mag*. 2009;47(7):74–80. <https://doi.org/10.1109/MCOM.2009.5183475>
69. Wu L, Du X, Guizani M, Mohamed A. Mohamed. Access Control Schemes for Implantable Medical Devices: A Survey. *IEEE Internet Things J*. 2017;4(5):1272–83. <https://doi.org/10.1109/JIOT.2017.2708042>
70. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technol Health Care*. 2017;25(1):1–10. <https://doi.org/10.3233/THC-161263>
71. Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S. Health Care and Cybersecurity: Bibliometric Analysis of the Literature. *J Med Internet Res*. 2019;21(2):e12644. <https://doi.org/10.2196/12644>
72. Fernández-Alemán JL, Señor IC, Lozoya ÁO, Toval A. Toval. Security and privacy in electronic health records: A systematic literature review. *J Biomed Inform*. 2013;46(3):541–62. <https://doi.org/10.1016/j.jbi.2012.12.003>
73. Raja SP. Joint medical image compression-encryption in the cloud using multiscale transform-based image compression encoding techniques. *Sadhana*. 2019;44(28). <https://doi.org/10.1007/s12046-018-1013-9>
74. Ameli A, Hooshyar A, El-Saadany EF, Youssef AM. Attack Detection and Identification for Automatic Generation Control Systems. *IEEE Trans Power Syst*. 2018;33(5):4760–74. <https://doi.org/10.1109/TPWRS.2018.2810161>
75. Ali S, Qaisar S, Saeed H, Khan M, Naeem M, Anpalagan A. Network Challenges for Cyber Physical Systems with Tiny Wireless Devices: A Case Study on Reliable

- Pipeline Condition Monitoring. *Sensors*. 2015;15(4):7172–205.
<https://doi.org/10.3390/s150407172>
76. Alsaadi H H, Aldwairi M, Al Taei M, AlBuainain M, AlKubaisi M. Penetration and Security of OpenSSH Remote Secure Shell Service on Raspberry Pi 2. In 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris. 2018;1–5.
<https://doi.org/10.1109/NTMS.2018.8328710>.
 77. Liu X, Qian C, Hatcher WG, Xu H, Liao W, Yu W. Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. *IEEE Access*. 2019;7:79523–544.
<https://doi.org/10.1109/ACCESS.2019.2920763>
 78. Shar LK, Tan HB. Automated removal of cross site scripting vulnerabilities in web applications. *Inf Soft Technol*. 2012;54(5):467–78.
<https://doi.org/10.1016/j.infsof.2011.12.006>
 79. Shahriar H, Zulkernine M., S2XS2: A Server Side Approach to Automatically Detect XSS Attacks. In 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, Sydney, Australia. 2011;7–14.
<https://doi.org/10.1109/DASC.2011.26>
 80. Barhoom TS, Kohail SN. A new server-side solution for detecting cross site scripting attack. *Int J Comput. Inf Syst*. 2011;3(2):19-23.
<https://doi.org/10.13140/RG.2.1.4698.2882>
 81. Parasuraman S, Sangaiah AK. Fog-driven healthcare framework for security analysis. In *Computational Intelligence for Multimedia Big Data on the Cloud with Engineering Applications*. 2018:253–70.
<https://doi.org/10.1016/B978-0-12-813314-9.00012-8>
 82. Kombade RD, Meshram BB. CSRF Vulnerabilities and Defensive Techniques. *Int J Comput Netw Inf Secur*. 2012;4(1):31–7.
<https://doi.org/10.5815/ijcnis.2012.01.04>
 83. Xu HJ, Hu XM, Zhang DD. XSS Defensive Scheme Based on Behavior Certification. *Appl Mech Mater*. 2012;241(244):2365–9.
<https://doi.org/10.4028/www.scientific.net/AMM.241-244.2365>
 84. Gupta S, Gupta BB. Enhanced XSS Defensive Framework for Web Applications Deployed in the Virtual Machines of Cloud Computing Environment. *Procedia Technol*. 2016;24:1595–602.
<https://doi.org/10.1016/j.protcy.2016.05.152>.
 85. Batarfi OA, Alshiky AM, Almarzuki AA, Farraj NA. CSRFDtool: Automated Detection and Prevention of a Reflected Cross-Site Request Forgery. *Int J Inf Eng. Electron. Bus*. 2014;6(5):10–5.
<https://doi.org/10.5815/ijieeb.2014.05.02>
 86. Alberca C, Pastrana S, Suarez-Tangil G, Palmieri. Security analysis and exploitation of arduino devices in the internet of things. *Proceedings of the ACM International Conference on Computing Frontiers, Como Italy*. 2016:437–42.
<https://doi.org/10.1145/2903150.2911708>
 87. Naik N, Jenkins, Cooke R, Ball D, Foster A, Jin Y. Augmented windows fuzzy firewall for preventing denial of service attack. 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), Naples, Italy. 2017;1–6.
<https://doi.org/10.1109/FUZZ-IEEE.2017.8015701>

How to Cite: Potlabathini R, Jamalpur B, Khan NU. Securing Medical Imaging Systems Against Emerging Cyber Threats: A Multi-faceted Approach. *Int Res J Multidiscip Scope*. 2026;7(4):517-536.
 DOI: 10.47857/irjms.2026.v07i04.011127