Chapter 11

Responsible IoHT Ecosystem for Smart Healthcare

Md. Hasanul Ferdaus,[a,*] *Fares Alharbi,*[b] *Savitri Bevinakoppa,*[c] *Md. Sawkat Ali,*[a] *Mohammad Manzurul Islam,*[a] *Maheen Islam,*[a] *Taskeed Jabid,*[a] *Sadia Nur Amin*[a] and *Rajkumar Buyya*[d]

1. Introduction to the Internet of Health Things

1.1 Definition and Scope

The Internet of Health Things, simply IoHT, means the application of Internet of Things (IoT) technologies in the healthcare sector [1]. IoHT forms networks of interconnected medical devices, sensors, software applications, and health-monitoring systems that communicate with each other to collect, analyze, share, and store health-related data through internet connectivity. This reduces human intervention in the processes and aims at enhancing healthcare delivery and patient outcomes [2]. These

[a] Department of Computer Science and Engineering, East West University, Dhaka, Bangladesh.
[b] Department of Computer Science, College of Computing and IT, Shaqra University, Shaqra, Saudi Arabia.
[c] School of IT and Engineering, Melbourne Institute of Technology, Melbourne, Australia.
[d] School of Computing and Information Systems, The University of Melbourne, Melbourne, Australia.
Emails: faalhrbi@su.edu.sa, savitri@mit.edu.au, alim@ewubd.edu, mohammad.islam@ewubd.edu, maheen@ewubd.edu, taskeed@ewubd.edu, sadian.amin@ewubd.edu, rbuyya@unimelb.edu.au
* Corresponding author: hasanul.ferdaus@ewubd.edu

interconnected devices such as wearable health trackers, implantable sensors, and remote monitoring systems are designed to collect real-time information on a range of health indicators such as body temperature, blood pressure, heart rate, glucose levels, and oxygen saturation. The IoHT integrates patient data seamlessly which enables healthcare providers to monitor health conditions continuously, make data-driven decisions, and deliver personalized care in a timely manner. IoHT systems reduce the need for frequent in-person visits and enable proactive health management, primarily for chronic conditions, which contributes to enhanced healthcare efficiency.

The impact of IoHT extends beyond mere patient care. It facilitates advancements in healthcare research, predictive analytics, and clinical trials. IoHT facilitates the analysis of large-scale health data. This enables researchers to identify trends, assess the effectiveness of treatments, and detect potential outbreaks. This way IoHT supports evidence-based medical practices. Notwithstanding the immense benefits and potentials of IoHT technologies, this digital transformation brings forth significant challenges, such as cybersecurity, data privacy, and system interoperability. Such hurdles and issues must be addressed to ensure IoHT systems are safe, reliable, and compliant with healthcare standards.

1.1.1 The Architecture of IoHT

The IoHT has a multilayer architecture that integrates various components at different layers to support data collection, processing, transmission, and storage. This layered architecture ultimately facilitates secure and efficient healthcare delivery [3]. Typically, the IoHT architecture comprises four main layers at its core (Figure 1): the Sensing Layer, the Network Layer, the Processing and Storage Layer, and the Application layer [4–6]. Each of these layers serves distinct functions within the healthcare ecosystem.

- **Sensing Layer:** This is the foundational layer where various IoHT devices, such as wearable health trackers, implantable devices, smart medical devices, and environmental sensors, collect relevant data. These devices continuously collect healthcare data, such as heart rate, glucose levels, temperature, and patient activity, through monitoring of physiological and environmental parameters. Various edge devices that pre-process data to reduce latency and bandwidth requirements are also included in this layer.
- **Network Layer:** The network layer transmits data securely from IoHT devices to the cloud or healthcare information systems for further processing and storage. This layer contains wireless communication technologies such as Wi-Fi, Bluetooth, cellular networks, and emerging

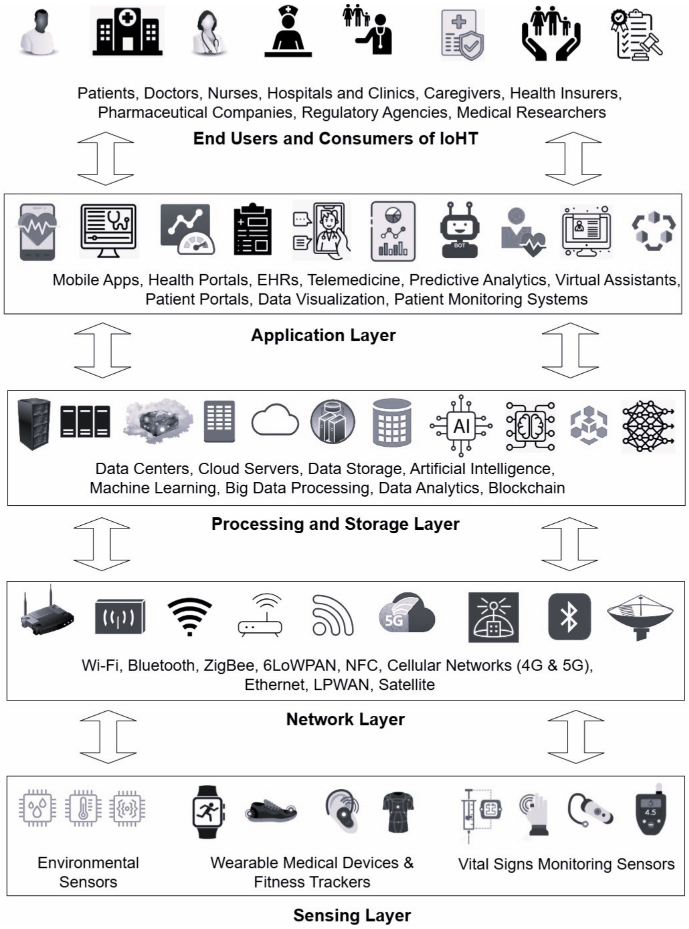
Patients, Doctors, Nurses, Hospitals and Clinics, Caregivers, Health Insurers,
Pharmaceutical Companies, Regulatory Agencies, Medical Researchers
End Users and Consumers of IoHT
BOT
Mobile Apps, Health Portals, EHRs, Telemedicine, Predictive Analytics, Virtual Assistants,
Patient Portals, Data Visualization, Patient Monitoring Systems
Application Layer
AI
Data Centers, Cloud Servers, Data Storage, Artificial Intelligence,
Machine Learning, Big Data Processing, Data Analytics, Blockchain
Processing and Storage Layer
5G
Wi-Fi, Bluetooth, ZigBee, 6LoWPAN, NFC, Cellular Networks (4G & 5G),
Ethernet, LPWAN, Satellite
Network Layer
4.5
Environmental Sensors
Wearable Medical Devices & Fitness Trackers
Vital Signs Monitoring Sensors
Sensing Layer

Figure 1: Layered architecture of IoHT.

5G technology. Such communication facilities enable seamless data transfer across devices and systems. This layer is responsible for ensuring appropriate security protocols are put in place to protect the data from unauthorized access and interception during transmission.

- **Processing and Storage Layer:** This layer includes data centers and cloud servers where large volumes of patient data are stored, processed, and analyzed. In some cases, this layer can be incorporated into the network layer. Analytical techniques leveraging Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) algorithms can be utilized in this layer to extract actionable insights from raw data, such as identifying health trends or predicting potential health risks.

- **Application Layer:** This layer interacts directly with patients and healthcare providers by presenting analyzed data via user-friendly interfaces. Mobile health applications, electronic health records (EHRs), and healthcare management platforms are included in this layer. These facilities allow patients, doctors, and caregivers to access healthcare data and make informed decisions. Various health alerts and notifications can be generated in this layer so that immediate medical intervention can be carried out whenever necessary.

This multilayered architecture of IoHT supports seamless flows of healthcare data from sensors to relevant observation and practical recommendations. Moreover, the integration of security protocols at each layer addresses data privacy and integrity challenges which are extremely crucial for secure and effective functioning of digital health ecosystems.

1.1.2 The Scope of IoHT

The IoHT represents a significant evolution in healthcare technology that integrates advanced connectivity with health-related devices. This enhances patient care, streamlines operations, and promotes better health outcomes. The IoHT aims to create a holistic ecosystem by leveraging the power of cutting-edge IoT technologies within the healthcare sector. This connects patients, medical providers, and healthcare systems, bringing them under a single umbrella. The following key points outline the expansive scope of IoHT [3, 4, 6–8] (Figure 2):

- **Remote Patient Monitoring:** IoHT facilitates continuous and remote monitoring of health data through wearable devices, smart sensors, and medical implants. These devices sense and collect vital health data such as heart rate, blood pressure, blood oxygen levels, glucose levels, and body temperature. This assists in providing real-time health information to both patients and healthcare providers, which in turn facilitates timely interventions and personalized care.
- **Telehealth Services:** Integration of IoHT facilitates virtual consultations and telemedicine services, and improves access to care for patients in remote or underserved areas.
- **Personalized Medicine:** By analyzing data collected from health devices, IoHT supports tailored treatment plans that align with individual patient needs and preferences.
- **Enhanced Data Analytics:** IoHT devices collect and generate vast amounts of healthcare data that can be harnessed for predictive analytics. This can help in early disease diagnosis and prevention and facilitate in creating personalized care plans.

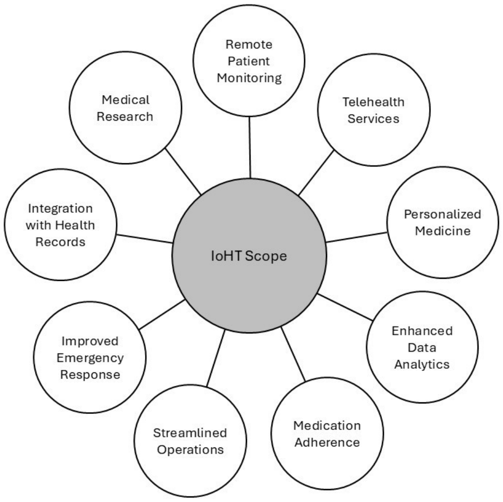

Figure 2: The scope of the IoHT.

- **Medication Adherence:** Digital tools and apps, such as smart pillboxes and reminders, connected to IoHT can improve medication adherence among patients, particularly the elderly and those with chronic conditions.
- **Streamlined Operations:** Healthcare provider organizations, such as hospitals and clinics, can utilize IoHT for efficient management of resources, such as staff allocation and inventory control. Moreover, they can optimize operations through automated workflows and real-time tracking of medical equipment. This can potentially lead to increased efficiency and cost-effective solutions.
- **Improved Emergency Response:** Smart sensors, medical gadgets, and other IoHT-enabled devices can alert healthcare providers in emergencies by tracking vital signs and detecting early signs of chronic diseases. This can ensure timely interventions and potentially save lives.
- **Integration with Health Records:** IoHT can seamlessly integrate with EHRs and enable comprehensive patient profiles, thus empowering healthcare providers in decision-making.
- **Medical Research:** IoHT has been accelerating medical research by enabling large-scale data collection and analysis for drug discovery and personalized treatment plans.

In summary, the scope of IoHT covers a broad spectrum of applications and services. These applications and services, through their enhanced efficiency and data-driven insights, collectively strive to revolutionize healthcare delivery, improve patient outcomes, and reduce operational costs.

