

Engineering Cyber-Physical Systems
and Critical Infrastructures 11

Pardeep Kumar
Prabhishek Singh
Manoj Diwakar
Deepak Garg *Editors*


Healthcare Industry Assessment: Analyzing Risks, Security, and Reliability

 Springer

Engineering Cyber-Physical Systems and Critical Infrastructures

Volume 11

Series Editor

Fatos Xhafa , Departament de Ciències de la Computació, Technical University of Catalonia, Barcelona, Spain

The aim of this book series is to present state of the art studies, research and best engineering practices, real-world applications and real-world case studies for the risks, security, and reliability of critical infrastructure systems and Cyber-Physical Systems. Volumes of this book series will cover modelling, analysis, frameworks, digital twin simulations of risks, failures and vulnerabilities of cyber critical infrastructures as well as will provide ICT approaches to ensure protection and avoid disruption of vital fields such as economy, utility supplies networks, telecommunications, transports, etc. in the everyday life of citizens. The intertwine of cyber and real nature of critical infrastructures will be analyzed and challenges of risks, security, and reliability of critical infrastructure systems will be revealed. Computational intelligence provided by sensing and processing through the whole spectrum of Cloud-to-thing continuum technologies will be the basis for real-time detection of risks, threats, anomalies, etc. in cyber critical infrastructures and will prompt for human and automated protection actions. Finally, studies and recommendations to policy makers, managers, local and governmental administrations and global international organizations will be sought.

Pardeep Kumar · Prabhishek Singh ·
Manoj Diwakar · Deepak Garg
Editors

Healthcare Industry Assessment: Analyzing Risks, Security, and Reliability

 Springer

Editors

Pardeep Kumar
Department of Computer Science
and Engineering
Jaypee University of Information
Technology
Solan, Himachal Pradesh, India

Manoj Diwakar
Department of Computer Science
and Engineering
Graphic Era (Deemed to be University)
Dehradun, Uttarakhand, India

Prabhishek Singh
Department of Computer Science
and Engineering
School of Computer Science Engineering
and Technology
Bennett University
Greater Noida, Uttar Pradesh, India

Deepak Garg
School of Computer Science and Artificial
Intelligence
SR University
Warangal, Telangana, India

ISSN 2731-5002

ISSN 2731-5010 (electronic)

Engineering Cyber-Physical Systems and Critical Infrastructures

ISBN 978-3-031-65433-6

ISBN 978-3-031-65434-3 (eBook)

<https://doi.org/10.1007/978-3-031-65434-3>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024, corrected publication 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

Preface

Recently, healthcare industry stands as one of the most demanding and exciting aspects of the information era. The subject matter encompasses a wide range of topics, including the growing utilization of digital tools in medical practice, the rising occurrence of cyber-attacks on healthcare institutions, the need for stricter measures to protect sensitive patient information, the paramount importance of dependability and availability in healthcare, the difficulties of adhering to regulations, and the role of risk management in the healthcare system. The book extensively addresses the various risks, security concerns, and dependability issues encountered by the healthcare industry. It provides comprehensive coverage of the latest security risks and trends, offers practical recommendations for risk reduction and enhanced reliability, incorporates real-world examples and case studies from healthcare organizations, and caters to a diverse audience including healthcare professionals, IT professionals, and security experts.

Outline of the Book and Chapter Synopsis

The book caters to a wide range of readers, including professionals in the healthcare and IT sectors, as well as security practitioners. This resource provides valuable perspectives on the risks and difficulties currently faced by the healthcare industry, and presents practical recommendations for effectively managing these risks and enhancing security and reliability. This book is beneficial for anyone seeking to enhance their understanding of the risks, security, and reliability challenges encountered by the healthcare industry. The provided information offers a comprehensive overview of the issues at hand and provides recommendations for mitigating risks and enhancing security and stability. A brief and orderly introduction to the chapters is provided in the following. The book contains fifteen chapters.

Chapter “[Introduction to Security Risk Assessment in Medical and Healthcare Industry](#)” presents an introductory chapter of the book which, critically reviews the exponentially growing cybersecurity landscapes in the field of healthcare, specifically

focusing on implantable medical devices. This chapter highlights the irony of how the medical devices that have been developed to improve human health have become mass targets for malicious cyber-attacks. It serves as a starting point to illustrate the complex as well as important role that cyber security plays in the field of healthcare, thus highlighting the need for implementing a strong defense network to reduce the escalating cyber threats. Through a detailed review of the real-world instances, this chapter unravels the importance of detecting and removing the vulnerabilities in implantable medical devices (IMDs) and Internet of Medical Things (IoMT) devices.

Chapter “[Identifying the Risk in Lie Detection for Assessing Guilty and Innocent Subjects for Healthcare Applications](#)” presents a study that aims to critically assess the implications and potential hazards of employing deep learning algorithms for the identification of innocence and guilt through lie detection methodologies within healthcare environments. This study highlights the importance of band-pass filters in lie detection, which enable the isolation of particular EEG signal frequencies that may reflect cognitive processes associated with deception.

Chapter “[Building Trust: The Foundations of Reliability in Healthcare](#)” presents a study on reliability in healthcare which is essential in the healthcare industry to guarantee patient safety and deliver optimal services. The crucial components that support healthcare organisations’ dependability are also highlighted. Modern technology must be used, clinical processes must be given priority, and an effective communication culture must be fostered. Leadership is essential because it promotes responsibility, encourages lifelong learning, and actively takes part in efforts to raise standards. Leadership is crucial because it fosters accountability, supports lifelong learning, and actively participates in initiatives to improve quality. Frontline healthcare workers who participate in decision-making processes develop a collaborative atmosphere that enhances reliability and fosters a sense of responsibility.

Chapter “[Predictive Modeling to Identify Syndrome Patterns](#)” presents predictive modeling to identify syndrome patterns. Machine Learning (ML) advances have demonstrated the potential to enhance medical diagnosis. To generate the best model and ideal feature selection, feature selection strategies that make use of a range of machine learning models—such as Support Vector Machine (SVM), Random Forest (RF), Gradient Boosting (GB), and Logistic Regression (LR) are used. To do this, machine learning methods were used on a dataset accessible to the public in the Kaggle repository. Of the 541, 177 individuals had PCOS, and those patients’ 45 attributes were part of the dataset. The optimal features for PCOS prediction were initially identified using the univariate feature selection method. Following the ranking of the features, the most important factor in PCOS detection was the ratio of luteinizing hormone (LH) to follicle-stimulating hormone (FSH).

Chapter “[Advancing Healthcare Security: Exploring Applications, Challenges, and Future Research Paths in Healthcare 5.0](#)” aims to delve into the progression of the industry elucidating the principles behind both industrial revolutions and emphasizing the driving forces propelling the move toward Industry 5.0. Moreover, it explores how Industry 5.0 impacts the healthcare system by discussing its uses and effects on healthcare delivery. It also addresses security requirements and risks associated with Industry 5.0 while proposing a customized threat model to bolster

security measures. By conducting an analysis of security frameworks in healthcare during both phases of advancement. From 4.0 to 5.0. This research sheds light on their evolution and deployment practices. Additionally, it thoroughly examines the challenges encountered when implementing Industry 5.0 in healthcare settings offering insights, into areas that require attention and development. The paper concludes by outlining areas, for research offering a roadmap to progress Healthcare 5.0 and tackle the new challenges, in the industry.

