Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 5, 2025

SECURING IOT DEVICES IN HEALTHCARE: CHALLENGES AND SOLUTIONS

Azeem Akram[*1], Muhammad Ismail[2], Syed Tahir Hussan[3], Aqsa Arshad[4], Saad Ishaq Qureshi[5], Dr. Jawaid Iqbal[6]

[*1,2,3,4,5]*Master in Software Engineering, Department of Software Engineering Riphah International University, Islamabad*
[6]*Assistant Professor, Department of Cyber Security, Riphah International University Islamabad*

[*1]akramazeem947@gmail.com, [2]mi477048@gmail.com, [3]hussansyedtahir@gmail.com, [4]aqsaarshad4@gmail.com, [5]saadq094@gmail.com, [6] jawaid.Iqbal@riphah.edu.pk

DOI: https://doi.org/10.5281/zenodo.15348564

All authors participated equally in this research.

Keywords
component, IoT security, Healthcare, Blockchain technology, Machine learning, Authentication, IoT-Blockchain integration

Article History
Received on 28 March 2025
Accepted on 28 April 2025
Published on 06 May 2025

Corresponding Author: * Azeem Akram

Abstract

This review article investigates the use of blockchain technology and powerful machine learning algorithms to improve IoT device security in healthcare. The main objective is to tackle crucial security issues like anomaly detection, authentication, and data integrity. A decentralized, unchangeable ledger for transactions and data transfers is made possible by blockchain technology, guaranteeing strong data integrity and transparency. By detecting abnormalities from typical behavior patterns, advanced machine learning models such as anomaly detection algorithms are used to detect and mitigate security threats in real-time. Furthermore, context-aware dynamic Bayesian networks and blockchain greatly enhance authentication methods, guaranteeing that only authorized users have access to IoT devices and data. The review emphasizes how important it is to strike a balance between strict adherence to regulations and thorough security measures in IoT systems for healthcare. Best practices for defending IoT networks against changing threats are also presented. The results highlight how blockchain and machine learning can be used to secure Internet of Things applications in the healthcare industry, laying the groundwork for more research in this important area.

INTRODUCTION

Healthcare organizations are increasingly depending on Internet of Things (IoT) devices for patient monitoring, data collection, and operational efficiency, which has made these devices a prime target for cyberattacks. According to reports, 82% of healthcare organizations have experienced attacks on their IoT devices. Integration of IoT technology enhances patient care and streamlines hospital operations, but it also introduces significant security vulnerabilities [1], [2]. Cyberattacks on IoT devices may result in data breaches, expose personal patient information, impede the provision of essential medical services, or even jeopardize patient safety [3]. Owing to the sensitive nature of patient data and the possible influence on patient safety, IoT device security in healthcare settings is essential. Large volumes of personal health data are collected and transmitted by Internet of Things (IoT) devices used in healthcare, including wearables, connected medical equipment, and patient monitoring systems

[4]. These devices may be susceptible to cyberattacks if they are not well secured, which might result in data breaches and unauthorized access to private information [5].

Healthcare companies need to use strong security measures, such as network segmentation, encryption, regular firmware updates, and strong authentication, to reduce these threats. Healthcare providers may safeguard patient privacy, guarantee the accuracy of medical data, and uphold the dependability of linked medical devices by placing a high priority on IoT security. The search results indicate that because the healthcare industry deals with sensitive data, it is among the most susceptible to hackers. Attacks like ransomware not only increase the expenses of a breach but also have the potential to disrupt operations and postpone patient care. Although there is currently no proof that a hacker has harmed a patient via a medical device, top cybersecurity experts have noted that any medical device can be compromised. In 2020, ransomware attacks cost healthcare organizations $20.8 billion, resulting in the malware's takedown of 560 healthcare facilities. The number of attacks against the healthcare sector increased by 75% in 2021 [6].

Healthcare organizations need to use strong security measures, such as network segmentation, encryption, frequent firmware updates, and strong authentication, to reduce these threats. IoT attacks on medical devices can be avoided with the use of effective information security protocols [7]. In order to significantly lower patient risk, vendors must be held responsible for all aspects of the design, security baselines, and robust security measures, including regular patching. Healthcare organizations may avoid data breaches, safeguard patient privacy, and guarantee the continuous provision of medical services by giving IoT security first priority. It is essential that those involved in the healthcare sector make investments in strong cybersecurity measures in order to handle the particular difficulties brought about by IoT devices and preserve patient and healthcare provider safety [8]-[9].