1.2 The Rise of IoHT

The rise of the IoHT has been accelerated by progressive technological advancements, the integration of connectivity, and healthcare demands. The rapid evolution of IoHT has reshaped patient-centered care and health system efficiencies. The inception of digital health technologies has its roots back in 1947 when the initial steps into the digital revolution began with the emergence of transistors and integrated circuits [9]. Initially, IoHT appeared as a part of the broader IoT movement. As wearable devices and remote monitoring technologies become more prevalent, IoHT quickly gained traction among the stakeholders of the healthcare industry. IoHT can be traced back to the early 2000s when wireless communication technologies and the miniaturization of electronic devices fostered the development of wearable health devices such as fitness trackers, activity monitors, sleep trackers, and heart rate monitors.

Early applications primarily focused on fitness tracking and chronic disease management. Advancements in sensor technologies, AI, and data analytics have expanded the potential and efficiency of IoHT technologies. However, IoHT has seen its true proliferation with the improvements in cloud computing, big data analytics, and AI. Gradually the field has seen exponential growth over time through the development of various applications such as high-throughput genomic sequencing, robotic care assistants, and EHRs [10, 11]. Today, a wide range of medical applications and services function in the field of IoHT, including telemedicine, remote diagnostics, personalized treatment plans, and predictive healthcare. These technologies have improved operational efficiency, patient outcomes, and public health responses, enhancing global healthcare services significantly [12, 13]. For example, in the field of cardiovascular care, the application of digital technologies has shown promising results in reducing morbidity and mortality rates. To accommodate digital health technologies and tools, regulatory frameworks have also been adapted. This emphasizes the need for collaboration among stakeholders for successful implementation in IoHT development.

From the inception of IoHT, the development of the IoHT can be discussed as a five-stage process (Figure 3):

- **Initial Connectivity and Data Collection:** The early stages of IoHT started with basic health devices, such as fitness trackers and glucose monitors, that collect vital health data. These health devices had data communication services for basic data sharing. This laid the foundation for more advanced IoHT applications.

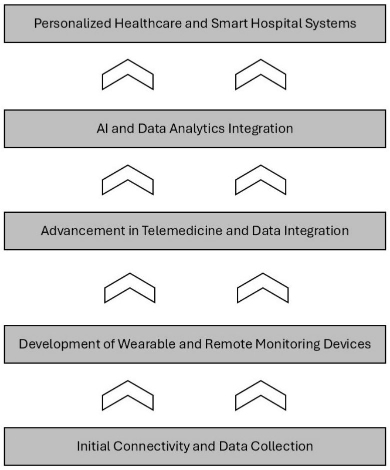
Personalized Healthcare and Smart Hospital Systems
AI and Data Analytics Integration
Advancement in Telemedicine and Data Integration
Development of Wearable and Remote Monitoring Devices
Initial Connectivity and Data Collection

Figure 3: The rise of IoHT development.

- **Development of Wearable and Remote Monitoring Devices:** Later wearables and sensors were developed which were capable of continuously tracking health metrics, such as heart rate and blood oxygen levels. This facilitated remote patient monitoring services that were helpful for the early detection of health issues without hospital visits.
- **Advancement in Telemedicine and Data Integration:** The proliferation of wireless technologies and global internet connectivity paved the way for efficient real-time data transmission from devices to healthcare providers. Professional-grade telemedicine services were developed by leveraging this connectivity. Moreover, the health data were integrated with EHRs through efficient communication facilities for creating holistic patient profiles.
- **AI and Data Analytics Integration:** The various health devices collect and generate large volumes of health data by monitoring patients and their environments. This opened the opportunity to apply AI algorithms and tools for predictive analytics to identify trends and patterns that are leveraged for proactive healthcare measures.
- **Personalized Healthcare and Smart Hospital Systems:** Through the development of mobile applications and integration with cloud services, the IoHT capabilities now support personalized medicine and smart hospital systems. It enables patient-centered care with predictive insights, efficient use of resources, and better patient outcomes.

2. Understanding the Cybersecurity Landscape in Digital Health

2.1 Unique Risks Posed by IoHT Devices

The IoHT connects sensors, medical devices, and healthcare systems to facilitate real-time patient monitoring and health data exchange. This integration improves the efficiency and outcomes of healthcare services. However, it also introduces unique security risks due to the sensitive nature of health data and the high level of interconnectedness of medical devices [14]. The IoHT devices are often highly specialized, resource-constrained, and deployed in sensitive environments. This makes them vulnerable to cyberattacks and privacy breaches.

Usually, traditional medical systems operate within controlled environments. Unlike this, IoHT devices often function in less secure settings, such as patients' homes or wearable technologies. This can make them more vulnerable to exploitation. Moreover, the growing number of connected medical devices exacerbates these issues by expanding the attack surface and increasing the likelihood of security breaches. A compromised device could lead to the exposure of personal health information (PHI). This could have serious legal and ethical consequences for healthcare providers. The proliferation of IoHT devices has introduced new and complex security challenges. Understanding the specific risks posed by IoHT devices is essential. This knowledge helps in developing robust security measures to protect patient safety and ensure data privacy and integrity [15]. Figure 4 presents a taxonomy of the unique security risks posed by IoHT devices. These risks are further discussed below [16–18].

- **Limited Security Capabilities:** Many IoHT devices are designed with limited computational power and memory. This restricts their ability to implement strong security protocols such as encryption and authentication. As a result, such limitations make them easier targets for cyberattacks.
- **Unauthorized Access:** The IoHT devices can serve as entry points for malicious actors to gain unauthorized access to sensitive patient data due to their interconnected nature. This has the potential to disrupt healthcare operations and even compromise patient safety.
- **Data Breaches and Privacy Violations:** Wearable Internet of Medical Things (WIoMT) devices are particularly vulnerable to security risks. Examples include smartwatches, fitness bands, and other health-monitoring wearables. Such gadgets are frequently used for constant tracking of health metrics and transmitting real-time data to healthcare providers. This can make them vulnerable to data breaches if sufficient

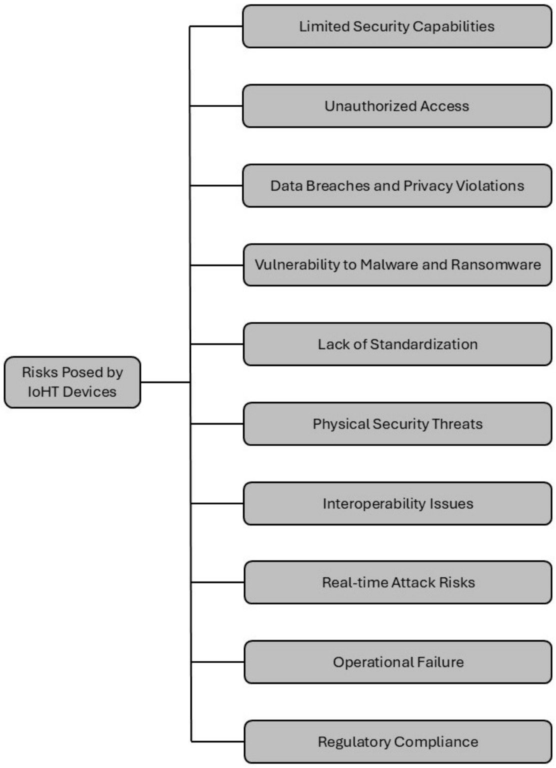
Risks Posed by IoHT Devices
Limited Security Capabilities
Unauthorized Access
Data Breaches and Privacy Violations
Vulnerability to Malware and Ransomware
Lack of Standardization
Physical Security Threats
Interoperability Issues
Real-time Attack Risks
Operational Failure
Regulatory Compliance

Figure 4: A taxonomy of the unique risks posed by IoHT devices.

protection mechanisms are not employed. As a consequence, this can expose patients to identity theft, discrimination, and privacy violations. Furthermore, the sharing of patient data between different healthcare providers and organizations can increase the risk of data breaches and unauthorized access. This raises security concerns requiring a focus on security and privacy measures to protect users' personal information.

- **Vulnerability to Malware and Ransomware:** IoHT devices often operate on outdated or unsupported software. This makes them vulnerable to malware and ransomware attacks. Such malware and ransomware have the potential to disable critical medical equipment and compromise patient safety.
- **Lack of Standardization:** The lack of uniform security standards across IoHT devices and manufacturers leads to inconsistent security practices. This effectively increases the overall risk of vulnerabilities in healthcare ecosystems.

- **Physical Security Threats:** IoHT devices can be physically accessed by unauthorized personnel as they are deployed in hospital environments. This increases the risk of device tampering or device theft.
- **Interoperability Issues:** Due to the inherent heterogeneity in the design and implementation, IoHT devices from different manufacturers often lack seamless interoperability. This can lead to communication gaps and vulnerabilities in data transmission between devices and healthcare systems. As a result, such interoperability issues make it easier for attackers to exploit the weak points.
- **Real-time Attack Risks:** Many IoHT devices are deployed for providing real-time monitoring of critical patient health data. Any successful attack on such devices can lead to immediate consequences, such as altering medical treatments and delaying life-saving interventions. Effectively this can put patients' lives at risk.
- **Operational Failure:** Another critical risk associated with IoHT devices is their potential for operational failures and device malfunctions. Many IoHT devices play a direct role in patient care, such as insulin pumps or heart monitors. Any malfunction or failure of such medical devices could have life-threatening consequences. These devices are dependent on stable connectivity and accurate data transmission. As a result, any disruption in network performance or incorrect data processing could result in delayed medical interventions or erroneous diagnoses. Moreover, regulatory standards for the development and security of IoHT devices are still evolving. This leads to inconsistencies in safety measures across manufacturers that increase the risks associated with their deployment in healthcare settings.
- **Regulatory Compliance:** Ensuring compliance with data privacy and security regulations can be challenging for healthcare organizations, especially as the regulatory landscape continues to evolve.

The world of IoHT devices is evolving rapidly. To address the unique risks associated with IoHT devices, dynamic risk assessment approaches are emerging to limit unauthorized intrusions, secure personal data, and ensure uninterrupted device usage [19]. Notwithstanding the advantages of IoHT for healthcare, patient-specific health information security is still a major issue that requires constant attention and creative solutions [20].

2.2 Threat Actors Targeting Digital Health Systems

Healthcare organizations are developing a growing dependence on the usage of digital health technologies for providing various health services. These digital health systems encompass EHRs, telemedicine platforms, and IoHT devices. This renders them one of the prime targets for cybercriminals [21]. The sensitive nature and high value of PHI and the critical reliance on these systems in healthcare delivery make them highly attractive to various threat actors. Threat actors targeting digital health systems have become increasingly sophisticated, exploiting vulnerabilities in the expanding landscape of interconnected healthcare technologies [22].

A variety of threat actors, including cybercriminals, nation-states, organized crime groups, individual hackers, and hacktivists, are targeting digital health systems for various malicious purposes. These attackers seek to exploit vulnerabilities in digital health infrastructure for financial gain, political motives, or disruption of healthcare services. The IoHT faces challenges such as network interruptions, denial of service attacks, and privacy threats, leading to compromised patient data and healthcare infrastructure [23]. The disruption of health services can also lead to severe operational consequences, incentivizing organizations to meet attackers' demands to minimize patient harm. These attackers may seek access to digital health systems for the purpose of obtaining sensitive research, intellectual property related to medical technologies, or population health data, which can be exploited for strategic advantages.

Figure 5 presents a taxonomic classification of the threat actors that target digital health systems. Each of these threat actors is further discussed below [24–26].

- **Cybercriminals:** Motivated primarily by financial gain, cybercriminals target digital health systems to steal patient data for identity theft, launch ransomware attacks, or sell health records on the black market. The high value of medical data makes healthcare systems particularly lucrative for these actors.