Chapter “[The Impact of Machine Learning on Chronic Kidney Disease: Analysis and Insights](#)” explores the application of neural network models to improve the diagnosis and treatment of chronic kidney disease (CKD), leveraging a comprehensive dataset of health-related attributes from 400 patients. The methodology involved preprocessing the dataset to handle missing values, encode categorical data, and address label imbalance, ensuring the data was primed for neural network analysis. Following data preparation, a neural network architecture was designed, focusing on reducing dimensionality and balancing the dataset to enhance model training and generalization capabilities. The outcomes of the neural network model showed promising improvements in predicting CKD, outperforming traditional diagnostic methods.

Chapter “[Embryonic Machine-Deep Learning, Smart Healthcare and Privacy Deliberations in Hospital Industry: Lensing Confidentiality of Patient’s Information and Personal Data in Legal-Ethical Landscapes Projecting Futuristic Dimensions](#)” explores the various dimensions of the legal and ethical landscapes governing patient data privacy in the hospital industry, exploring the challenges and opportunities posed by Machine and Deep Learning in Smart Healthcare.

Chapter “[Legal and Regulatory Consideration in Healthcare Industry of India](#)” delves into the elaborateness of the Seven Health Laws of India, elucidating the rules and regulations that underpin the country’s healthcare system to ensure that individuals receive standard and quality health services. The laws and regulatory bodies of India’s healthcare system ensure continued advancement of patient safety and healthcare quality.

Chapter “[Smart Health Revolution: Exploring Artificial Intelligence of Internet of Medical Things](#)” proposes a model to ensure a secure AIoMT ecosystem since the medical endpoint devices (MePD) make data processing using AI systems available to the medical midpoint devices (MiPD) (fog, mist, or edge) from the user through the AIoMT Cloud, besides blockchain and data encryption frameworks. Finally, patients’ and doctors’ involvement during model development will increase trust, acceptance, and collaboration.

Chapter “[IoTs-Based Wearable Health Monitoring Through Wireless Body Area Networks](#)” discusses the body area network architecture, communication types, and their issues in IOT healthcare. This work also presents the working of IoT-based BANs in the human body for monitoring and diagnosis the diseases and discusses the potential healthcare application of IoT (HIoT).

Chapter “[Revolutionizing Healthcare: Telemedicine and Remote Diagnostics in the Era of Digital Health](#)” discusses remote diagnostics which is also used in wearable devices and sensors to monitor health parameters from afar, thereby ensuring

early detection of health problems, customized treatment strategies, among other interventions. When looked at together, these progressions improve the way healthcare services are delivered while deepening the experience and giving the power to control health as a personal decision. Nevertheless, there is a need to acknowledge these challenges: ensuring data security, equal access for all, and keeping the human touch in healthcare delivery. In order to successfully exploit telemedicine and remote diagnostics potential in this digital health period with all its possibilities, it is essential that fairness, availability, and patient-focused care should be of primary consideration.

Chapter “[Wearable Devices—A New Dimension in Healthcare](#)” discusses on how wearable health technology can motivate individuals to take more responsibility for their own health. This chapter also provides instructions on how to set up a wristwatch to track vital signs. The chapter discusses potential obstacles to the use of wearable technology, the role of providers, the benefits of encouraging wearable use, and the ways in which wearable technology could influence behavior.

Chapter “[Operational Challenges in Modern Business Evolution in Healthcare Technology Startups](#)” provides an in-depth analysis of the rapidly evolving sector of healthcare technology startups. The discussion spans various critical aspects, including the historical evolution of healthcare technology, operational challenges specific to this sector, and the technological advancements that are reshaping healthcare delivery. The depth of problems is explored within themes such as regulatory compliance, financial management, and strategic market positioning in order to understand the unique landscape these startups traverse.

Chapter “[Mathematical Framework for Class Self-correction Through Reverse Validation in Hierarchical Classification](#)” proposed mathematical framework auto-corrects errors of the AI models through reverse validation in hierarchical classification (RVHC). The said framework honors the (a) condense scores of classification, (b) superclass-subclass interaction configuration, and (c) adaptive weight matrix of overlapped subclass components to formulate projection matrix as far as the RVHC is concerned. The proposed work also has proved that the formulated math works well with various kinds of critical real-life problem statements in machine learning and deep learning-based classification cutting across the domains of computer vision, speech processing, and natural language processing.

Finally, Chapter “[Addressing the Emerging Healthcare Environment: Risk Assessment for Healthcare 5.0](#)” aims to examine the risk assessment for Healthcare 5.0 as well as the evolving healthcare environment. From discussing the advent of cutting-edge technologies to the reason behind why risk assessment matters. The in-depth analysis of conventional risk approaches is examined, along with their shortcomings. The risk assessment frameworks pertaining to Healthcare 5.0 which are inclusive of Safeguarding Information Systems, Mitigating Risks to Patient Wellbeing as well as Ensuring the Reliability of Medical Devices are studied in a comprehensive manner.

We especially thank the Studies in Engineering Cyber-Physical Systems and Critical Infrastructures Book Series Editor, Prof. Fatos Xhafa for his continuous support and great guidance.

We would also like to thank publishers at Springer, in particular, Thomas Ditzinger, Editorial Director, Interdisciplinary and Applied Sciences and Engineering and Hemavathy Manivannan (MS.), Production Editor for their helpful guidance and encouragement during the creation of this book.

We are sincerely thankful to all authors, editors, and publishers whom works have been cited directly/indirectly in this manuscript.

Special Acknowledgements

The first author gratefully acknowledges the authorities of *Jaypee University of Information Technology, Wagnaghat, Solan, Himachal Pradesh, India* for their kind support to come up with this book.

The second author gratefully acknowledges the authorities of *School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India*, for their kind support to come up with this book.

The Third author gratefully acknowledges the authorities of *Department of Computer Science and Engineering at Graphic Era Deemed to be University, Dehradun, India*, for their kind support to come up with this book.

The Fourth author gratefully acknowledges the authorities of *SR University, Warangal, India*, for their kind support to come up with this book.

Solan, Himachal Pradesh, India
Greater Noida, Uttar Pradesh, India
Dehradun, Uttarakhand, India
Warangal, Telangana, India

Prof. (Dr.) Pardeep Kumar
Dr. Prabhishek Singh
Prof. (Dr.) Manoj Diwakar
Prof. (Dr.) Deepak Garg

Contents

Introduction to Security Risk Assessment in Medical and Healthcare Industry	1
Vandit Akhilesh Barola, Prabhishek Singh, and Manoj Diwakar	
Identifying the Risk in Lie Detection for Assessing Guilty and Innocent Subjects for Healthcare Applications	25
Tanmayi Nagale and Anand Khandare	
Building Trust: The Foundations of Reliability in Healthcare	43
Ghousia Jabeen, Gurunadham Goli, and Kafila	
Predictive Modeling to Identify Syndrome Patterns	67
Garima Jaiswal, Gargi Bhardwaj, Tarushi, Abhiruchi Sarswat, and Ritu Rani	
Advancing Healthcare Security: Exploring Applications, Challenges, and Future Research Paths in Healthcare 5.0	93
Aryan Dahiya, Anuradha Dhull, and Akansha Singh	
The Impact of Machine Learning on Chronic Kidney Disease: Analysis and Insights	121
K. P. Swain, Rabindra Kumar Nayak, Ayusee Swain, and Soumya Ranjan Nayak	
Embryonic Machine-Deep Learning, Smart Healthcare and Privacy Deliberations in Hospital Industry: Lensing Confidentiality of Patient’s Information and Personal Data in Legal-Ethical Landscapes Projecting Futuristic Dimensions	149
Bhupinder Singh and Christian Kaunert	
Legal and Regulatory Consideration in Healthcare Industry of India	171
Rachoru Himani Srihita, Gurunadham Goli, and M. Rajya laxmi	