The objective of this review paper is to comprehensively investigate the challenges and potential solutions involved with securing IoT devices in healthcare settings, identify key concerns, and provide techniques for mitigating security risks while improving patient safety and data protection.

II. LITERATURE REVIEW

The potential for the Internet of Things (IoT) to transform the healthcare business has attracted a great deal of research interest in its integration. The works that address the difficulties and developments in IoT healthcare applications are examined in this overview of the literature.

IoT devices used in healthcare have grown to be major security vulnerabilities, resulting in multiple security breaches. According to an analysis, during the previous two years, 56% of healthcare organizations had at least one hack using IoT or IoMT equipment, which caused significant data loss and operational disruptions [10], [11]. Certain Internet of Things (IoT) devices have been outlined as major risks in healthcare settings, including wearable health monitors, smart infusion pumps, and remote patient monitoring systems. When these devices are hacked, serious data breaches may result, jeopardizing patient privacy and the accuracy of medical information [12]. IoT data breaches in the healthcare industry have a serious negative influence on reputation in addition to operational effectiveness. Users' confidence in healthcare professionals may be damaged by intruders keeping an eye on their personal lives. The willingness of patients to employ linked health technology may be negatively impacted in the long run by this breakdown of trust [13]. Medical IoT device security breaches can have a major financial impact because of fines and regulatory penalties. Robust security protocols are essential because weak security measures and design defects can cost healthcare organizations a lot of money [14]. Infusion pumps and patient monitoring are among the top six medical IoT devices that can be hacked, according to a study that puts cybersecurity at risk. These weaknesses may have an immediate effect on patient care, possibly resulting in risky changes to treatment plans and patient outcomes [15]. A survey of thirty recent attack stories revealed a variety of valuable and surprising data. The survey found that information about IoT vulnerabilities comes in many forms, with little uniformity. 76% of TAS21 vulnerabilities occurred in the software layer of the device, which

includes device-specific code, third party libraries, and third-party SDKs. The survey also revealed a range of vendor responsiveness, with some taking multiple attempts to respond to vulnerabilities, while others took years to develop and deploy fixes [1], [7]. Memory corruption, overflow, DoS, and bypass something vulnerabilities were found to be the most common. The study found that E-class and S-class IoT devices have the most vulnerabilities, but the growing trend of using H-class and M-class devices requires further attention. The risk of security vulnerabilities in IoT devices is high, and special attention must be paid to prevent them. The results can be used to study various devices and software vulnerabilities in the future, preventing hacking and industrial accidents [5]. Organizations can secure sensitive information, prevent threats, and preserve stakeholder trust by following the NIST framework and applying IA mechanisms [5], [9]. The researchers propose a two-step approach to identify sensitive information in firmware. The first step involves extracting the firmware file system from the firmware image, typically a BIN file. The second step involves analyzing the firmware to identify vulnerabilities and understand device behavior. Key information to look for includes login credentials, backdoors, URLs, cryptographic keys, encryption algorithms, and authentication mechanisms. Binwalk is recommended for extracting firmware files from the image. Other methods require physical access to the device. This method allows manufacturers and users to test their devices for common cyberattack vulnerabilities. Two test devices were identified, with some controlled without authentication or physical access. The Shodan database identifies thousands of devices for potential internet exploits [3].

Role-Based Access Control (RBAC) is an essential cybersecurity measure in healthcare that lowers the risk of unauthorized disclosures by assigning roles based on job functions and guaranteeing that only authorized personnel can access sensitive patient information. Healthcare establishments also employ diverse network security measures, including firewalls, intrusion detection systems, and secure network architectures, to safeguard networks from cyber hazards and unapproved entry [16]. Another essential tactic is to encrypt sensitive data while it's in transit and at rest to make sure that intercepted data cannot be decrypted without the right keys [17]. Frequent security audits and risk assessments aid in locating possible weak points and opportunities for development, enabling healthcare providers to keep up with new threats and uphold strong security postures. Furthermore, it is crucial to educate healthcare workers on cybersecurity best practices and the value of patient information protection [18]. Employee education in social engineering, phishing, and secure data handling techniques lowers the possibility that human mistake will result in security breaches. Last but not least, having a clearly defined incident response plan enables healthcare organizations to react to security breaches swiftly and efficiently. This strategy includes actions for recovery, containment, eradication, and post-incident analysis to lessen the effects of breaches and stop them from happening again [19].