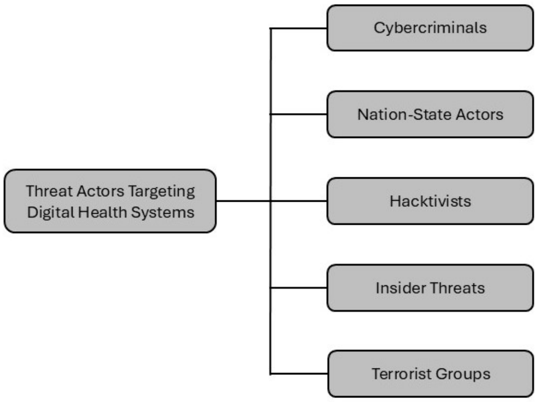

Figure 5: A taxonomy of threat actors targeting digital health systems.

- **Nation-State Actors:** State-sponsored attackers pose a different set of threats and may target healthcare systems for espionage or disruption, especially during geopolitical tensions. These actors are often highly sophisticated and launch cyberattacks to disrupt critical healthcare infrastructure, obtain sensitive medical research, and steal intellectual property to gain a strategic advantage.
- **Hacktivists:** Hacktivists are groups who are driven by certain ideologies or political motives. Such groups may target healthcare organizations to protest or raise awareness of specific causes. As part of their campaigns, they may deface websites, leak sensitive information, or disrupt services.
- **Insider Threats:** Employees or contractors, who have access to healthcare systems and sensitive data, can pose significant risks. Motivations or causes of insider threats may include personal gain, sabotage, or negligence. Insider threats expose significant risks as they can exploit their privileged access to compromise data or systems.
- **Terrorist Groups:** Terrorist organizations may target digital health systems to disrupt healthcare services or instill fear. Attacks on critical infrastructure, such as hospitals and clinics, can have far-reaching consequences on public safety.

The motivations of threat actors targeting digital health systems can vary widely. However, the potential consequences of their attacks are severe. Cyberattacks on healthcare organizations can result in data breaches, disruptions in patient care, financial losses, and reputational damage. Additionally, the theft of sensitive patient data can have far-reaching consequences, including identity theft, discrimination, and emotional distress for affected individuals. These threats are further amplified due to the growing connectivity of healthcare systems through the pervasive use of IoHT. Each of these connected devices presents a potential entry point for threat actors to exploit any vulnerabilities. Consequently, understanding the diverse range of threat actors is essential for healthcare organizations to implement effective security strategies and protect patient safety. Robust security measures, such as lightweight identity authentication protocols [27] and ML models for optimal security [28], are essential to mitigate the risks posed by the diverse array of threat actors. It is extremely crucial to understand the specific threat models and privacy policy gaps in the domain of IoHT to tackle the unique risks and ensure user confidence in these fast-evolving digital health systems.

2.3 Regulatory Scrutiny and Compliance

Regulatory scrutiny and compliance for cybersecurity in the digital health sector are essential due to the wide adoption of advanced healthcare technologies, such as IoHT. The growing vulnerability of healthcare systems to cyber threats underscores the need for strong cybersecurity measures. Regulations relating to digital health are critical to protect patient safety, ensure data privacy, and maintain the integrity of healthcare services [29]. With the increasing collection, transmission, and storage of sensitive health data, regulators are emphasizing that healthcare providers and technology companies maintain stringent safeguards to protect patient privacy and security. The evolution of digital technologies in healthcare necessitates adherence to industry standards, laws, and guidelines to mitigate risks effectively [29]. Compliance management includes activities such as risk identification, assessment, and treatment.

The global implementation of digital medication and treatment requires strict compliance with existing laws and regulations. This highlights the need for strong political will to protect confidential data and increase accountability among stakeholders [30]. A proper understanding of the common vulnerabilities and challenges faced in regulatory compliance is essential for safeguarding healthcare infrastructure and digital applications in the face of cybersecurity threats. As healthcare increasingly relies on digital technologies, governments worldwide have implemented various regulations to address the unique challenges posed by digital health solutions. The most important and relevant regulations in this context are the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) and Medical Device Regulation (MDR) in the European Union, and the Cyber Security Act in Singapore. These regulations set stringent standards for handling sensitive health data. Compliance with these regulations helps ensure that healthcare providers and technology developers implement robust protections by mitigating the risks of data breaches, cyberattacks, and device malfunctions [31]. This can foster trust among patients and healthcare providers and promote the ethical and secure use of digital health innovations. Ultimately, regulatory scrutiny and compliance contribute to a more trustworthy and secure digital health ecosystem. This facilitates fostering public confidence and promoting innovation in healthcare delivery. Further details on legal compliance and governance challenges in IoHT are discussed in Section 4.

3. Vulnerabilities in the IoHT Ecosystem

3.1 Insecure Device Design and Configuration

The design and configuration of IoHT devices pose significant vulnerabilities [32–34]. One of the primary reasons is that the traditional encryption models may not be optimized for IoT devices. This leads to the development of lightweight encryption algorithms to ensure strong security while minimizing computational and power requirements [35]. Moreover, vulnerability scans have revealed alarming statistics showing outdated components in webcams, devices with expired SSL certificates, and insecure default settings in consumer devices [36]. Furthermore, the interconnected nature of IoHT devices, such as wearables, sensors, and implantable devices, and the lack of built-in security features in medical equipment open avenues for cyberattacks [37]. This can lead to data theft and manipulation, denial-of-service, facility disruptions, and even patient harm [38]. Additionally, the shift toward remote access and monitoring in medical implants introduces new risks that increase end-user vulnerability. As a consequence, such vulnerabilities due to insecure device design and configuration can have a wide range of adverse impacts.

Insecure device design and configuration in IoHT raise the following key concerns (Figure 6):

- **Increased Vulnerability to Cyberattacks:** Poorly designed and configured IoHT devices are easier targets for malware, ransomware, and unauthorized access, compromising the entire healthcare network.
- **Data Breaches and Privacy Violations:** Insecure devices can lead to the exposure of sensitive patient data, resulting in privacy violations and regulatory non-compliance.
- **Disruption of Critical Healthcare Services:** Compromised IoHT devices may malfunction or become unavailable, affecting the timely delivery of essential medical care.
- **Patient Safety Risks:** Insecure devices can be manipulated, leading to inaccurate diagnoses or inappropriate treatments that put patient lives at risk.
- **Compliance Challenges:** Inadequately secured devices fail to meet regulatory standards such as HIPAA, leading to potential legal and financial repercussions for healthcare providers.

Designers of medical devices must consider security from the beginning to completion of their designs, focusing on hardware security to address concerns about patient data privacy [39]. Implementing security checks throughout the design and development phases, along with incorporating advanced security measures such as DL and other AI models, is crucial to mitigating cyber threats in the medical IoT ecosystem. Furthermore, it is critical to implement robust cybersecurity measures, adhere to regulatory requirements, and continuously assess and update the security protocols of IoHT devices.

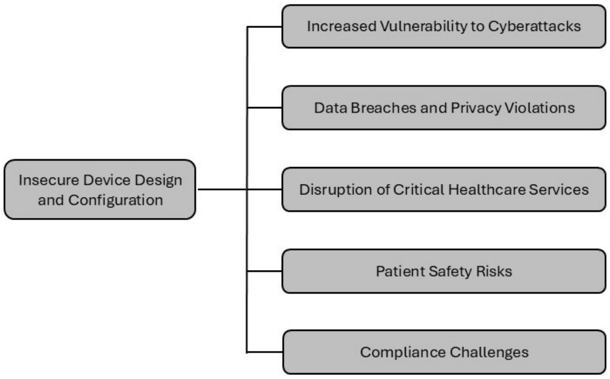
Insecure Device Design and Configuration
Increased Vulnerability to Cyberattacks
Data Breaches and Privacy Violations
Disruption of Critical Healthcare Services
Patient Safety Risks
Compliance Challenges

Figure 6: Key concerns due to insecure IoHT device design and configuration.

3.2 *Lack of Standardized Security Protocols*

The lack of standardized security protocols and consistent guidelines and requirements across IoHT devices and platforms poses significant risks. Without consistent and universally adopted security measures, the entire IoHT infrastructure remains vulnerable to cyberattacks, data breaches, and privacy violations. These concerns highlight the critical need for establishing robust and standardized security frameworks to ensure the safety, privacy, and reliability of IoHT systems. The lack of standardized security protocols in IoHT can potentially raise the following key concerns [40, 41, 43] (Figure 7):

- **Interoperability Challenges:** IoHT devices are often designed by different manufacturers with varying security practices. This can potentially create fragmented and inconsistent security frameworks. This fragmentation increases vulnerabilities and makes healthcare networks more susceptible to cyberattacks. Moreover, the absence of unified standards complicates the integration of devices into existing healthcare infrastructure. This could reduce operational efficiency and increase patient safety risks.
- **Vulnerability to Cyberattacks:** The lack of uniform security standards makes IoHT systems more vulnerable to cyberattacks such as ransomware, phishing, and unauthorized access. Attackers can exploit inconsistencies in security practices and infiltrate networks to commit further crimes.
- **Data Privacy Issues:** Without standardized encryption and data protection mechanisms, patient information is at greater risk of unauthorized access and breaches. This can compromise sensitive personal and medical data.

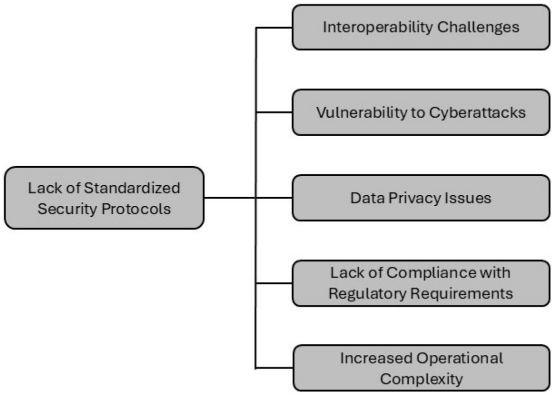
Lack of Standardized Security Protocols
Interoperability Challenges
Vulnerability to Cyberattacks
Data Privacy Issues
Lack of Compliance with Regulatory Requirements
Increased Operational Complexity

Figure 7: Key concerns due to the lack of standardized security protocols in IoHT.

- **Lack of Compliance with Regulatory Requirements:** The variations in security measures make it harder for healthcare providers to comply with healthcare regulations such as HIPAA and GDPR. This can potentially result in legal consequences for healthcare providers.
- **Increased Operational Complexity:** To ensure security for various IoHT devices manufactured by different vendors, healthcare organizations must implement multiple security solutions. This increases operational complexity and costs while possibly leaving gaps in security coverage.

As solution measures, various security protocols have been proposed. However, many of the protocols suffer from extensive communication, storage, and computation overheads due to negligence on crucial attack models [42, 43]. To address the lack of standardized security protocols in the IoHT, a unified and comprehensive approach is needed to mitigate risks and enhance the security of medical devices and healthcare systems. Implementation of standardized security measures can ensure interoperability, protect patient data, and safeguard healthcare networks from cyber threats. A list of potential solution approaches to address the lack of standardized security protocols in IoHT is discussed below [41, 44, 45] (Figure 8):

- **Development of Universal Security Standards:** Regulatory bodies and industry stakeholders should collaborate to establish universal security protocols. Such protocols must apply to all IoHT devices so that they ensure secure communication and data exchange across platforms and manufacturers.
- **Mandating End-to-End Encryption:** End-to-end encryption should be enforced for all IoHT devices to protect sensitive health data from

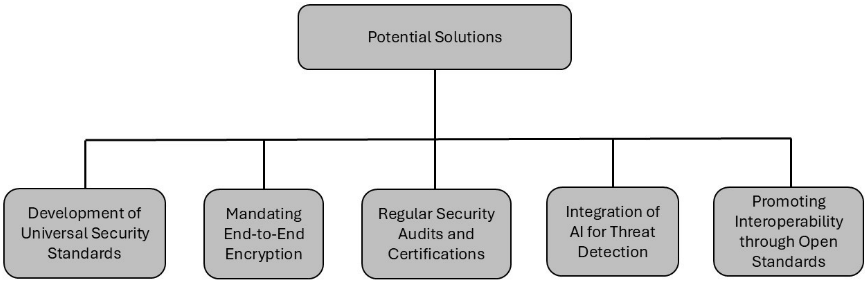
Potential Solutions
Development of Universal Security Standards
Mandating End-to-End Encryption
Regular Security Audits and Certifications
Integration of AI for Threat Detection
Promoting Interoperability through Open Standards

Figure 8: Potential solutions to the lack of standardized security protocols in IoHT.

security attacks, such as eavesdropping and man-in-the-middle attacks. This will prevent unauthorized access and data breaches during transmission and ensure confidentiality and integrity.