Smart Health Revolution: Exploring Artificial Intelligence of Internet of Medical Things 201
Wasswa Shafik

IoT-Based Wearable Health Monitoring Through Wireless Body Area Networks 231
Meenakshi Yadav, Preety Shoran, Esha Saxena, Anchit Bijalwan, and Jyotsna Ghildiyal Bijalwan

Revolutionizing Healthcare: Telemedicine and Remote Diagnostics in the Era of Digital Health 255
Pongkit Ekvitayavetchanukul, Ch. Bhavani, Namita Nath, Lokesh Sharma, Gaurav Aggarwal, and Rakhi Singh

Wearable Devices—A New Dimension in Healthcare 279
Preetam Suman, Amrit Suman, Sasmita Padhy, Naween Kumar, Masood H. Siddiqui, Akansha Singh, and Aditi Sharma

Operational Challenges in Modern Business Evolution in Healthcare Technology Startups 301
Vikesh Lalit, Yogita Sharma, Pongkit Ekvitayavetchanukul, Jayeeta Majumder, Susmi Biswas, and Sourav Gangopadhyay

Mathematical Framework for Class Self-correction Through Reverse Validation in Hierarchical Classification 325
Apurba Das and Pallavi Saha

Addressing the Emerging Healthcare Environment: Risk Assessment for Healthcare 5.0 341
Duiena Rai, Anuradha Dhull, Akansha Singh, and Krishna Kant Singh

Correction to: Predictive Modeling to Identify Syndrome Patterns C1
Garima Jaiswal, Gargi Bhardwaj, Tarushi, Abhiruchi Sarswat, and Ritu Rani

Introduction to Security Risk Assessment in Medical and Healthcare Industry



Vandit Akhilesh Barola, Prabhishek Singh, and Manoj Diwakar

Abstract This is an introductory chapter of the book which, critically reviews the exponentially growing cybersecurity landscapes in the field of healthcare, specifically focusing on implantable medical devices. This chapter highlights the irony of how the medical devices that have been developed to improve human health have become mass targets for malicious cyber-attacks. It serves as a starting point to illustrate the complex as well as important role that cyber security plays in the field of healthcare, thus highlighting the need for implementing a strong defense network to reduce the escalating cyber threats. Through a detailed review of the real-world instances, this chapter unravels the importance of detecting and removing the vulnerabilities in implantable medical devices (IMDs) and Internet of Medical Things (IoMT) devices. The motivation of this chapter, that rigorous security assessments and multifaceted mitigation strategies are the foundational pillars of any secured healthcare infrastructure, is the culmination of an extensive literature survey. By fostering a proactive stance grounded on technological innovation and collective vigilance, healthcare stakeholders can bolster resilience against the pervasive threat of cybercrime. In essence, this chapter serves as a beacon of knowledge, guiding stakeholders towards a future where healthcare systems remain steadfast in safeguarding patient well-being and sensitive medical data from the ever-present and ever-evolving cyber threat landscape.

V. A. Barola (✉) · P. Singh
School of Computer Science Engineering and Technology, Bennett University, Greater Noida,
India
e-mail: technovandit18@gmail.com

M. Diwakar
Department of CSE, Graphic Era Deemed to Be University, Dehradun, Uttarakhand, India

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
P. Kumar et al. (eds.), *Healthcare Industry Assessment: Analyzing Risks, Security,
and Reliability*, Engineering Cyber-Physical Systems and Critical Infrastructures 11,
https://doi.org/10.1007/978-3-031-65434-3_1

1 Introduction

In the twenty-first century, technology is evolving at an exponential rate where humans are on the stage of converting themselves into semi-humanoids. In this era, doctor's main job—operation is shifting to the hands of robots, which is well termed as the technology of robotic arms. And unfortunately, with the evolution of this superpower technology, we are now also capable and well-grown to the evolving cyber-crime. Now, if there are 100 ways to protect a human being with the help of implanted medical devices or by any other means, there is an evolving rate of 1 method per day to defeat that technology and sentence the target person to death. The evolving technology is coming up with various cyber security challenges. One of the increasing threats is the advancement in the healthcare sector as the interconnectivity of the medical devices and clinical devices in the networked computing system leads to a high risk of creating vulnerabilities to security breaches. Today, many devices are available in the market that are prone to cybercrime such as implantable defibrillators, pacemakers, insulin pumps, implantable monitors and sensors, EHR systems, surgical robots, hospital infrastructure systems, and many more. These all were made to decrease the problems related to the biological aspects but now, also result in an increasing rate of cybercrimes. Attacks on all the devices listed above are the fact statements in the news articles.

1.1 Security Risk Assessment

Let's look at the statement that why should one want to attack such medical devices? There can be many reasons a financial cause may be one of the biggest reasons, where attackers demand a high payment for the information they had stolen or some of the political aspects of the society may matter. According to WHO the global market is surrounded with 2 million plus different medical devices. These devices include the list of all IMDs such as cardioverter defibrillators, pacemakers, neurostimulators, insulin pumps and all kinds of implantable drug-delivering systems, monitors and sensors, medical imaging equipment, EHR systems, and all kinds of connected wearable devices. Some of the major and heavy devices also include surgical robots, hospital infrastructure systems, telemedicine platforms, and various laboratory equipment. It can be very easy to understand the importance of security in such devices with the real-life encountered hacks which include the most powerful cyber-crime of the time on 5th July 2023, HCA Healthcare in Nashville, Tennessee where 11 million patient's data was breached and manipulated over 20 states. Similarly, an event occurred in December 2022 in Medibank which became the victim of an attack by a hacker group named Revil Ransomware gang who stole the personal data of over 9.7 million people including 1.8 million international customers including the great politician Prime Minister Anthony Albanese and cyber security minister Mr. Clare O' Neiland demanded for an amount of 10 million Dollars. These security

issues have not started at the current time, it has been there for several years back too. In 2012, Dr. Barnaby Jack a renowned cyber security researcher demonstrated a practical attack on a pacemaker, and he made a successful attempt to do this. He was able to perform his attack around 30–40 feet away from the person’s body through his laptop. This is not only one incident that has happened, in 2016, FDA warned about the vulnerabilities in certain ST. Jude Medical cardiac devices, in 2019 the vulnerability was found in Medtronic insulin pump that could give potentially access to the attacker to unauthorized insulin doses [1].

1.2 Mitigation Strategies

Various solutions have been developed by security teams across the globe if we talk about implantable medical devices robotic arms or hospital management networks they have implemented strict authentication and access control, encryption of all data, secure programming interface, wireless security, secure communication protocols, regular monitoring and auditing, rigorous security testing and certification, emergency access procedures, secure boot, regular software update, firewalls and intrusion detection systems, biometric authentication and the most important thing proper training and education about the medical device and it’s security to the patients. Now, we are still in a developing phase of the technology where many unbelievable things are to be made and as I have discussed earlier, evolving in technology will also lead to more security breaches and cyber-attacks. Training the medical staff as well as patients about the security risks associated with medical devices and how to potentially safeguard them from such attacks is definitely a pivotal element of imparting protection from such attacks as it enhances the awareness as well as the preparedness of the concerned people, thus aiding in the overall effectiveness of the security ecosystem in the era of evolving cyber threats.

1.3 Motivation of Work

With the increasing cyber security threats in the healthcare sector, the strong motivation is to address the concerned issues specifically with implantable medical devices. The growing technology leads to security risks by powering the robotic surgeries and interconnecting the medical devices. By encouraging awareness among healthcare professionals and implementing security protocols, aimed to fortify the strength of healthcare infrastructures against cyber security threats. Moreover, the motivation to write this chapter stands along with the dynamic updation in the technology which leads to generating more possible ways to create vulnerabilities in the healthcare ecosystem. Thus, combining all the leading strategies developed, reviewing a paper defines major possible threats associated with IMD security and stating the possible mitigation solutions to prevent the potential threats.