The effectiveness of these approaches varies with implementation quality and adherence to best practices. Data encryption and role-based access control are very good at preventing unwanted access and preserving the integrity of the data. When updated on a regular basis, network security procedures offer robust protection against external threats. Frequent personnel training and audits greatly minimize vulnerabilities and raise general security awareness. Plans for incident response guarantee that security incidents are handled quickly and effectively, reducing damage and recovery time [20]. However, because cyber risks are always changing, it is imperative to continuously assess and react. Effective information security in healthcare organizations requires full implementation and the development of a security-conscious culture.

Regulations and standards are essential for protecting sensitive data and guaranteeing that data privacy regulations are followed in the field of healthcare data protection. The regulatory environment consists of a complicated web of rules and regulations designed to protect the privacy, accuracy, and accessibility of medical records. Important components of these frameworks are data privacy laws such as the General Data privacy Regulation (GDPR) in Europe and the traditional healthcare regulatory framework, which includes the common law duty of confidentiality and the regulation of medical equipment. These policies

cover concerns such as product liability, patient redress programs, safety, and data exchange across health institutions. Furthermore, while striking a balance between ethical concerns and innovation, the execution of regulatory measures concentrates on guaranteeing prompt access to high-quality, safe digital health goods and services. Through demonstrating the dependability of systems in managing data, software, and devices within healthcare delivery, the regulatory frameworks also seek to foster confidence between patients and healthcare providers. In order to preserve patient privacy and the integrity of healthcare services, compliance with these criteria is crucial in creating a setting where healthcare data is managed safely, morally, and legally.

One of the most important laws is the Health Insurance Portability and Accountability Act (HIPAA) in the US, which requires administrative, technical, and physical measures to be put in place to protect health information [21]. Additionally, in the United States, the HITECH Act improves privacy and security safeguards and encourages the use of electronic health records, therefore fortifying HIPAA. The European Union's General Data Protection Regulation (GDPR), which focuses on data subject rights and accountability measures, establishes strict data protection obligations for personal data, including health information [22]. Furthermore, the 21st Century Cures Act safeguards patient data while advancing the interoperability of health information technology. The Payment Card Industry Data Security Standard (PCI-DSS), which covers payment data in the healthcare business and guarantees that thorough data security procedures are in place, is one of the industry standards supporting these requirements.

III. METHODOLOGY

With a focus on vulnerability quantification and considering both breadth and depth, this study attempts to examine cutting edge frameworks for assessing IoT vulnerabilities. Three stages make up this methodical approach.

A. Phase 1: Planning the Review

1) Determining the Review's Need

The first step is realizing how important it is to evaluate IoT vulnerability frameworks in the healthcare industry, with a special emphasis on how well they can quantify vulnerabilities. To confirm the necessity of this study, a preliminary literature analysis and discussion with subject matter experts are required.

2) Research Questions

For the research focused on IoT security in healthcare, the following research questions are proposed:

What are the primary security vulnerabilities in IoT devices used in healthcare settings?

What are the effective authentication protocols that can be implemented in IoT-based healthcare systems to ensure only authorized access?

What are the best practices for securing IoT networks in healthcare against emerging threats?

3) Creating the Review Protocol

A thorough review protocol is created that covers the databases to be searched, the search techniques, and the inclusion and exclusion criteria for choosing research. Peer review is used to make sure the procedure is accurate and up to date.

B. Phase 2: Conducting the Review

1) Search Approach

Academic databases including IEEE Xplore, PubMed, ScienceDirect, and Google Scholar are searched thoroughly using keywords like "vulnerability quantification," "healthcare security," and "IoT vulnerability assessment."

2) Study Selection

There are three steps in the selection process:

First Screening: Unrelated research are weeded out of the retrieved articles based on their titles and abstracts.

Full-Text Review: The remaining publications' full texts are analyzed to determine their relevance in light of the inclusion criteria, which include research that primarily focus on IoT vulnerability assessment frameworks in healthcare.