- **Regular Security Audits and Certifications:** IoHT devices should undergo compulsory security audits and obtain certifications to ensure regulatory compliance according to the established security standards. This would ensure that devices meet baseline security requirements before their deployments.
- **Integration of AI for Threat Detection:** AI-driven security systems can monitor IoHT devices in real time and help detect and respond to potential threats. This can effectively prevent and reduce the risk of cyberattacks.
- **Promoting Interoperability through Open Standards:** Open standards should be adopted to promote interoperability between different IoHT devices while maintaining security standards. This can effectively reduce compatibility issues and simplify the integration process for healthcare providers.

3.3 Vulnerabilities in Connected Medical Devices

Vulnerabilities in connected medical devices within the IoHT pose significant risks due to the potential exposure of patient-specific data. This can lead to wider attack surfaces and increase damage possibilities, including unauthorized data access, cyberattacks, and device tampering [16]. These devices, also known as Medical Internet-of-Things (MIoT), are crucial for remote patient care and require robust security measures to protect against cyberattacks in real time [19]. Connected medical devices offer advantages such as enhanced patient monitoring and improved healthcare delivery. Such MIoT devices are especially beneficial for remote or immobile patients; however, they also introduce risks to patient privacy and medical record integrity [46]. Furthermore, IoHT devices, such as wearables, implants, and remote monitoring systems, often lack robust security features that make them susceptible to threats such as malware, ransomware, and phishing attacks. These vulnerabilities are exacerbated by the increasing number of connected IoHT devices. This can effectively expand the attack surface within healthcare networks. For instance, a breach in one device can compromise an entire system and lead to the exposure of sensitive patient data or disruption of essential medical services.

The commonly identified vulnerabilities in connected medical devices are discussed below [47–49] (Figure 9):

- **Weak Authentication Mechanisms:** Many connected medical devices lack strong authentication, allowing unauthorized access to sensitive data or device control.
- **Unencrypted Data Transmission:** Data transmitted between devices and healthcare systems are often unencrypted, making them vulnerable to interception and theft.
- **Outdated Software and Firmware:** Many IoHT devices run on outdated software, leaving them susceptible to known vulnerabilities and exploits.
- **Lack of Secure Updates:** Insufficient mechanisms for securely updating device software can lead to exploitable weaknesses being left unpatched.
- **Insecure Default Configurations:** Many devices are deployed with default settings that have weak security, making them easy targets for attackers.

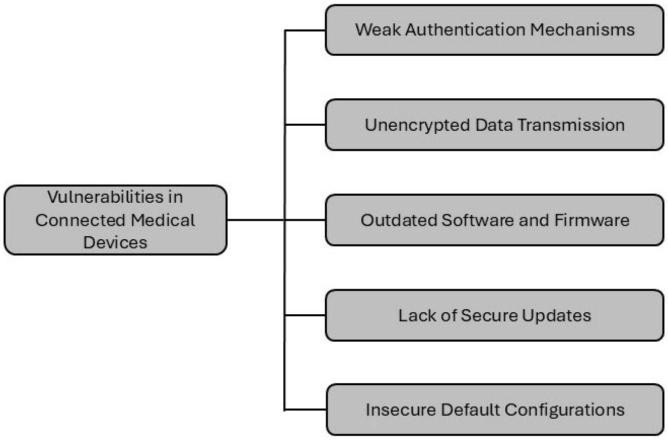
Vulnerabilities in Connected Medical Devices
Weak Authentication Mechanisms
Unencrypted Data Transmission
Outdated Software and Firmware
Lack of Secure Updates
Insecure Default Configurations

Figure 9: Common vulnerabilities in connected medical devices.

To ensure the security of these devices and their communications, it is critical to protect patient data and maintain system integrity. Vulnerabilities in device communication channels and network protocols can lead to data breaches, device malfunctions, or even patient harm. Figure 10 presents the strategies specifically designed to mitigate risks in connected devices and their communications discussed below [48–50].

- **Secure Communication Protocols:** Secure communication protocols, such as TLS (Transport Layer Security) and DTLS (Datagram TLS), can be implemented to encrypt data transmitted between connected devices and healthcare systems. This can prevent data interception and tampering during transit.
- **Device Authentication and Pairing:** It is crucial to ensure that devices are authenticated before being allowed to communicate with the network. For this purpose, techniques such as digital certificates or secure device pairing can be utilized to prevent unauthorized devices from accessing the system.
- **Network Segmentation:** Appropriate network segmentation should be implemented to isolate IoHT devices from other parts of the healthcare network. This can minimize the potential spread of attacks and contain security breaches to specific device groups.
- **Device Firmware Integrity Checks:** Integrity checks for device firmware must be implemented to verify that it has not been altered or compromised during updates or communication. This will guarantee that only trusted firmware is running on devices.
- **Encrypted Device-to-Device Communication:** It is critical to ensure that data exchanges between connected medical devices are encrypted to prevent eavesdropping and manipulation during real-time patient monitoring and treatment.
- **Wireless Security Enhancements:** Wireless communication security must be strengthened by using WPA3 (Wi-Fi Protected Access 3) or

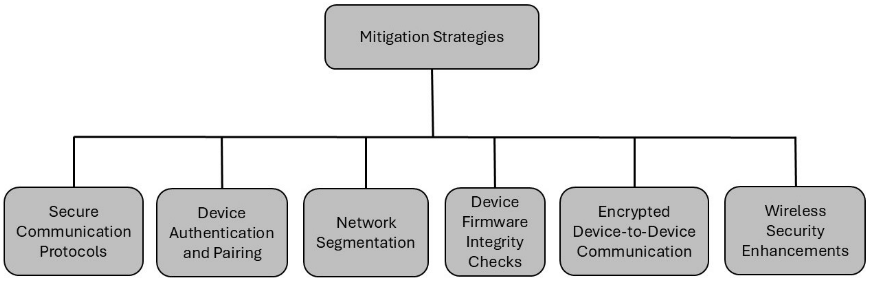
Mitigation Strategies
Secure Communication Protocols
Device Authentication and Pairing
Network Segmentation
Device Firmware Integrity Checks
Encrypted Device-to-Device Communication
Wireless Security Enhancements

Figure 10: Mitigation strategies of risks in connected devices and their communications.

other advanced encryption standards for Wi-Fi networks that IoHT devices rely on. This is important to protect against unauthorized access to the network and devices.

3.4 Data Privacy and Confidentiality Concerns

Data privacy and confidentiality are critical concerns in the IoHT due to the continuous exchange of sensitive healthcare data across interconnected devices [51–55]. The rapid expansion and pervasive use of IoMT (Internet of Medical Things) devices increase the risk of data breaches, unauthorized access, and misuse of PHI [51–55]. These devices, such as wearables and implantable sensors, remote diagnostic tools, smart insulin pumps, and wearable health monitors, are vulnerable to cyberattacks such as keyloggers and spyware. This can compromise patient data and lead to identity theft. A breach in confidentiality can lead to a loss of trust in healthcare providers and legal repercussions under regulations such as HIPAA and GDPR.

Figure 11 presents the primary concerns relating to data privacy and confidentiality in IoHT that are discussed below [51–55]:

- **Data Breaches and Unauthorized Access:** The interconnected nature of IoMT devices can increase the risk of data breaches and unauthorized access to sensitive patient data.
- **Identity Theft and Discrimination:** The misuse of medical data can lead to identity theft, discrimination, or other harmful consequences.

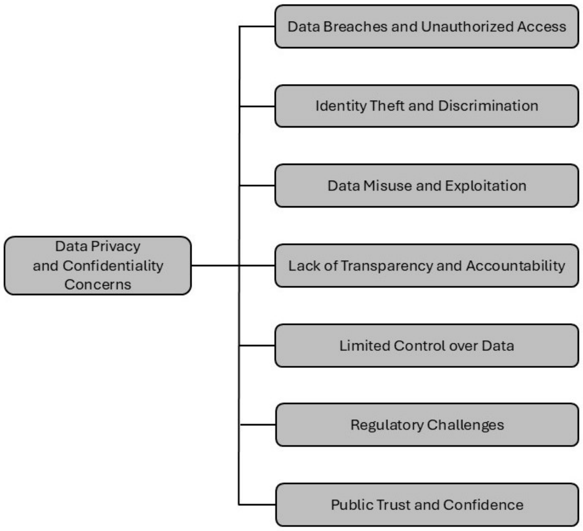
Data Privacy and Confidentiality Concerns
Data Breaches and Unauthorized Access
Identity Theft and Discrimination
Data Misuse and Exploitation
Lack of Transparency and Accountability
Limited Control over Data
Regulatory Challenges
Public Trust and Confidence

Figure 11: Primary concerns relating to data privacy and confidentiality in IoHT.

- **Data Misuse and Exploitation:** Unauthorized access to medical data can lead to its misuse and exploitation for various purposes.
- **Lack of Transparency and Accountability:** It can be very difficult to ensure transparency and accountability in the handling of patient data without clear guidelines and regulations.
- **Limited Control over Data:** Patients may have limited control over their medical data and lack of knowledge regarding how their data are utilized, stored, and shared.
- **Regulatory Challenges:** Ensuring compliance with data privacy and security regulations can be complex and costly for healthcare organizations.
- **Public Trust and Confidence:** Concerns about data privacy and confidentiality can erode public trust and confidence in IoMT technologies.

The growing field of smart healthcare highlights the urgent need for strong security measures to safeguard patient privacy. It is a critical concern to protect data in the interconnected IoMT environment. To address these concerns, several solution approaches are proposed as discussed below [56–60] (Figure 12):

- **Strong Encryption:** Implementation of robust and end-to-end encryption for data transmission, such as the Secret Sharing Algorithm (SSA) [61], is crucial. This can protect sensitive patient data from unauthorized access even though the devices are compromised.
- **Access Control:** Implementing multi-factor authentication and role-based access controls is essential to restrict access to IoMT systems and patient data to authorized individuals only.
- **Data Minimization:** Risks of data breaches and misuse can be reduced by collecting only the required data.
- **Secure Data Sharing:** Developing secure and standardized protocols for sharing patient data can ensure that data are transmitted and stored securely.
- **Blockchain Technology:** Adopting **blockchain technology** can enhance data security by providing a decentralized, tamper-proof system for managing medical records.
- **Security Audits and Vulnerability Assessments:** Regular **audits and vulnerability assessments** should be conducted to identify weaknesses and mitigate potential security gaps in IoMT systems.
- **Privacy-preserving Technologies:** Utilizing privacy-preserving technologies, such as differential privacy and homomorphic

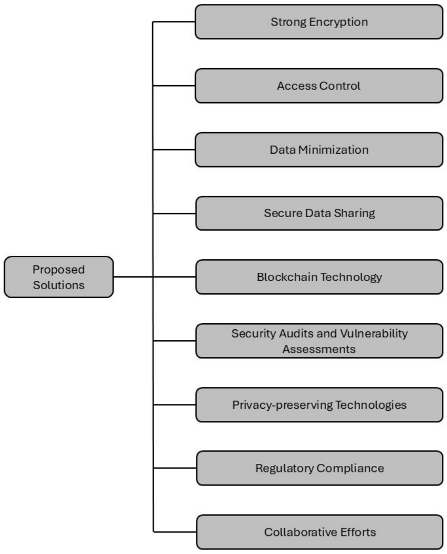

Figure 12: Solution approaches for data privacy and confidentiality concerns in IoHT.

encryption, can enable data analysis without compromising individual privacy.