1.4 Contribution of Work

The primary focus of the paper is to understand the security solutions of the healthcare sector and cyber risks, particularly in implantable medical devices and the internet of medical devices. These are some of the key contributions of the work done in this paper.

The paper made a detailed overview of various factors that impact the security of medical devices such as equipment management, threats, networked medical devices, etc. by deconstructing all the factors and interconnecting them to make a set of protocols to decrease the potential threats on implantable medical devices and healthcare sector. Precisely analyze and jot down all the potential threats and vulnerabilities impacting on the IMDs such as denial of service attacks, man-in-the-middle attacks, patient data extraction, and device reprogramming. By projecting light on all these risks raising the potential awareness among healthcare stakeholders. Additionally, talked about various proposed mitigation strategies, in-depth analysis of the security solutions, experimental validation and recommendations, comprehensive conclusion and guidance. Overall, contributing to the advanced knowledge and understanding in the sector of healthcare cybersecurity, offering practical guidance and recommendations for mitigating cyber threats, thus warrants the integrity of patient care in an exponentially raising digitalized healthcare environment.

2 Literature Survey

Kim et al. provide practical guidelines for medical practitioners and patients to understand concerns related to the security risks related to medical devices and IoMT [2]. The author used the approach of analyzing the significant cases of security vulnerabilities in IoMT devices, outlining the need for a scientific, risk-based assessment. The study illuminates all these vulnerabilities through experiments, appreciating the importance of standardized and rigorous evaluations in this field. On top of this, the authors have examined and reviewed the cyber security vulnerabilities related to medical devices and the different methods of attack [3]. This study examines the conflict between the security of medical devices and the regulatory constraints imposed on manufacturers by governing bodies. The methodology used is based on a conceptual analysis of the issues surrounding cyber security vulnerabilities in medical devices by listing out examples of incidents, including their integration with networks and software. Addressing challenges with managing cyber security risks in the context of medical devices, such as the need for a socio-technical approach and the impact on clinical workflow.

With the evolution in the development of modern technologies in the medical era, cyber security risks also evolved at a rapid rate. Thus, the ways developed to prevent such cyber threats are discussed in [4]. The methodology used by the author is to find out the presence of malware on hospital servers and computers, monitoring

systems, and implanted medical devices. Managing the uncontrolled distribution of passwords, disabled passwords, hard-coded passwords, and poor coding/SQL injection for software of medical devices and main servers. In addition to identifying the requirements for traceability at each stage of the software development lifecycle, the paper describes the scope and diversity of traceability requirements within medical device standards and guidelines [5]. The report also summarises the results of our implementation in two SME organizations of a lightweight assessment tool (Med-Trace), which we developed based on the traceability procedures in these standards. The author follows a two-step process of methodology. Initially, an extensive examination of medical equipment regulations and recommendations was undertaken to pinpoint the traceability necessities throughout every phase of software development.

The following paper discusses how the security risks integrated with IoT devices in the healthcare sector together also known as IoMT devices [6]. This paper focuses mainly on the technologies of internet connectivity, which improves doctors to check the reports, on the other hand, it increases the risks of hacking those devices on the network channel. It deals with various domains such as major cyber-attacks that cause a major loss in the healthcare business, identifying various firmware/software/hardware weaknesses, gateways associated with the clouds, and app association with passage through wi-fi, PC, or mobile phones-based software. Additionally contributing to this paper, another paper also focuses primarily on the Internet of Healthcare Applications (IoHA) which leads to major issues like fatalities, decreased revenue, and reputation loss of the company [7]. Unlike the above paper, this paper proposes various proofs and protocols for IoHA combinedly known as Zero-Knowledge Proofs (ZKP) based on Authentication Key Agreement (AKA). To maintain integrity, anonymity, confidentiality, and safety from cyber security threats, it uses zero-knowledge proofs as physically unclonable functions, symmetric cryptography, biometrics, message digest, etc.

The paper mainly analyses the instances involving the Merlin-compatible cardiac implantable electronic devices (CIEDs) made by St. Jude Medical and the vulnerabilities that researchers discovered [8]. The experiment aimed to evaluate the critical clinical performance of medical devices in various scenarios. The methodology involved gaining practical advice on how to handle and evaluate cyber security issues about medical devices from cardiac electrophysiologists. The paper also emphasizes the necessity of following accepted scientific standards in security reports and advocates for a strict methodology in assessing and disclosing security issues related to medical devices. The paper addresses the security challenges in the context of IoMT security by focusing on the Robot Operating System (ROS)-based swing door automation in a robotic hospital framework [9]. Like others, this paper also tries to safeguard sensitive healthcare data and protect against potential cyber-attacks that could threaten patient health and compromise data confidentiality. The methodology used by identifying and discussing security issues within ROS1, emphasizes the need for improved information security, especially in medical applications. It analyses the common IoT attacks, such as Hijacking, Man-in-the-Middle (MITM), and DOS/DDOS, considering their in-healthcare domain. Proposed a security solution by providing ROS-based swing door automation, considering network setup,

cryptography aspects, and conceptual security policies. Comparing the advantages of different types of architectures leads to a recommended approach for the target application.

The paper refers to a crucial part of the healthcare sector i.e. the privacy and security of the medical images [10]. The author aims to propose a secure and efficient method for encrypting and decrypting medical images using various AI/ML models and deep learning techniques, specifically the ResNet-50 architecture. The goal is to contribute to the development of a robust system that ensures the confidentiality, integrity, and privacy of sensitive medical data. The author achieved the objective of the research paper [10] by using the concept of a deep learning approach, specifically using the Resnet-50 architecture, to extract features from chest X-rays and MRI images. These features are then used to generate encryption keys for securing medical images. By using Data Encryption Standard (DES), Advances Encryption Standard (AES) and Hash functions, such encryption processes are carried on. A lightweight cryptography technique is used to operate resource-limited devices efficiently. This paper also reviews the field work, by comparing all the encryption methods and their effectiveness. This paper also examines various rising cyber threats in the healthcare sector, such as anesthesia and intensive care, which were provoked by the widespread adoption of Electronic Medical Records (EMR), of Things (IoT) devices, and the COVID-19 pandemic [11]. This paper mainly focuses on the growing cyber threat because of the IoMT and increasing wireless connectivity of medical devices. The research delves into the chronic underfunding of cybersecurity in healthcare and its correlation with the rising incidence of cyberattacks. The impact of the COVID-19 pandemic on cybersecurity, coupled with changes in caregivers' working patterns, is also examined.

While examining the security implications of implantable medical devices (IMDs), the author tries to enclose open-loop as well as closed-loop systems [12]. The research categorizes various IMDs, inspecting the possible threats and security measures for devices like nerve stimulators, insulin pumps, and cochlear implants. Real-world examples highlight the risks, and design constraints, including urgent access, energy consumption, and device size are thoroughly explored. This paper also proposed different solutions such as close-range communication, cryptography and biometric access. This paper defines a descriptive overview, thus helping in understanding the security challenges in IMD devices [12]. While this paper research also analyzes the cybersecurity threats of wireless implantable medical devices (IMDs) such as insulin pumps, spanning cardiac implants, and neurological pulse generators [13]. Allowing integration of wireless controls in IMDs with the development of remote monitoring and control in the early 2000s, brought noticeable advancements in the healthcare sector but also raised concerns about potential malicious cyber attacks. According to the analyses of vulnerabilities in various IMDs underscores the immediate requirement for improved security measures. The methodology involves a thorough analysis of technological flaws, historical advancements, and human factors which impacts on IMD security. The most common manufacturer warnings and FDA safety communications suggested two examples of remedies that are examined as

stakeholder suggestions and machine learning algorithms. Despite technical challenges, collaboration among manufacturers, clinicians, researchers, and regulators is emphasized to fortify IMD security and address the increasing risks posed by cyber threats.