Quality Assessment: The methodology rigor, validity of the findings, and relevance to the research questions are some of the factors used to evaluate the quality of the chosen studies.

3) Data Synthesis and Extraction

Information is taken from the chosen studies and analyzed, with particular attention paid to the features of the frameworks used for vulnerability assessments, the methods they use to measure vulnerabilities, and how they are used in the healthcare industry. The gathered data is combined to offer a thorough summary of the most recent frameworks.

C. Phase 3: Reporting the Review

1) Descriptive Analysis

The main characteristics of the IoT vulnerability assessment frameworks, including their methods for quantification and the kinds of vulnerabilities they address, are summarized in a descriptive analysis of the chosen studies.

2) Comparative Analysis

The frameworks are contrasted according to parameters such their efficacy in a healthcare environment, comprehensiveness (breadth), depth of analysis, and simplicity of use. This analysis focuses on each framework's advantages and disadvantages.

3) Discussion and Implications

The results are analyzed in terms of healthcare security, with a focus on how the existing frameworks consider the particular requirements of IoT systems in the healthcare industry. Future research directions and areas for improvement are suggested, along with implications for practitioners and researchers.

4) Conclusions and Recommendations

A summary of the major conclusions and helpful suggestions for healthcare professionals and legislators on the choice and application of efficient IoT vulnerability assessment frameworks are provided at the end of the study.

This approach guarantees a methodical and thorough examination of IoT vulnerability assessment frameworks, offering insightful information on how well they work in healthcare settings.

D. Ethical Considerations

The research on IoT vulnerability assessment frameworks in the healthcare sector is crucial to ensure the protection of sensitive patient data and the integrity of the research process. Key ethical issues include privacy and confidentiality, informed consent, data security, ethical use of technology, and regulatory compliance. Data should be anonymized to protect patient identities, and informed consent is essential for participants to understand the research scope, potential risks, and data protection. Robust data security measures, such as encryption, secure storage solutions, and regular security audits, are essential to protect against breaches and cyber threats. The deployment of IoT devices should respect patient autonomy and avoid surveillance that could infringe on personal freedoms. Adhering to legal frameworks like HIPAA and GDPR is mandatory to ensure research aligns with existing laws designed to protect patient data and privacy. Addressing these ethical considerations comprehensively will help conduct responsible and ethical research in the healthcare sector.

IV. IOT SECURITY CHALLENGES IN HEALTHCARE

Healthcare IoT devices have several safety concerns, such as data privacy and confidentiality, device integrity and reliability, authentication and access control, and regulatory compliance. Healthcare IoT systems handle sensitive patient data, so protecting data privacy and confidentiality is crucial. Unauthorized access to and misuse of personal health information can result from data privacy violations [23], [24]. Access control and authentication are essential for preventing illegal users from connecting to IoT networks and devices. Enforcing strong authentication procedures is necessary in order to confirm user identities and manage access according to roles and permissions [25]. Maintaining the credibility of healthcare IoT systems depends on device integrity and reliability. Device functionality and data integrity must be safeguarded against manipulation and cyberattacks. Lastly, regulatory

compliance with standards like GDPR and HIPAA guarantees that IoT solutions for healthcare data protection and patient privacy follow the law. Serious fines and a decline in patient confidence may follow noncompliance [8], [26]. A comprehensive strategy incorporating cutting-edge security measures, ongoing monitoring, and adherence to regulatory standards is needed to address these challenges, tabulated in table 1.

TABLE I. CHALLENGES IN SECURITY OF IOT DEVICES IN HEALTHCARE

YEAR	CHALLENGES ADDRESSED	REFERENCE
2024	Summarizes challenges in implementing IoT in healthcare systems, including data privacy, interoperability, and infrastructure requirements	[1]
2023	Examines issues related to sensor accuracy, data integration, and communication methods in IoT healthcare applications	[2]
2022	Focuses on technical and regulatory challenges, including cybersecurity risks and compliance with healthcare regulations	[3]
2021	Discusses dominant trends and their associated challenges, Such as scalability, data security, and patient acceptance	[1]
2020	Analyzes technological, ethical, and logistical challenges in deploying IoT in healthcare environments	[4]
2019	Reviews both positive impacts and significant hurdles like high implementation costs, data privacy concerns, and technological complexity	[5]

V. SOLUTIONS AND BEST PRACTICES

Encryption is crucial for safeguarding medical data. To avoid unwanted access, data should be encrypted while it's in transit and at rest. Data storage and transmission are frequently secured through the use of Transport Layer Security (TLS) protocols and Advanced Encryption Standards (AES). Encryption keys are also handled safely when secure key management procedures are put in place [28].