- **Regulatory Compliance:** Adhering to relevant regulations, such as HIPAA and GDPR, can help ensure that IoMT devices and systems are compliant with data privacy and security standards.
- **Collaborative Efforts:** Effective collaboration between healthcare providers, regulatory bodies, and technology developers is necessary to establish comprehensive security frameworks. This is essential for safeguarding patient privacy and confidentiality in IoMT systems.

3.4.1 Patient Data Leakage Risks

Patient data leakage risks pose a significant threat to data privacy in the IoHT. The IoMT integrates medical devices with the IoT. Such medical devices contain sensitive patient health data [62]. Traditional ML and DL models face challenges as patient data must be transferred to central servers. This increases risks of security and privacy breaches [63]. To address these risks, dynamic risk assessment (DRA) approaches are emerging to combat sophisticated cyberattacks in real time. This can safeguard patient data and ensure uninterrupted device usage [64]. Specialized encryption algorithms, such as Rail Fence Data Encryption (RFDE), can be utilized to protect Personal Health Records (PHRs) in the cloud, enhancing data security and privacy [65]. Overall, mitigating patient data leakage risks is crucial to maintaining the confidentiality and integrity of healthcare information in the IoMT ecosystem.

3.4.2 Challenges of Securing Health Data in Transit and Storage

The sensitive nature of healthcare data collected by IoMT devices makes it vulnerable to malicious attacks such as tampering, eavesdropping, and forgery [66]. These security risks emphasize the need for data integrity, authenticity, and privacy [53]. Innovative approaches, such as utilizing distributed InterPlanetary File System (IPFS) storage, blockchain technology, redactable signature schemes, and specialized encryption algorithms such as Rail Fence Data Encryption (RFDE) are proposed to address these challenges. Implementing these security measures ensures that health data remain confidential, secure, and integral during transmission and storage. This can effectively safeguard patient privacy and the integrity of medical information in IoMT systems.

3.5 Targeted Attacks on IoHT Infrastructure

Targeted attacks on IoHT infrastructure pose significant security risks due to the sensitive nature of medical data [67]. Various attack scenarios, including Deauthentication (Deauth), Distributed Denial of Service (DDoS), brute force, and so on, target data transfer, storage, and access points within the IoHT ecosystem [68]. Additionally, the IoHT domain faces threats from malicious intruders conducting blackhole, rank, and DoDAG (Destination-Oriented Directed Acyclic Graph) attacks that impact the performance of patient-centric IoHT systems [69]. Understanding these attack methodologies and vulnerabilities is crucial to implementing robust security measures and safeguarding patient data and healthcare infrastructure in the IoHT environment.

Figure 13 presents the most common targeted attacks on IoHT infrastructures as discussed below [70–73].

- **Ransomware Attacks:** Cybercriminals often deploy ransomware to encrypt critical health data and demand payment for its release. Such attacks disrupt healthcare services, cause delays in treatments, and compromise patient safety.
- **Data Breaches:** Attackers target IoHT devices to steal sensitive patient information, such as medical records. These data can be sold on the dark web or used for identity theft. These breaches effectively erode patient trust, cause significant financial losses, and lead to legal consequences for healthcare providers.
- **Device Manipulation:** Malicious actors can compromise IoHT devices, such as insulin pumps or pacemakers. This can lead to potentially life-threatening situations. Device manipulation can result in altered dosages of medications or malfunction of critical health devices.
- **Distributed Denial-of-Service (DDoS) Attacks:** IoHT infrastructure can be overwhelmed by DDoS attacks that can render systems

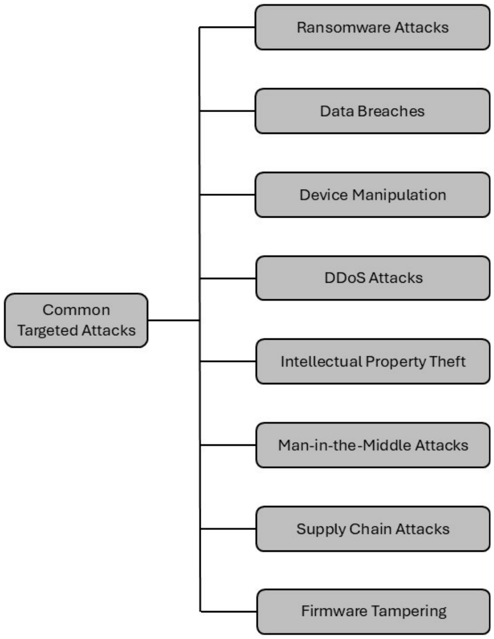

Figure 13: The most common targeted attacks on IoHT infrastructures.

inaccessible to legitimate users. This paralysis of healthcare operations can delay critical care, especially in emergency scenarios.

- **Intellectual Property Theft:** Attackers also target IoHT systems to steal proprietary medical technology and research data. This can result in the loss of competitive advantage and stifle innovation.
- **Man-in-the-Middle (MitM) Attacks:** In this attack, cybercriminals intercept and potentially alter the communication between IoHT devices and healthcare systems. This can lead to unauthorized data access, tampering with medical records, or even the manipulation of real-time medical data being transmitted by devices. Such attacks pose a severe threat to patient safety.
- **Supply Chain Attacks:** IoHT systems are often dependent on multiple third-party components. Attackers may exploit vulnerabilities in the supply chain, such as compromised software or hardware updates. This can open opportunities for attackers to infiltrate healthcare systems. These attacks can introduce malware or backdoors that facilitate attackers with prolonged access to IoHT networks.
- **Firmware Tampering:** Attackers also target the firmware of IoHT devices which controls the basic operations of these devices. By altering the firmware, attackers can disable the devices, modify

their functionality, or even take control of them. This can lead to malfunctions in critical devices, such as pacemakers or insulin pumps, and pose direct risks to patient health.

3.6 Exploitation of Weaknesses in IoHT Networks and Protocols

The IoHT relies on interconnected devices and networks to monitor, transmit, and analyze patient data in real time. This connectivity is crucial for enhancing healthcare efficiency. However, it also introduces significant security vulnerabilities [74]. The complexity and heterogeneity of IoHT networks, and the weaknesses in communication protocols make healthcare systems particularly susceptible to cyberattacks. These security gaps can lead to data breaches, compromised patient safety, and disruptions in medical services. Therefore, it is critical to understand the specific threats arising from weak networks and protocols to safeguarding IoHT infrastructure and ensuring the secure handling of sensitive health information [75].

The major security threats associated with the weaknesses of the IoHT network and protocol, and their consequences are discussed below [76–79] (Figure 14):

- **Unsecured Communication Channels:** IoHT devices often transmit data through unsecured or poorly encrypted channels. This exposes sensitive medical information to eavesdropping or interception. Consequently, this can lead to data breaches that violate privacy regulations (such as HIPAA and GDPR) and could cause identity theft.
- **Vulnerable Wireless Protocols:** Many IoHT devices rely on outdated or weak wireless protocols. This makes the devices easy targets for attacks such as MitM attacks. These attacks enable cybercriminals to intercept, alter, or inject malicious data and potentially compromise the integrity of medical treatments.
- **Insufficient Device Authentication:** Weak authentication protocols or their absence allow attackers to gain unauthorized access to IoHT devices. This can lead to device manipulation, such as altering the performance of life-critical systems (e.g., pacemakers) and endanger patient lives.
- **Inadequate Firmware Security:** Many IoHT devices run on outdated firmware with security flaws. Attackers can exploit these vulnerabilities to introduce malware or disable devices. This can lead to disruptions in healthcare services and delayed treatment for patients.
- **DDoS (Distributed Denial-of-Service) Attacks:** DDoS attacks target IoHT infrastructure by overwhelming it with a flood of traffic from multiple sources. This situation causes legitimate requests to be

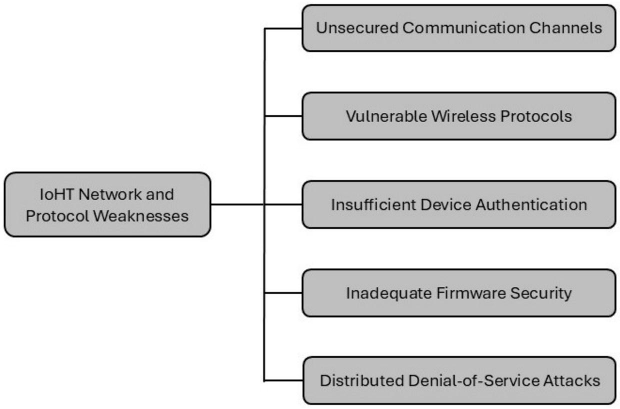
IoHT Network and Protocol Weaknesses
Unsecured Communication Channels
Vulnerable Wireless Protocols
Insufficient Device Authentication
Inadequate Firmware Security
Distributed Denial-of-Service Attacks

Figure 14: Major security threats associated with the weaknesses of the IoHT networks and protocols.

denied. This can render critical healthcare systems and services inaccessible which can lead to significant operational disruptions. In emergency situations, such downtime can delay critical medical treatments and potentially jeopardize patient health and safety. Furthermore, the inability to access patient data during such attacks can hinder healthcare providers' ability to make informed decisions. This effectively can lead to further complications in patient care and treatment outcomes. Additionally, prolonged service outages can result in financial losses for healthcare organizations and damage their reputation among patients and stakeholders.

To address these issues, researchers have proposed improved lightweight authentication schemes utilizing techniques such as hash functions, XOR operations, and Elliptic Curve Cryptography [80, 81]. Additionally, security experiments have been conducted to identify flaws in existing IoMT security protocols and recommend solutions to mitigate cyberattacks on smart medical devices in Healthcare systems. The focus remains on enhancing the security of IoMT networks to ensure the confidentiality and integrity of patient data.

3.7 Supply Chain Risks

Risks in IoMT-based supply chains include lack of knowledge, technical infrastructure maintenance, cybersecurity, and network dependability [82]. These risks can lead to disruptions, expiry of products, and compromised patient safety [83, 84]. Implementing smart systems in IoMT-based supply chains requires addressing these risks through comprehensive risk management strategies. Blockchain technology can enhance security, integrity, and data provenance in health E-supply chains. However, further research and integration with regulatory frameworks are needed to unlock its full potential. Healthcare supply chains can be made more reliable, traceable, and secure by leveraging IoMT and blockchain technologies. Ultimately, this can improve patient outcomes and operational efficiency [83].