The threat of cyberattacks has grown in the healthcare industry in recent years, with ransomware incidents endangering patient care and resulting in large financial losses. The study of this paper explores how vulnerabilities in legacy software are exacerbating the growing cyber threats that target medical devices, including vital hospital hardware [14]. Because many medical devices run on antiquated systems and lack crucial security features, they are especially vulnerable to hacking. The goal of this research is to find different approaches to improve security in medical devices without having to replace outdated software. This scoping review was carried out using the Arksey and O'Malley framework and adheres to PRISMA guidelines. Using three highly cited "pearls" as search criteria, a bidirectional citation search method was used to generate the literature set, which consists of 849 studies. The English language, peer-reviewed status, and applicability to security solutions for medical devices running outdated software without a replacement were the main inclusion criteria. There were 35 studies in the final selection. With data charting, systems were categorized according to their types, risks, security measures, and analytic techniques. This thorough methodology lays the foundation for future research and enhanced cybersecurity measures in the healthcare sector by providing insightful information about the cyber solutions available for legacy systems in IMDs.

This paper examines the security threats associated with IMDs. It presents the surveys on IMD security, talks about the various intentions behind the exploitations of IMDs, and also discusses about potential threats to IMDs [15]. This review paper analyzes all the vulnerabilities and cyber threats by analyzing primary research articles, official reports, and incident reports. It discusses about the threats associated with defibrillators, and the recall of all Abbott ICDs in April 2018. FDA announced the recall of 350,000 ICDs. The concern was that the system contained the inbuilt programmable computer which caused vulnerability attacks and harm to the patient's body due to oversoon battery drain. Somewhere these IMDs offer more cyber-threats, due to their wireless connectivity. Also, electromagnetic interference attacks have the potential to target IMDs with several common technical faults. This paper offers some of the security solutions to prevent cyber threats on IMDs such as cryptographic keys, anomaly detection, distance control protocols, external devices, and many more.

The growing era of medical devices and the integration of software phases into it increases the potential growth of cyber security threats. The paper analyses the datasets of vulnerabilities in medical devices across 36 countries and examines the concerned landscape with a large number of medical devices purchased by national health services and more than half are deemed to be highly critical on more vulnerability risks [16]. This paper talks about various result analyses, exposures, severity, risks, weaknesses, and various OSINT methodologies. It also focuses on comprehension of the dataset including common vulnerabilities and exposures, platform enumeration, weakness enumeration, vulnerability scoring system, ICSMA along

with data mining, ethics and lawfulness of the analysis, limitation of these analyses, and extension and regulated work. Three fundamental detection methodologies, signature-based, anomaly-based, and specification-based are recognized. The study investigates the positioning of detection systems (including host-based, network-based, and cloud-based systems), the categories of analyzed data, the main attack scenarios, the datasets employed for Evaluation, and the methodologies that integrate preventive measures. Challenges unique to MCPS, such as real-time detection requirements, are underscored. The paper follows software engineering guidelines for structured reviews by adopting a systematic literature review as its methodology. A comprehensive database search is required to investigate 22 terminologies related to networked medical devices. The selection of pertinent, peer-reviewed studies published before March 2023 is ensured by inclusion criteria. Quantitative title and abstract evaluation are the first step in a two-step screening process; the qualitative full-text evaluation comes next. Data synthesis and extraction are conducted systematically, with one researcher verifying the precision of the data and another extracting it.

3 Comparative Analysis Based on Its Merits and Demerits

There is a collective emphasis on the critical intersection of cyber security and healthcare, particularly in the context of medical devices and systems. The merits tell us the significant growth of the identification of cyber security vulnerabilities and the development of effective solutions and protocols. However, challenges include the complexity of implementation, limited generalization of findings, and potential barriers for non-specialists. You can find the comparative analysis of merit and demerit in Table 1.

4 Result Analysis

The assessment of cyber security research in medical devices has experienced substantial progress. Upon thorough examination of the research findings, we have identified four primary factors pertaining to medical devices, specifically Equipment Management, Threats, Networked Medical Devices, and Risk Mitigation as shown in Fig. 1a. These factors are the primary determinants influencing the susceptibility of medical devices to external disruptions. As stated by the authors, the equipment management score for any medical device can be determined by adding together three score values: [FV] Function Value, [RV] Risk Value, and [RM] Required Maintenance [2]. The function value of any device can be determined by the sum of its four-factor scores: [CT] Connection Type, [DF] Data Flowtype, [DT] Data Type, and [FT] Function Type. The Risk Value can be calculated by multiplying three

Table 1 Merit and demerit

Paper	Merits	Demerits
[2]	Prioritize clinical impacts in assessing medical device security Propose unified evidence standard, urging collaboration for thorough vulnerability assessments	The need for improved cyber security practices within the medical device
[3]	Examines cybersecurity in networked medical devices identifies threats and analyses attacker motivations/methods Provides best practices for heightened awareness of cybersecurity challenges in healthcare	The paper lacks real-world examples and in-depth discussions on regulatory compliance Finding technical complexity and terminology challenges
[4]	Hospitals should use a threat modeling technique for assessing threats	Establish device priorities in security architecture for a clear role Hospitals should proactively enhance security measures for patient services
[6]	Implantation therapy improves adherence by simplifying dosage Medical implants boost comfort, convenience, satisfaction, and recovery Wearables and IoT devices enhance patient monitoring for informed, self-directed care	Emphasizes risks in implanted medical devices, including hacking Identifies threats: data extraction, tampering, reprogramming, persistent access Urges strong security measures, addressing healthcare cybersecurity concerns in networked devices
[7]	ZKP-AKA boosts IoT healthcare security Resource-efficient design minimizes impact Emphasizes secrecy and anonymity for privacy	PUF dependency: security relies on PUF integrity; tampering may disable devices Complex implementation: ZKP-AKA may be challenging due to cryptography requirements Compatibility limitation: only devices with PUF support can use the protocol
[8]	Helps electrophysiologists manage cybersecurity risks in medical devices Provides an experimental model to understand reported vulnerabilities Emphasizes evaluating security claims for accurate clinical insights	Limited generalization: findings may not apply to other devices Complexity for non-specialists: non-experts may struggle to evaluate device vulnerabilities
[9]	Comprehensive Analysis: Thorough examination of ROS security issues in the medical IoT context Application of proposed solutions to real-world robotic hospital scenarios Emphasis on conceptual security rules for a holistic approach Recognition of the importance of an isolated network for enhanced security	Primarily focuses on ROS1, with limited coverage of ROS2 Tailored to swing door automation in a robotic hospital, limiting generalizability Theoretical soundness lacks empirical validation for practical effectiveness

(continued)

Table 1 (continued)