Ensuring that sensitive healthcare data is only accessed by authorized persons requires strong authentication procedures. Users that utilize multi-factor authentication (MFA) must submit various forms of verification, which adds an additional degree of protection. Security can be further improved by protocols like OAuth and biometric authentication, which make sure that access is only given to legitimate users and devices. By splitting a network into smaller parts, network segmentation helps to confine assaults and restrict the spread of any breaches [29]. Network segmentation can be

used to isolate systems and sensitive data from other parts of the network. Real-time security threat identification and mitigation can be facilitated by employing intrusion detection systems IDS) and intrusion prevention systems (IPS) to continuously monitor network traffic [30]. Safeguarding health information requires adherence to laws like the Health Insurance Portability and Accountability Act (HIPAA). This entails putting rules and processes in place to guarantee protected health information's availability, confidentiality, and integrity (PHI) [29]. Organizations can detect and resolve potential vulnerabilities by solutions as proposed in table 2 with the support of routine audits and risk assessments, which guarantee continuous compliance with regulatory standards.

TABLE II. PROPOSED SOLUTIONS FOR SECURITY OF IOT DEVICES IN HEALTHCARE

YEAR	CHALLENGES ADDRESSED	REFERENCE
2024	Summarizes challenges in implementing IoT in healthcare systems, including data privacy, interoperability, and infrastructure requirements	[1]
2024	Comprehensive Overview of IoT applications in healthcare, highlighting motivations, challenges, and recommendations for implementation	[3]
2023	Proposes a smart system using IoT technology to assist patients with influenza symptoms in determining their COVID-19 status	[5]
2022	Detailed analysis of IoT applications in healthcare, focusing on the technological advancements And challenges encountered	[6]
2021	Organizes IoT Healthcare literature according to dominant trends, providing an instructive overview of current research	[1]
2020	Addresses uncertainties and proposes frameworks for managing technological challenges in IoT-based healthcare systems	[7]
2018	Proposes the design and implementation of an IoT-based monitoring system in medical applications	[8]
2016	Discusses various IoT-based healthcare solutions aimed at improving patient care And monitoring	[9]

The proposed approach that aims to improve the security of IoT devices in the healthcare industry combines cutting-edge machine learning algorithms with blockchain technology. This method covers data integrity, authentication, and anomaly detection, among other aspects of security. A decentralized, unchangeable ledger for tracking all transactions and data transfers between Internet of Things devices can be produced by blockchain technology. This guarantees strong data integrity by making sure that once information is recorded, it cannot be changed or tampered with. The blockchain enables the registration of every Internet of Things device and the logging of all data transmissions, resulting in a safe and transparent audit trail. Using machine learning algorithms helps improve the identification of irregularities and possible security risks. IoT device behavior patterns can be used to build machine learning models, which can then be used to swiftly detect deviations that could point to a security breach. IoT devices can be continuously monitored by methods like Support Vector Machines (SVMs) and anomaly detection algorithms, which can indicate questionable activity in real time. Authentication procedures can be considerably enhanced by combining blockchain technology with context-aware dynamic Bayesian networks. Blockchain technology can be used to verify the unique cryptographic identity of each Internet of Things device, and Bayesian networks can adjust to contextual changes to guarantee that only authorized people and devices can access the system.

VI. CONCLUSION

This study focuses on major security concerns for IoT devices in healthcare, such as data privacy, authentication, device integrity, and regulatory compliance. The main conclusions highlight the need for strong data protection and encryption strategies, sophisticated authentication mechanisms, efficient network segmentation, and close compliance with HIPAA and other healthcare laws. It is advised that future studies investigate how to improve security frameworks by integrating cutting-edge technology like blockchain, AI, and machine learning. It will be essential to look at how 5G networks affect Internet of Things security and to create extensive, flexible security protocols that can change as technology advances. Ensuring the safety of IoT devices in healthcare settings requires regular upgrades to combat emerging threats and ongoing security measure enhancement.