4. Legal Compliance and Governance Challenges of IoHT

4.1 Regulatory Authorities for Digital Health

The most relevant and prominent regulations relating to IoHT and digital health are discussed below:

- **Health Insurance Portability and Accountability Act (HIPPA):**[1] One of the most important regulations in this space is the HIPAA in the United States, which establishes national standards for the protection of PHI. HIPAA mandates that healthcare organizations implement technical, administrative, and physical safeguards to ensure the confidentiality, integrity, and availability of PHI. Effectively, this makes HIPPA a cornerstone of digital health compliance. HIPAA was enacted in 1996 and it sets standards for the privacy and security of patient health information. It requires healthcare providers and their business associates to implement safeguards to protect EHRs from unauthorized access, disclosure, or use.
- **General Data Protection Regulations (GDPR):**[2] The GDPR is a comprehensive data protection law that applies to any organization processing personal data of EU residents. It grants individuals greater control over their personal data and imposes stringent requirements on data controllers and processors to ensure data security and privacy. It went into effect in 2018. In addition to HIPAA, the GDPR in the European Union (EU) plays a vital role in shaping data privacy practices in digital health. GDPR applies to any organization that processes the personal data of EU citizens. This includes healthcare providers, medical device manufacturers, and digital health platforms. GDPR sets a high bar for data protection and requires organizations to obtain explicit consent from patients. Consequently, this ensures data minimization and implements stringent security measures to protect patient information.
- **Medical Device Regulation (MDR):**[3] The MDR, also in the EU, imposes additional compliance requirements for digital health

[1] https://www.hhs.gov/hipaa/index.html.

[2] https://ec.europa.eu/info/law/law-topic/data-protection_en.

[3] https://health.ec.europa.eu/medical-devices-sector/overview_en.

products classified as medical devices. This regulation emphasizes the need for rigorous testing, clinical evaluation, and continuous monitoring of medical devices. This helps in ensuring the safety and efficacy of the medical devices, especially as they integrate with IoHT ecosystems.

- **Cyber Security Act:**[4] The Cyber Security Act in Singapore was passed in 2017. It aims to enhance the cybersecurity capabilities of critical information infrastructure, including healthcare organizations. It requires the implementation of cybersecurity measures and mandates organizations to report data breaches to the government.

4.2 Legal Compliance Issues and Solutions

Compliance with healthcare legal authorities and regulations in the IoMT is a critical challenge due to the complexities involved in managing vast amounts of sensitive health data across interconnected devices. Various challenges, such as data privacy protection, security risks, and compliance issues, have been identified [85, 86]. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) impose strict requirements for data privacy, security, and patient confidentiality. However, the integration of diverse IoHT devices often results in fragmented security measures. This makes compliance difficult and increases the risk of security breaches. Non-compliance can lead to severe financial penalties, operational disruptions, and reputational risks. Consequently, this can be damaging to the trust between patients and healthcare providers, and lead to potential legal consequences [86, 87].

The key concerns relating to compliance with healthcare regulations in IoHT are discussed below [87–90] (Figure 15):

- **Multiple Regulations:** Healthcare organizations must comply with a complex array of regulations, including HIPAA, GDPR, and local data protection laws.
- **Regulatory Complexity:** Understanding and interpreting regulations can be challenging, especially as regulations evolve.
- **Changing Regulatory Landscape:** Regulations can change frequently, making it difficult for organizations to keep up with the latest requirements.
- **Data Privacy and Security:** Ensuring compliance with data privacy and security regulations is essential to protect patient data and avoid penalties.

[4] https://www.csa.gov.sg/Legislation/cybersecurity-act.

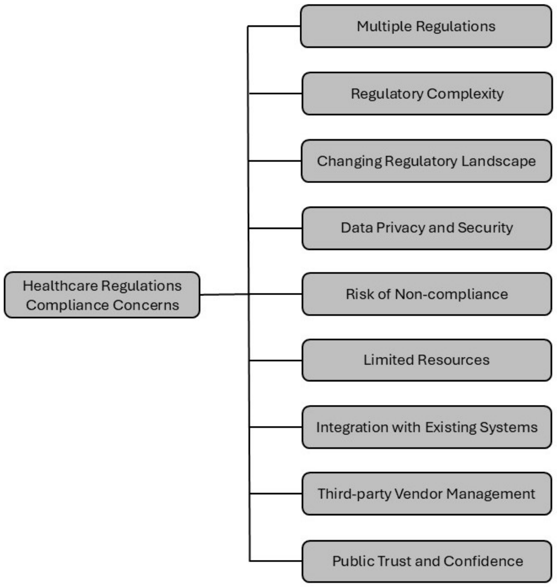
Healthcare Regulations Compliance Concerns
Multiple Regulations
Regulatory Complexity
Changing Regulatory Landscape
Data Privacy and Security
Risk of Non-compliance
Limited Resources
Integration with Existing Systems
Third-party Vendor Management
Public Trust and Confidence

Figure 15: Concerns relating to compliance with healthcare regulations in IoHT.

- **Risk of Non-compliance:** Non-compliance with regulations can result in hefty fines, reputational damage, and legal consequences.
- **Limited Resources:** Healthcare organizations may have limited resources to allocate to compliance efforts.
- **Integration with Existing Systems:** Ensuring that IoHT devices and systems comply with existing regulatory frameworks can be complex.
- **Third-party Vendor Management:** Managing the compliance of third-party vendors can be challenging.
- **Public Trust and Confidence:** Non-compliance with regulations can erode public trust and confidence in healthcare organizations and IoHT technologies.

To mitigate the above-mentioned concerns**,** privacy-by-design frameworks are essential, embedding regulatory compliance and robust security protocols into the development and deployment of IoHT devices from the outset [91]. Furthermore, continuous monitoring and real-time auditing of IoHT systems are necessary to identify and address vulnerabilities that may arise over time, ensuring ongoing adherence to regulatory standards. The use of advanced encryption and data anonymization techniques can also help protect patient data while ensuring compliance with regulations such as HIPAA and GDPR.

To address these concerns, several solutions are proposed [86, 92–95] (Figure 16):

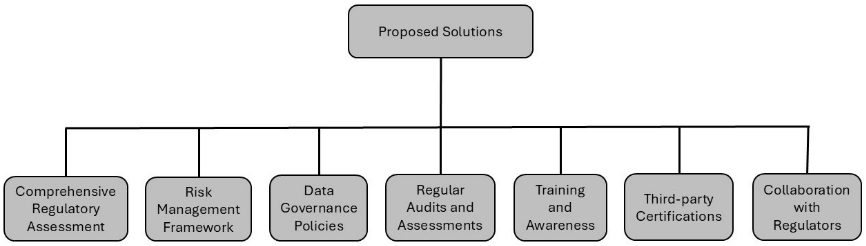
Proposed Solutions
Comprehensive Regulatory Assessment
Risk Management Framework
Data Governance Policies
Regular Audits and Assessments
Training and Awareness
Third-party Certifications
Collaboration with Regulators

Figure 16: Proposed solutions to healthcare regulatory compliance concerns in IoHT.

- **Comprehensive Regulatory Assessment:** A thorough assessment of applicable regulations can help organizations identify and address potential compliance gaps.
- **Risk Management Framework:** Implementation of a risk management framework can help organizations prioritize compliance efforts and allocate resources effectively.
- **Data Governance Policies:** The design and development of robust data governance policies can establish clear guidelines for data collection, storage, use, and sharing.
- **Regular Audits and Assessments:** Regular audits and assessments can be conducted to help organizations identify and address compliance issues proactively.
- **Training and Awareness:** Training and awareness programs can be provided to employees to ensure that they understand and comply with relevant regulations.
- **Third-party Certifications:** Obtaining third-party certifications, such as ISO 27001[5] or HITRUST,[6] can demonstrate an organization's commitment to data security and compliance.
- **Collaboration with Regulators:** Collaboration with regulatory bodies can help organizations stay informed about regulatory changes and best practices.

Overall, robust regulatory frameworks based on standardized practices, security measures, and compliance standards are crucial for the successful implementation and adoption of IoHT technologies. By fostering collaboration among regulators, healthcare providers, and device

[5] https://www.iso.org/standard/27001.

[6] https://hitrustalliance.net.

manufacturers, such frameworks can help build a secure compliance ecosystem and protect sensitive health information.

4.3 Fragmentation of Regulatory Standards for IoHT and Solutions

The lack of uniform regulatory standards in the IoHT creates major obstacles to maintaining the security, privacy, and safety of healthcare devices. This fragmentation is caused by a diverse range of standards development organizations (SDOs) and the absence of a universally accepted vision [96]. The IoHT devices are developed and deployed across various jurisdictions. In such situations, the absence of harmonized regulations creates inconsistencies in data protection, security protocols, and device interoperability. This fragmentation increases vulnerabilities as health devices created under weaker regulations may fall short of essential cybersecurity and privacy standards. Consequently, healthcare networks become more susceptible to data breaches and cyberattacks. Moreover, the lack of standardized protocols hinders cross-border data sharing and collaboration, thus slowing down the advancements in global healthcare systems.

This issue mirrors the broader problem seen in the IoT security standards. In IoT, a fragmented environment led by various de facto standards makes it challenging to establish uniform security measures across different applications and domains. This lack of a consistent baseline for security increases risks and complicates the protection of connected systems [97]. The current surge in collaboration of distributed IoT devices exacerbates interoperability issues. This, in turn, limits data reuse and new service development due to diverse networking technologies and performance impairments with increasing device interactions [98].

The major issues relating to the fragmentation of regulatory standards for IoHT are discussed below [93, 99, 100] (Figure 17):

- **Inconsistent Security Protocols:** Different jurisdictions have varying security standards. This leads to IoHT devices with inconsistent cybersecurity measures that increases the risks of data breaches and cyberattacks.
- **Privacy Vulnerabilities:** Fragmented regulations create gaps in data privacy protection. This makes it difficult to ensure compliance with global privacy laws such as HIPAA and GDPR.
- **Device Interoperability Challenges:** Lack of standardized protocols across different regions impairs the interoperability of IoHT devices. As a consequence, this leads to inefficiencies in communication and data sharing between healthcare systems.
- **Regulatory Compliance Complexity:** Manufacturers of IoHT devices often face challenges in ensuring their devices meet the diverse and

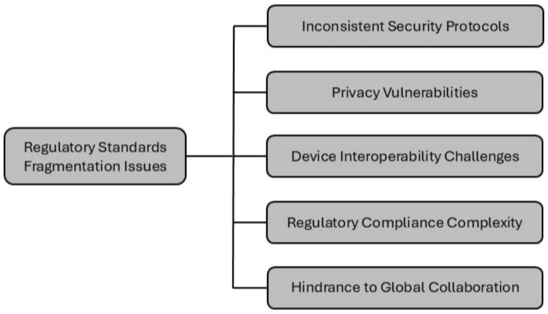
Regulatory Standards Fragmentation Issues
Inconsistent Security Protocols
Privacy Vulnerabilities
Device Interoperability Challenges
Regulatory Compliance Complexity
Hindrance to Global Collaboration

Figure 17: Major issues relating to the fragmentation of regulatory standards for IoHT.

sometimes conflicting regulatory requirements across multiple jurisdictions. This increases the costs and risks associated with regulatory compliances.

- **Hindrance to Global Collaboration:** Regulatory fragmentation limits the ability to share patient data and collaborate on healthcare innovations across borders. This potentially slows down advancements in global health solutions.

Addressing this issue requires strong leadership, collaboration, and a coherent approach to standard development. Such a holistic approach can ensure the successful establishment of foundational standards for a robust digital health ecosystem [87]. Collaborative efforts between international regulatory bodies, such as the U.S. Food and Drug Administration[7] (FDA) and the European Medicines Agency[8] (EMA), can promote the creation of unified standards for IoHT devices. Additionally, the implementation of seamless communication could facilitate smooth and secure information exchange between devices. This could potentially reduce operational inefficiencies and improve patient outcomes. Controlled environments for testing IoHT innovations could also enable developers to ensure compliance with diverse regulations before market release. As a result, this can effectively promote harmonization and security across the IoHT ecosystem.