Paper	Merits	Demerits
[10]	<p>Deep learning and cryptography ensure robust medical image security</p> <p>ResNet-50 enhances accuracy for improved system efficiency</p> <p>Deep learning-based encryption safeguards privacy in medical image storage</p> <p>Connects medical equipment for enhanced healthcare data handling</p>	<p>Integration demands specialized knowledge</p> <p>ResNet-50 requires substantial computational resources</p> <p>Effectiveness depends on diverse medical datasets</p> <p>Despite efforts, concerns persist. Careful implementation is crucial</p>
[11]	<p>Facilitates instant communication among healthcare devices</p> <p>IoT enhances treatment options and expedites patient care</p> <p>Allows for extensive data collection aiding in decision-making</p> <p>EMR and wireless connectivity offer advanced healthcare possibilities</p>	<p>Chronic lack of funding exposes healthcare to severe cyber threats</p> <p>Proliferation of IoT devices increases vulnerability</p> <p>Use of obsolete hardware and software raises cyber risks</p> <p>Despite safeguards, human error remains a cybersecurity weak point, requiring ongoing training</p>
[12]	<p>The review provides an in-depth examination of diverse IMDs, illustrating their vulnerabilities and security measures</p> <p>The inclusion of practical instances, like cyberattacks on insulin pumps, enhances the relevance of the discussion</p> <p>The paper systematically categorizes information, aiding clarity and comprehension</p> <p>The need for advancements in IMD security is ongoing due to the evolving nature of cyber threats, as shown by the inclusion of future research directions</p>	<p>The paper briefly touches on potential solutions without delving into recent technological developments, missing an opportunity to showcase evolving solutions</p> <p>The review lacks a comparative assessment of proposed solutions, leaving readers with limited insight into their relative effectiveness</p> <p>Ethical implications, such as privacy concerns and informed consent, are briefly mentioned but not extensively explored, presenting an area for further investigation</p>
[13]	<p>Comprehensive exploration of cybersecurity risks in wireless IMDs</p> <p>Identification of vulnerabilities in various devices</p>	<p>Technical limitations and challenges in implementing security measures</p> <p>Reliability and battery life constraints affecting security features</p> <p>Lack of widespread awareness and education among clinicians</p>
[14]	<p>Diverse solutions addressing different aspects of security vulnerabilities</p> <p>Practical applications for both implantable and non-wearable devices</p> <p>Integration of intrusion detection and prevention mechanisms</p>	<p>Some solutions may introduce inconvenience for users (e.g., wearing external devices)</p> <p>Potential legal and ethical concerns with indiscriminate jamming</p> <p>Challenges in protecting against all types of attacks</p>

(continued)

Table 1 (continued)

Paper	Merits	Demerits
[15]	Comprehensive overview of realistic security threats to IMDs Highlights NIST and FDA frameworks for structured security Presents a concise timeline of recent IMD attacks Advocates for stringent security tests by manufacturers	Lacks real-life instances, potentially impacting urgency Risks associated with easily accessible, inexpensive hardware Notes a gap in patient understanding of IMD security risks
[16]	It offers a detailed overview of intrusion detection in Medical Cyber-Physical Systems (MCPS), addressing unique healthcare challenges Categorizes detection approaches, explores placement and data analysis methods, and discusses attack scenarios and preventive measures	Focus on research until March 2023 may overlook recent developments in MCPS attack detection Use of 22 synonyms introduces complexity, potentially oversimplifying nuances in securing specific device types A unified MCPS framework may oversimplify diverse medical devices, lacking nuanced considerations for specific device types

separate scores: (PR) Physical Risk, (AOP) attack occurrence probability, and (ASP) attack success problem (Fig. 2).

Now, let’s delve into another significant element that impacts medical devices: Threats. The following are the most susceptible factors that could impact the entire healthcare system. Most of the medical devices in the market are introduced following approval from government regulatory agencies. However, as a result of advancements in hacking technologies, hackers continuously discover novel methods to potentially

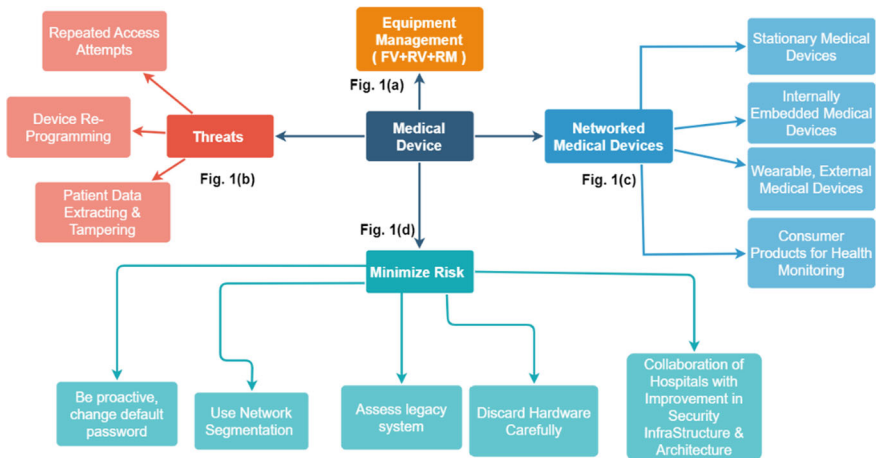


Fig. 1 Factors of medical devices [2, 4, 6]

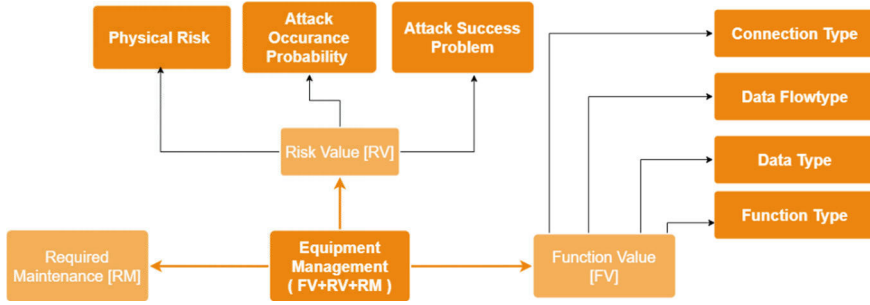


Fig. 2 Equipment management [2]

interfere with the regular operation of medical devices. Figure 1b identifies the most prevalent threats as Repeated Access Attempts, Patient’s information extraction, patient information tampering, and device reprogramming [6]. Patient data extraction and tampering involve the retrieval of diverse patient information to obtain comprehensive knowledge about the patients and subsequently manipulate their information to easily intimidate them. Device reprogramming threats involve modifying the logical components of a device, resulting in changes to its functionality, and modifying the device’s program code resulting in the temporary halt of regular operations and a subsequent reboot with the updated program capabilities. Repeated access attempts can disrupt the networking of medical devices. If the network security is weak, the devices can be compromised, resulting in a cyber threat attack.

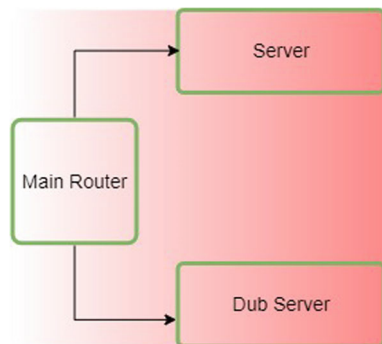
Now that we have comprehended the risks posed by medical devices, let us delve into the topic of networked medical devices Fig. 1c. The devices are classified into four categories: internal embedded medical devices, consumer goods for monitoring health, stationary medical, and wearable or external medical equipment [6]. Internally embedded medical equipment, are those IMDs that are injected into the human body, such as Pacemakers and ICDs. These devices possess crucial attributes including a small and efficient design, extended battery longevity, and secure wireless communication that adheres to all networking protocols. Stationary Medical Devices, in contrast to implantable medical devices, can have larger dimensions and can be either wired or wireless. Consumer Products for healthcare include Bluetooth operatable devices like various fitness trackers which are communicating themselves with adjoining personal smart phones. Mobile insulin pumps, continuous glucose meters, and wearable ECG monitors are classified as wearable or external medical devices.