Due to the delicate nature of medical data and the possible repercussions of data breaches, which include jeopardizing patient safety and privacy, securing IoT devices in the healthcare industry is crucial. Trust in IoT-enabled healthcare systems must be preserved by guaranteeing the privacy, availability, and integrity of healthcare data.

REFERENCES

[1] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges," J. Inf. Intell., p. S2949715923000793, Dec. 2023, doi: 10.1016/j.jiixd.2023.12.001.

[2] Steve Alder, "82% Of Healthcare Organizations Have Experienced an IoT Cyberattack in the Past 18 Months," HIPAA Journal i, Nov. 2021, [Online]. Available: https://www.hipaajournal.com/82-of-healthcare-organizations-have-experienced-an-iot-cyberattack-in-the-past-18-months/

[3] L. Costa, J. Barros, and M. Tavares, "Vulnerabilities in IoT Devices for Smart Home Environment:," in Proceedings of the 5th International Conference on Information Systems Security and Privacy, Prague, Czech Republic: SCITEPRESS - Science and Technology Publications, 2019, pp. 615–622. doi: 10.5220/0007583306150622.

[4] H. Pourrahmani, A. Yavarinasab, A. M. H. Monazzah, and J. Van Herle, "A review of the security Things solutions: A bright future for the Blockchain," Internet Things, vol. 23, p. 100888, Oct. 2023, doi: 10.1016/j.iot.2023.100888.

[5] S. A. V. Rohith Vallabhaneni, Abhilash Maroju, Sravanthi Dontu, "Analysis on Security Vulnerabilities of the Modern Internet of Things (IOT) Systems," Int. J. Recent Innov. Trends Comput. Commun., vol. 11, no. 9s, pp. 801–808, Aug. 2023, doi: 10.17762/ijritcc.v11i9s.9487.

[6] S. A. Baho and J. Abawajy, "Analysis of Consumer IoT Device Vulnerability Quantification Frameworks," Electronics, vol. 12, no. 5, p. 1176, Feb. 2023, doi: 10.3390/electronics12051176.

[7] M. K. Ryan and K. Y. Rozier, "A Survey and Analysis of Recent IoT Device Vulnerabilities." Mar. 26, 2024. doi: 10.21203/rs.3.rs-3982790/v1.

[8] H. H. Mohamad Jawad, Z. Bin Hassan, B. B. Zaidan, F. H. Mohammed Jawad, D. H. Mohamed Jawad, and W. H. D. Alredany, "A Systematic Literature Review of Enabling IoT in Healthcare: Motivations, Challenges, and Recommendations," Electronics, vol. 11, no. 19, p. 3223, Oct. 2022, doi: 10.3390/electronics11193223.

[9] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-Based Applications in Healthcare Devices," J. Healthc. Eng., vol. 2021, pp. 1–18, Mar. 2021, doi: 10.1155/2021/6632599.

[10] A. Hussain et al., "Security Framework for IoT Based Real-Time Health Applications," Electronics, vol. 10, no. 6, p. 719, Mar. 2021, doi: 10.3390/electronics10060719.

[11] Hiranmayi Krishnan, "Security challenges associated with healthcare IoT devices," Security challenges associated with healthcare IoT devices. [Online]. Available: https://www.manageengine.com/log-management/cyber-security/security-issues-healthcare -iot-devices.html

[12] Zac Amos, "IoT Devices Are a Leading Vulnerability in Healthcare Data Breaches," IoT Devices Are a Leading Vulnerability in Healthcare Data Breaches. [Online]. Available: https://www.iotforall.com/iot-devices-vulnerability-healthcare-data-breaches

[13] I. Sadek, J. Codjo, S. U. Rehman, and B. Abdulrazak, "Security and privacy in the internet of things healthcare systems: Toward a robust solution in real-life deployment," Comput. Methods Programs Biomed. Update, vol. 2, p. 100071, 2022, doi: 10.1016/j.cmpbup.2022.100071.