Potential solutions to the fragmentation of regulatory standards in IoHT include the following [92, 101–104] (Figure 18):

- **Global Regulatory Frameworks:** Collaborative efforts between international regulatory bodies (e.g., FDA and EMA) can create unified standards for IoHT devices. This can ensure consistent security and privacy protection.

[7] https://www.fda.gov.

[8] https://www.ema.europa.eu.

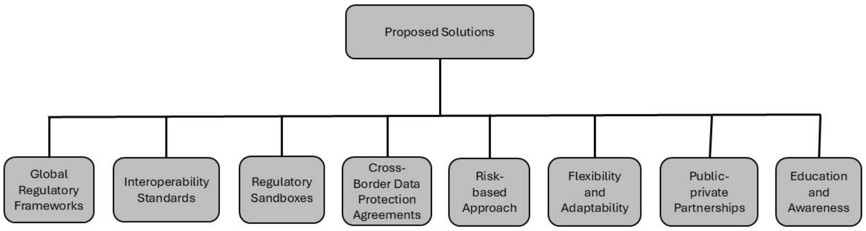
Proposed Solutions
Global Regulatory Frameworks
Interoperability Standards
Regulatory Sandboxes
Cross-Border Data Protection Agreements
Risk-based Approach
Flexibility and Adaptability
Public-private Partnerships
Education and Awareness

Figure 18: Potential solutions to the fragmentation of regulatory standards in IoHT.

- **Interoperability Standards:** The development and implementation of standardized interoperability frameworks can ensure seamless communication and data exchange between IoHT devices across different healthcare systems.
- **Regulatory Sandboxes:** Controlled environments for IoHT developers can be established to test devices for compliance with various regional regulations before releasing them to the market.
- **Cross-Border Data Protection Agreements:** International agreements can be formulated to standardize data privacy protections and allow safe cross-border data sharing within the IoHT ecosystem.
- **Risk-based Approach:** A risk-based approach can be adopted for regulation so that it can focus on addressing the most significant risks and avoid excessive burdens on healthcare organizations.
- **Flexibility and Adaptability:** Regulatory standards should be flexible and adaptable so that they can accommodate technological advancements and emerging trends.
- **Public–Private Partnerships:** Collaborating with industry stakeholders can help develop and implement effective regulatory frameworks.
- **Education and Awareness:** Raising knowledge and awareness among healthcare professionals and the public regarding the importance of regulatory compliance can help foster a more educated and harmonized environment.

4.4 Cross-Border Data Sharing and Jurisdictional Challenges in IoHT

Cross-border data sharing in the IoHT is essential for global healthcare collaboration. However, it introduces significant jurisdictional challenges [105]. Varying regulatory frameworks, differing privacy standards, and geopolitical complexities complicate the process of seamless data exchange and information sharing among the different stakeholders within the IoHT ecosystem. A holistic approach is required to ensure secure and compliant international health data sharing, including harmonization, innovative technological solutions, and robust governance.

The primary challenges and complexities associated with cross-border data sharing in IoHT are discussed below [86, 105–108] (Figure 19):

- **Regulatory Variations:** Conflicts in compliance arise due to different data protection laws such as GDPR in Europe and HIPAA in the USA.
- **Data Sovereignty:** Nation states have strict regulations on where and how health data can be stored, processed, and transmitted.
- **Lack of Standardization:** Due to the inconsistent data formats and exchange protocols interoperability across IoHT borders is hindered severely.
- **Geopolitical Tensions:** Political and economic conflicts and trade restrictions can sometimes obstruct data-sharing agreements.
- **Cybersecurity Risks:** The potential risks of cyberattacks and unauthorized access increases due to cross-border data exchanges.
- **Data Ownership Disputes:** In the context of multiple jurisdictions, unclear data ownership laws can lead to operational complexities and challenges.

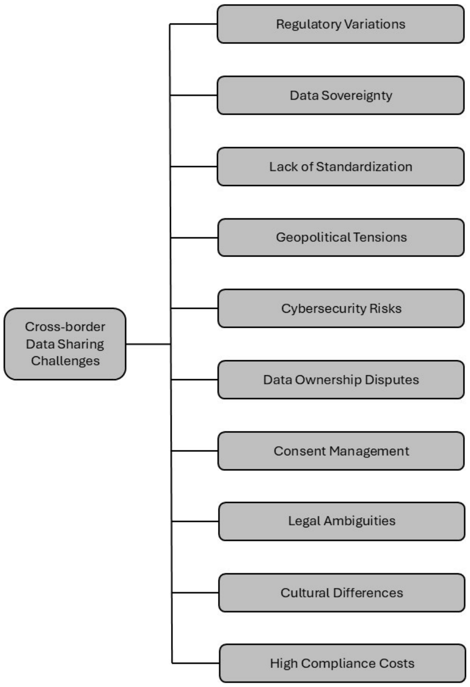

Figure 19: Primary challenges and complexities associated with cross-border data sharing in IoHT.

- **Consent Management:** Standards for obtaining and verifying patient consent for data use differ across jurisdictions which complicates the overall IoHT operations management.
- **Legal Ambiguities:** In the events of data breaches or misuse, unclear definitions of legal liabilities increase vagueness and nuances.
- **Cultural Differences:** Health data governance is further complicated by the varied perspectives on privacy and healthcare ethics across diverse cultures.
- **High Compliance Costs:** Adhering to multiple international regulations imposes financial burdens on IoHT stakeholders.

To address the above-mentioned issues and challenges, the following solution approaches are suggested to ensure secure and compliant data exchange, foster international healthcare cooperation, and improve patient outcomes [86, 105, 107, 109, 110] (Figure 20):

- **Global Regulatory Frameworks:** The development of unified international guidelines can harmonize data protection standards across regions for unified cross-border IoHT governance.

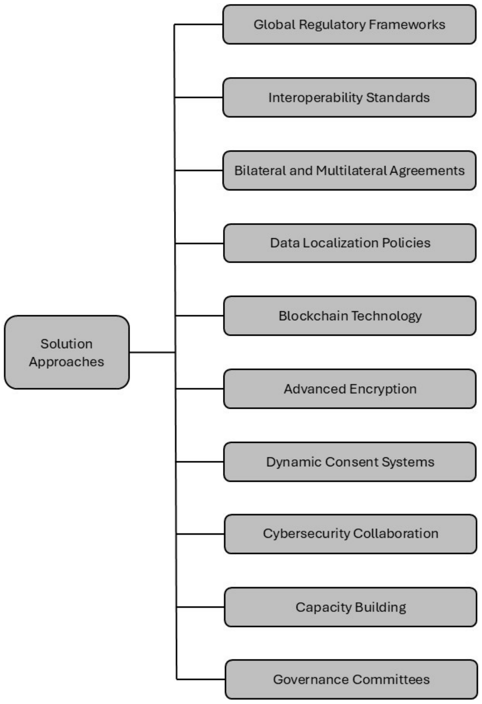
Solution Approaches
Global Regulatory Frameworks
Interoperability Standards
Bilateral and Multilateral Agreements
Data Localization Policies
Blockchain Technology
Advanced Encryption
Dynamic Consent Systems
Cybersecurity Collaboration
Capacity Building
Governance Committees

Figure 20: Solution approaches to address challenges associated with cross-border data sharing in IoHT.

- **Interoperability Standards:** Promotion of standardized data formats and exchange protocols globally can foster seamless data exchanges among IoHT stakeholders.
- **Bilateral and Multilateral Agreements:** The establishment of treaties and agreements among nations can foster consistent cross-border data exchange.
- **Data Localization Policies:** Implementation of hybrid models for data localization has the potential for balancing data sovereignty with diverse sharing needs.
- **Blockchain Technology:** The adoption of blockchain-based solutions, such as smart contracts and decentralized ledgers, can be leveraged for secure and auditable cross-border health data transactions and traceability in the IoHT ecosystem.
- **Advanced Encryption:** The application of advanced, robust data encryption methods can improve overall security during data transfer and storage.
- **Dynamic Consent Systems:** Digital solutions can be employed for secure and efficient management of patient consent activities, including obtaining, tracking, and managing patient consent.
- **Cybersecurity Collaboration:** Global partnerships for sharing threat intelligence and best practices can be fostered to improve cybersecurity measures across the IoHT landscape.
- **Capacity Building:** Global workshops on legal and regulatory requirements for IoHT can be conducted regularly to educate and train IoHT stakeholders on international compliance requirements.
- **Governance Committees:** Cross-national and global governance bodies can be developed to oversee cross-border IoHT data sharing and compliance frameworks to address disputes and enforce standards.

5. Strategies for Securing the Internet of Health Things

5.1 Implementing Strong Authentication and Access Controls

As the IoHT continues to expand, ensuring robust authentication and access control mechanisms becomes increasingly critical for the protection of sensitive health information and maintaining patient safety [111]. Strong authentication methods verify the identity of users and devices. On the other hand, access control measures restrict unauthorized access to medical data and IoHT systems. Implementing effective authentication and access control techniques helps mitigate security risks and enhances overall system integrity. Consequently, these techniques ensure that only authorized personnel can access sensitive information.

For implementing strong authentication and access controls in IoHT, the following methods and techniques are proposed [112–115] (Figure 21):

- **Multi-Factor Authentication (MFA):** MFA requires multiple forms of verification, such as passwords, biometrics (fingerprints or facial recognition), and security tokens. This way MFA enhances user identity verification and can reduce the risk of unauthorized access.
- **Multimodal Biometrics:** Methods that utilize multimodal biometrics, such as fingerprint and iris recognition, can develop robust identification and access control systems.
- **Role-Based Access Control (RBAC):** Implementation of RBAC allows organizations to grant permissions based on user roles. This can affirm that healthcare professionals have access only to the information that is necessary for their specific job functions and, thus, minimizes the risk of data exposure.
- **Public Key Infrastructure (PKI):** Utilization of PKI for encryption, digital signatures, and digital certificates helps verify device identities and secure communications. This can guarantee that data transmitted between IoHT devices and healthcare systems remains confidential and intact.

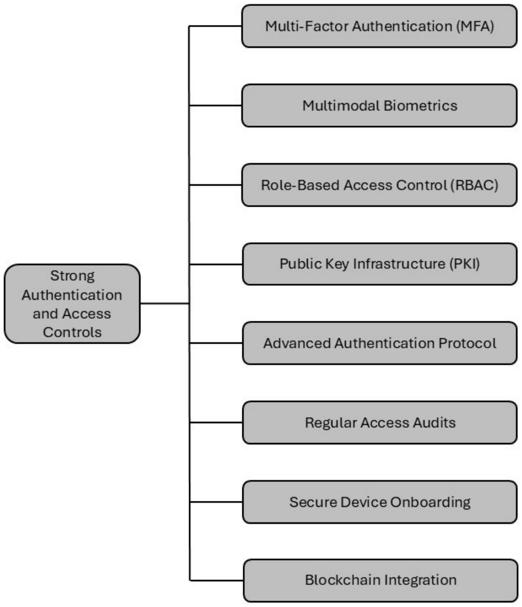
Strong Authentication and Access Controls
Multi-Factor Authentication (MFA)
Multimodal Biometrics
Role-Based Access Control (RBAC)
Public Key Infrastructure (PKI)
Advanced Authentication Protocol
Regular Access Audits
Secure Device Onboarding
Blockchain Integration

Figure 21: Methods and techniques for implementing strong authentication and access controls in IoHT.