Now after studying various networked medical devices and their threats to these devices, a very important factor is to be discussed known as “Minimize Risk” refer to Fig. 1d. Minimization of risk is very crucial when we are dealing with networked medical devices. As per the FDA, the primary reason for recalling medical devices from patients is the identification of vulnerabilities that pose risks to patient health. As a result, the medical device manufacturing companies incurred significant financial losses. There exist numerous strategies to scale down the risks associated with medical equipment. Here, we will find out the frequent methodologies used by

medical device manufacturing companies. The most common and important practice is to be proactive and change the default passwords by the user. Whenever a new device is supplied from the factories, they have default usernames and passwords, which leads the attacker to get a chance to penetrate your device. This proactive measure can reduce the chance of such unauthorized access. The term “Be Proactive” outlines the importance of taking initiative and addressing potential cyber security risks before they become actual threats [6]. This is the most common and easiest way to reduce the probability of hacking our device by changing its passwords on a regular interval of time, even when not required.

To improve the network security of hospitals and bigger architecture, the process of network segmentation is used in which a particular network is broken down into several segments. Where each segment consists of a different set of rules and regulations, their functions are different by applying different firewalls, and routers on each node based on requirements to regulate the traffic flow of information across the whole architecture [6]. Implementing all these practices reduces the risk of potential threats. If the attacker succeeds in breaking the protocol, the rest of the network system is protected. Like network segmentation, Collaborate with Hospitals for Improved Security Infrastructure and Architecture also plays a crucial role in enhancing complete security measures by establishing partnerships with other healthcare institutions to share insights, best practices, and threat intelligence. Collaborating on the development and implementation of standardized security measures helps create a comprehensive and proactive security strategy for medical devices. This strategy aims to reduce vulnerabilities, protect sensitive information, and strengthen the overall resilience of the healthcare infrastructure. Additional features to the Network Segmentation include the network infrastructure consisting of Wi-Fi repeaters, a sturdy main router, with separate routers for every floor of the medical institutions. In Fig. 3, the primary server/DUB server, the floor routers, and the main router are interconnected using physical wired connections. Repeaters are employed to enhance the wireless coverage offered by these floor routers [9]. The floor routers are equipped with dedicated wired connections to the cameras situated on each floor.

Fig. 3 Segmentation of network [9]



After using applying all the crucial steps to minimize the security risks, if the legacy systems of the softwares are not checked and updated thoroughly, it may create a risk of any vulnerability in the software. Legacy systems are the outdated software, patches that include hardware, software, file formats, or programming language. So, it is necessary to update the software patches regularly so that nobody can access the legacy systems of the devices [6]. But what about the old software and hardware, which are now not in current use? Here comes another way to discard hardware carefully. Disposing of all the components of hardware and software patches is very important from the view of security domains. As the old patches are vulnerable to cyber threats and malicious attacks [6]. This systematic archival will not only help in the disposal process, but also provide the staff with a thorough audit trail, which is particularly useful in compliance and security procedures. The disposal protocols involve total destruction of the hard drives and disposing of them in an ecologically sound manner. These protocols, including physical destruction of the components wherever required, should be properly supervised to ensure that the guidelines for hardware disposal are strictly observed and at the same time there is no compromise with the privacy (personal data) of the patients. Thus, the process of disposal of obsolete hardware components involves a collaborative effort by people from various disciplines such as IT staff, cybersecurity specialists, management committee of the organization etc.

To achieve this goal, we need to establish the collaboration of hospitals with the improvements in security and architecture, also implementing the robust encryption methods. There is a very simple concept behind this strategy by transforming data into an incomprehensible format so that, unauthorized access could be easily routed. To successfully implement the encryption mentioned in Fig. 4, the very first step is to identify the datasets that require additional security measures, specifically those that contain private or medical records. By implementing this measure, the data's confidentiality and integrity are preserved, rendering it indecipherable to unauthorized individuals even if intercepted. The meticulous preservation of encryption keys, which are indispensable for deciphering the encrypted data, is equally crucial. To prevent unwanted access, these keys must be stored securely. To enhance overall security, it is imperative that they are regularly updated. Healthcare systems can enhance their security and protect sensitive medical data from potential risks by integrating these encryption measures [10].

In Fig. 5, a detailed review of IMD security solutions is covered [13]. Here, Auditing refers to keeping a record of detailed logs of device activity and access events. This helps in diagnosing the malicious and unintentional faults which can be implemented in the mechanism that detects the anomalous activity and submit the report to the patient and clinicians. Bug Reporting is a post-market surveillance mechanism that identifies security flaws and patches them swiftly. Adding more than one form of authentication to the IMDs increases the challenges for the attackers like Biometric Access with other key passwords that are specific to the patient access control, and this defines the term Multi-Factor Authentication. Now, the most important term referred to is Education of proper security and awareness of IMDs and their

Fig. 4 Encryption technique [10]

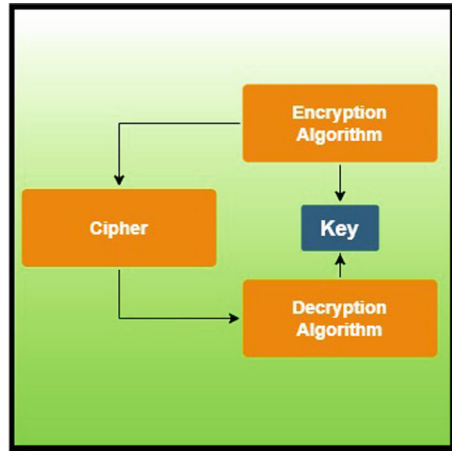
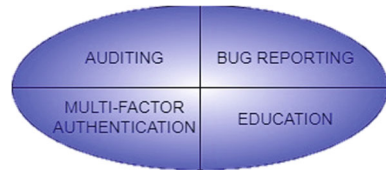


Fig. 5 Safety measures for IMDs [13]

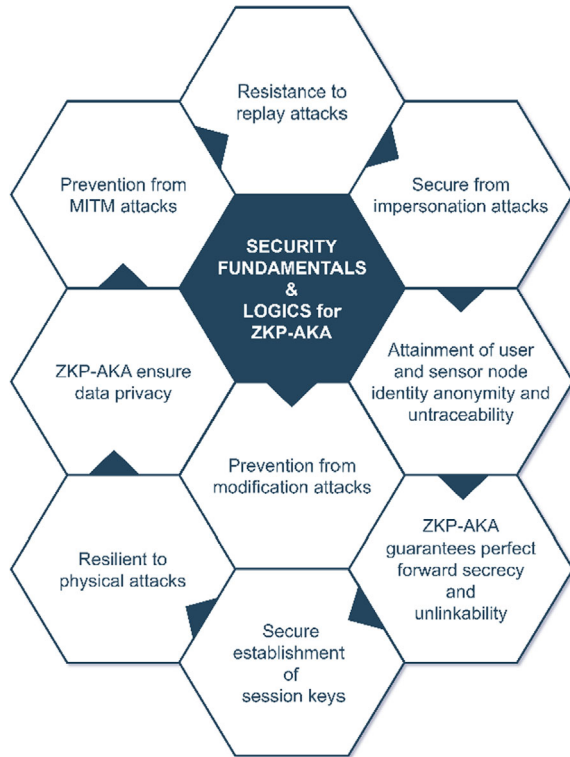


cyber security vulnerabilities. As per the report, the awareness of cyber security risks among clinicians is very low and finds lacking efforts in designing the secure IMDs.