[14] Ejona Preçi, "Addressing Security Risks to Medical IoT Devices," Addressing Security Risks to Medical IoT Devices. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/addressing-security-risks-to-medical-iot-devices

[15] Critical Insight, "Top 6 Hackable Medical IoT Devices," Top 6 Hackable Medical IoT Devices. [Online]. hackable-medical-iot-devices

[16] RioMed, "5 Major Healthcare Cybersecurity Measures to Prevent Cyberattacks," 5 Major Healthcare Cybersecurity Measures to Prevent Cyberattacks. [Online]. Available: https://www.riomed.com/5-major-healthcare-cybersecurity-measures-to-prevent-cyberattacks/

[17] R. Mahmoud and Y. A. Najjar, "CYBERSECURITY IN HEALTHCARE INDUSTRY," vol. 12, no. 2, 2024.

[18] HIMSS, "Cybersecurity in Healthcare," Cybersecurity in Healthcare. [Online]. Available: https://www.himss.org/resources/cybersecurity-healthcare

[19] P. Shojaei, E. Vlahu-Gjorgievska, and Y.-W. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," Computers, vol. 13, no. 2, p. 41, Jan. 2024, doi: 10.3390/computers13020041.

[20] A. T. Alanazi, "Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats," Cureus, Oct. 2023, doi: 10.7759/cureus.47026.

[21] Alexis Porter, "8 Healthcare Compliance Regulations You Should Know," 8 Healthcare Compliance Regulations You Should Know. [Online]. Available: https://bigid.com/blog/8-healthcare-compliance-regulations-you-should-know/

[22] T. Mazhar et al., "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," Brain Sci., vol. 13, no. 4, p. 683, Apr. 2023, doi: 10.3390/brainsci13040683.

[23] N. Li et al., "A review of security issues and solutions for precision health in Internet-of-Medical-Things systems," Secur. Saf., vol. 2, p. 2022010, 2023, doi: 10.1051/sands/2022010.

[24] A. Parihar, J. B. Prajapati, B. G. Prajapati, B. Trambadiya, A. Thakkar, and P. Engineer, "Role of IOT in healthcare: Applications, security & privacy concerns," Intell. Pharm., p. S2949866X24000030, Jan. 2024, doi: 10.1016/j.ipha.2024.01.003.

[25] C. Li, J. Wang, S. Wang, and Y. Zhang, "A review of IoT applications in healthcare," Neurocomputing, vol. 565, p. 127017, Jan. 2024, doi: 10.1016/j.neucom.2023.127017.

[26] W. AL-mawee, "Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey".

[27] R. Lederman, O. Ben-Assuli, and T. H. Vo, "The role of the Internet of Things in Healthcare in supporting clinicians and patients: A narrative review," Health Policy Technol., vol. 10, no. 3, p. 100552, Sep. 2021, doi: 10.1016/j.hlpt.2021.100552.

[28] R. Rajkamal, V. Anitha, P. G. Nayaki, K. Ramya, and E. Kayalvizhi, "A novel approach for waste segregation at source level for effective generation of electricity — GREENBIN," in 2014 International Conference on Science Engineering and Management Research (ICSEMR), Chennai, India: IEEE, Nov. 2014, pp. 1–4. doi: 10.1109/ICSEMR.2014.7043540.

[29] S. Boopathi, "Securing Healthcare Systems Integrated With IoT: Fundamentals, Applications, and Future Trends," in Advances in Healthcare Information Systems and Administration, A. Suresh Kumar, U. Kose, S. Sharma, and S. Jerald Nirmal Kumar, Eds., IGI Global, 2023, pp. 186–209. doi: 10.4018/978-1-6684-6894-4.ch010.

[30] I. Alam and M. Kumar, "A novel authentication protocol to ensure confidentiality among the Internet of Medical Things in covid-19 and future pandemic scenario," Internet Things, vol. 22, p. 100797, Jul. 2023, doi: 10.1016/j.iot.2023.100797.

[31] The Impact of Digital Technologies on Public Health in Developed and Developing Countries, vol. 12157, M. Jmaiel, M. Mokhtari, B. Abdulrazak, H. Aloulou, and S. Kallel, Eds., in Lecture Notes in Computer Science, vol. 12157. , Cham: Springer International Publishing, 2020, pp. 232–239. doi: 10.1007/978-3-030-51517-1_19.

[32] Darshan K R and Anandakumar K R, "A comprehensive review on usage of Internet of Things (IoT) in healthcare system," in 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), Mandya, India: IEEE, Dec. 2015, pp. 132–136. doi: 10.1109/ERECT.2015.7499001..