Now let's understand all the theorems proposed by the authors as shown in Fig. 6. Resistant to replay attacks: the system's robust resistance against replay attacks is demonstrated. When an adversary attempts to reuse a captured message to gain unauthorized access, the security mechanism effectively neutralizes the threat by incorporating a cryptographic measure known as a "nonce." This defense not only safeguards the specific message in question but extends its protective capability to other critical messages within the system. The proof succinctly establishes the system's resilience, affirming its efficacy in countering replay attacks and ensuring the integrity of secure communication and access to authorized resources.

Prevention from MITM Attacks: This methodology can be achieved by assigning temporary identities and protecting important information, such protocols make it more difficult for successful attacks. Secure from imposture attacks, explains the situation, where an attacker tries to stealth the secret conversation and manages to get the information. However, the attacker fails to gain the correct information, because at the IOT sensor node, a scalar product MF is sent instead of M and F, which ensures complete privacy of information. Data privacy is ensured by the Zero-Knowledge Proof Authenticated Key Agreement (ZKP-AKA), particularly in messages containing encrypted data. Unauthorized access is prevented by safely storing the decryption key in reliable organizations. Attainment of user and sensor

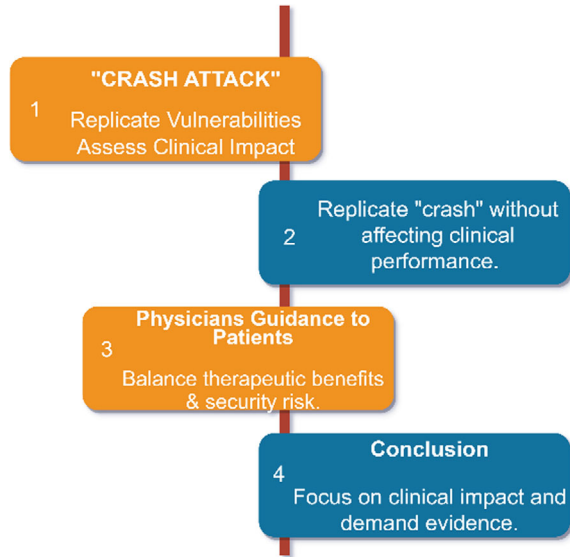
Fig. 6 Security fundamentals and logics for ZKP-AKA [7]



node identity anonymity and untraceability, this theorem prevents the traceability of user and sensor node identities by assigning temporary identities for users and new identities for each session, thus ensuring a certain level of privacy. **Prevention from Modification Attacks:** Because any changes made by the attackers can be quickly detected at the gateway, which results in the termination of the current session, thus preventing potential attacks, this protocol is impenetrable to modification attacks. **Resilient to Physical Attacks:** The protocol is resistant to physical attacks and prevents tampering and cloning by adversaries thanks to the use of Physical Unclonable Functions (PUF) in user devices and Internet of Things sensor nodes. **Secure Establishment of Session Keys:** ZKP-AKA encrypts session keys before transmission to guarantee their secure establishment. The encrypted keys are kept private and need data that is only possessed by reliable parties to be decrypted. **Guarantee of Perfect Forward Secrecy and Unlinkability:** ZKP-AKA uses different session keys for every session and modifies the random secret with each session to ensure perfect forward secrecy and unlinkability. Future and previous session keys stay safe and separate even if one is compromised [7].

A Rigorous approach for resolving the cyber security issues in the medical sector which underlines the requirement for security research standards, is discussed in this paper. It analyzes the Security Research Standard and disputes that reports should be

Fig. 7 Crash attack model [8]



assessed in clinical settings to guarantee suitability and relevance. The experimental model is shown in Fig. 7, which demonstrates the “Crash Attack” model that evaluates their clinical impacts [8]. We can find the significance in the experimental findings of the paper on how the ‘Crash’ model was successfully recast without affecting clinical performance. The model also covers physician guidance to patients, supporting an excellent strategy that takes security concerns and therapeutic benefits into account.

This paper focuses on how important it is to put patient safety before cyber security regulations in the healthcare system [3]. It points out the challenge of finding a balance between the ways to reduce compromises and guarantees patient safety in this era of constantly changing cyber security threats. This paper highlights the significance of medical devices and calls for increased cooperation among medical physicists, IT specialists, device manufacturers, and networked devices vendors, to ensure and maintain the security protection of medical devices. It emphasizes that while cybersecurity flaws in medical devices are like those in other networked systems, they pose a special risk because they could affect patient safety. They mentioned about the challenges that currently exist, like inadequate risk management, a lack of governance, and a lack of awareness and preparation on the part of organizations. Although adherence to laws like HITECH and HIPAA is acknowledged, it is stressed that adherence alone does not guarantee effective security. Though its global adoption has been slower, the proactive approach to cybersecurity awareness in healthcare, driven by data breach legislation, is acknowledged. The three-step plan that Fig. 8, outlines in its conclusion is to first understand the vulnerabilities that are currently in place, then integrate cybersecurity into the architecture and development of medical devices, and finally establish accountability through standards and regulatory oversight. The transitional period is acknowledged to potentially result in adverse outcomes for patient

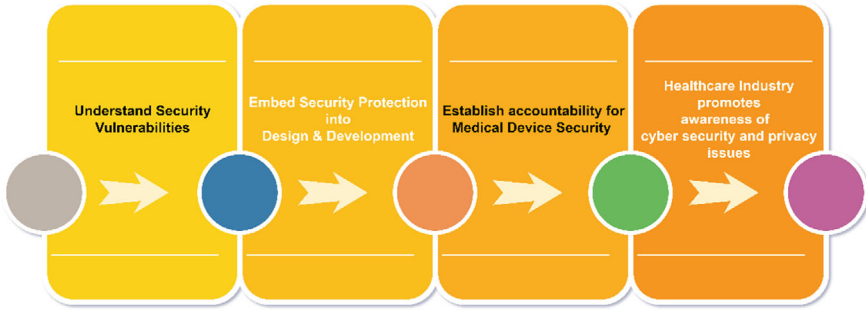


Fig. 8 Way to secure medical networks [3]

safety, emphasizing the need for a clear, workable process, enhanced awareness of vulnerabilities, and a perceptual shift.

For the enhancement of the security of implantable medical devices (IMDs), there is some set of rules/properties to be considered such as proper authentication, authorization, availability, non-repudiation, integrity, confidentiality, and patching. Now let's discuss each property one by one [12].

- Authentication refers to knowing about the proper identity of communicating devices to the IMDs.
- Whereas authorization means having proper rights to use the resource of the device or manage the device like the task of reprogramming of IMD must be done under collaborative oversight of technicians and doctors.
- Availability is the service that IMD provides to the patient and doctors. If the attacker used active jamming and succeeded in blocking the radio channels, then it means the availability of IMD is disturbed.
- Non-repudiation is a kind of task to store and verify the actions that are performed in the IMD device by checking the user logs. However, the current IMDs do not have logging in due to the memory and battery constrained.
- Integrity refers to the detection of any loopholes in the security threats and protection of any manipulation of parameters and reverse engineering.
- While confidentiality means the data of the device should only be accessed and read by authorized parties.
- Patching refers to the repetitive security testing before the deployment and also needs to be regularly updated to mitigate new security threats.

Several security solutions are also developed to strengthen the overall security framework of IMDs in response to various security concerns are shown in Fig. 9. It involves the method of Close Range Communication by introducing radio frequency identification (RFID) tag which can be attached to the IMDs and this RFID reader, reads the information in the tag. To protect the tag also it has an additional layer of liquid seal [12]. These RFID tags provide an additional data security against illegitimate entry which stores vital patient information. In addition to RFID, near-field