- **Advanced Authentication Protocol:** Advanced secure authentication protocols, such as the Q-Net-based secret key generation approach [116], can be effective in assuring accurate authentication and improving system security.
- **Regular Access Audits:** Conducting periodic audits of user access rights helps identify and revoke unnecessary permissions. This can ensure that only authorized individuals retain access to sensitive medical data.
- **Secure Device Onboarding:** Secure onboarding processes can be established for new IoHT devices including authentication checks and firmware verification. This could help ensure that only trusted devices connect to the healthcare network.
- **Blockchain Integration:** Integration of blockchain technology into access control systems for the IoHT demonstrates effectiveness in improving security by blocking data tampering and minimizing trust-related expenses. Such incorporation has the potential to enhance the overall reliability of the system.

5.2 Encryption Techniques for Data Protection

In the context of the IoHT, protecting sensitive patient data is paramount due to the increasing prevalence of cyber threats. Encryption techniques play a vital role in safeguarding data during transmission and storage, ensuring that only authorized parties can access and interpret sensitive health information [117]. By converting plaintext into ciphertext, encryption helps maintain the confidentiality and integrity of medical data, thereby fostering patient trust and compliance with regulations such as HIPAA and GDPR. Employing effective encryption methods is essential for mitigating risks associated with data breaches and unauthorized access in IoHT environments.

The following encryption techniques for data protection in IoHT are proposed [35, 60, 76, 118, 119] (Figure 22):

- **Symmetric Encryption:** Utilizing a single shared key for both encryption and decryption, symmetric encryption algorithms such as Advanced Encryption Standard (AES) offer fast processing speeds, making them suitable for encrypting large volumes of data transmitted between IoHT devices and healthcare systems.
- **Asymmetric Encryption:** Asymmetric algorithms, such as RSA or Elliptic Curve Cryptography (ECC), use a pair of keys (public and private) for secure data exchange. This method enhances security for communications between devices, allowing for secure key exchanges without transmitting sensitive information.

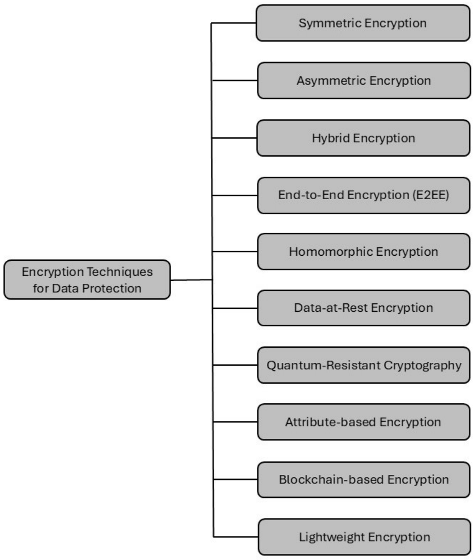
Encryption Techniques for Data Protection
Symmetric Encryption
Asymmetric Encryption
Hybrid Encryption
End-to-End Encryption (E2EE)
Homomorphic Encryption
Data-at-Rest Encryption
Quantum-Resistant Cryptography
Attribute-based Encryption
Blockchain-based Encryption
Lightweight Encryption

Figure 22: Proposed encryption techniques for data protection in IoHT.

- **Hybrid Encryption:** Combines symmetric and asymmetric encryption for optimal security and performance. A symmetric key is used to encrypt the data, and the symmetric key itself is encrypted using a public key.
- **End-to-End Encryption (E2EE):** Implementing E2EE ensures that data are encrypted on the sender's device and only decrypted on the recipient's device. This approach protects data throughout its entire journey, preventing interception during transmission.
- **Homomorphic Encryption:** This advanced technique allows computations to be performed on encrypted data without decrypting it, preserving data privacy while enabling data analysis in healthcare applications, even in cloud environments.
- **Data-at-Rest Encryption:** Encrypting stored data on IoHT devices and databases protect sensitive health information from unauthorized access in the event of physical device theft or compromise.
- **Quantum-Resistant Cryptography:** Exploits quantum mechanics to provide security against potential quantum computing attacks. Examples: Lattice-based cryptography, code-based cryptography, and multivariate cryptography.
- **Attribute-based Encryption:** Implements access control policies based on user attributes, ensuring fine-grained data access management.

- **Blockchain-based Encryption:** Leverages distributed ledger technology to create tamper-resistant and transparent data storage systems.
- **Lightweight Encryption:** Lightweight Cryptography (LWC) is commonly used for securing IoHT data due to its efficiency in low-power environments. Additionally, Lightweight Medical Image Cryptography (LW-MIC) systems, utilizing ensemble lightweight cryptographic protocols, enhance security for sensitive medical data transmitted through IoMT devices.

These encryption techniques not only secure health data but also optimize performance in resource-constrained IoHT environments, emphasizing the importance of tailored cryptographic solutions for data protection in healthcare IoT applications.

5.2.1 End-to-End Encryption

End-to-end encryption plays a crucial role in safeguarding sensitive health data in the IoHT. Various encryption techniques have been proposed to address security challenges in IoHT devices [120, 121]. Lightweight encryption systems, such as the Photon-Beetle AEAD algorithm and ensemble lightweight cryptographic protocols, have been designed to ensure robust security while minimizing resource consumption in resource-constrained IoHT devices [122, 123]. These encryption methods utilize techniques such as the Secret Sharing Algorithm (SSA) and Cha-Cha-based encryption to protect medical data during transmission and storage. Implementing end-to-end encryption through these lightweight cryptographic solutions enhances data privacy, security, and integrity in IoHT environments, addressing the critical need for secure communication and storage of sensitive health information.

5.2.2 Data Masking and Tokenization

Tokenization is a technique that replaces sensitive data with non-sensitive tokens, reducing the risk of data breaches. Data masking and tokenization play crucial roles in safeguarding data in the IoHT systems. In the realm of IoMT, where security and privacy are paramount [124], techniques such as masking-enabled data protection and Physically Unclonable Functions (PUFs) are employed to ensure data privacy [59]. The use of masking techniques, such as the Secret Sharing Algorithm (SSA) and the Octopus, helps in splitting and encrypting health data, preventing unauthorized access, and maintaining data integrity [125]. These methods not only secure sensitive health information but also leverage ML for data retrieval with high accuracy, showcasing their effectiveness in enhancing data protection in IoHT environments.

5.3 Secure Software Development Practices for IoHT Applications

Given that IoHT is a rapidly evolving domain, for ensuring the protection of sensitive health data and the integrity of connected medical devices, it is essential to secure the software development practices [126, 127]. Various applications run on IoHT devices and infrastructures providing different healthcare services. Day by day an increasing number of cyber threats are being directed to these healthcare applications. Consequently, the integration of security into every phase of the software development lifecycle (SDLC) is extremely critical. Moreover, the incorporation of frameworks that can enable secure and scalable IoHT platforms is essential for further strengthening application security [128]. Such proactive approaches mitigate vulnerabilities and foster a culture of security awareness among developers. This can guarantee that IoHT applications are resilient against potential attacks. Furthermore, establishing data security during data flow and storage is a prerequisite for ensuring privacy and confidentiality in medical IoT environments [129]. To mitigate risks and build resilient IoHT applications, system and software developers need to follow standards and recommendations and leverage advanced security protocols. Through the adoption of secure software development practices, the overall reliability and safety of healthcare systems be protected which will facilitate safeguarding patient information and maintaining trust in IoHT technologies.

For robust protection of IoHT applications, the following secure software development practices are proposed [126, 130–134] (Figure 23):

- **Threat Analysis and Modeling:** For creating a secure IoHT system, it is essential to analyze threats that are specific to healthcare IoT applications so that the security measures can be tailored accordingly. Threat modeling should be conducted starting from the design phase as it can identify potential security risks and vulnerabilities from the beginning of SDLC. This empowers developers to implement appropriate countermeasures early in the development process.
- **Secure Coding Practices:** Software developers should follow established secure coding guidelines such as OWASP Top Ten. Adhering to the standards and best coding practices, developers can avoid common vulnerabilities such as SQL injection and cross-site scripting (XSS) that would reduce the risk of exploitation.
- **Input Validation:** Input validation and sanitization process can prevent malicious code injection and other attacks.
- **Output Encoding:** The application of appropriate encoding for outputs can prevent vulnerabilities such as cross-site scripting and other vulnerabilities.

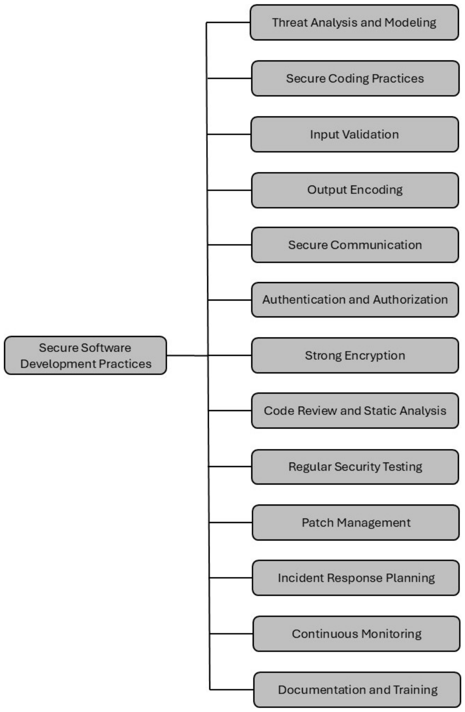
Secure Software Development Practices
Threat Analysis and Modeling
Secure Coding Practices
Input Validation
Output Encoding
Secure Communication
Authentication and Authorization
Strong Encryption
Code Review and Static Analysis
Regular Security Testing
Patch Management
Incident Response Planning
Continuous Monitoring
Documentation and Training

Figure 23: Secure software development practices for IoHT applications.

- **Secure Communication:** Secure Communication: Data in transit must be secured using secure communication protocols such as TLS/SSL and HTTPS.
- **Robust Authentication and Authorization:** Strong privacy-preserving authentication and authorization mechanisms must be implemented to control access to IoHT applications and data, including Zero-Knowledge Proof Authentication [135] and Anonymous Credential Systems [136].
- **Strong Encryption:** Encryption mechanisms must be applied to sensitive data at rest and in transit to protect it from unauthorized access.
- **Code Review and Static Analysis:** Ahead of software deployment, regular code review exercises and static analysis tools should be applied so that any security flaws and vulnerabilities can be detected early enough. This can guarantee higher levels of code quality and security.
- **Regular Security Testing:** To identify and fix security weaknesses in IoHT applications, periodic security testing, such as penetration

testing and vulnerability assessments, must be conducted throughout the SDLC before rolling out the software applications.

- **Patch Management:** A robust patch management process must be ensured so that software can be updated in a timely fashion and any security vulnerabilities can be corrected before security attacks can be successful. This can reduce the risk of exploitation in IoHT applications active in operations.
- **Incident Response Planning:** An incident response plan must be developed and implemented so that any unforeseen security breaches can be responded quickly and effectively to minimize the adverse effects.
- **Continuous Monitoring:** IoHT applications and services need to be monitored closely to identify any signs of security attacks and take necessary actions promptly to contain the security risks and reduce the impact.
- **Documentation and Training:** Software developers should be provided with proper documentation of security practices and facilitated with regular training for their continuous and sustained professional development. Such measures and activities foster a culture of security awareness and promote adherence to secure software development practices.

6. Risk Management in Digital Health

6.1 Conducting Threat Modeling Exercises

Threat modeling plays a crucial role in risk management within digital health systems [130, 137]. The interconnected nature of healthcare IT infrastructures makes them susceptible to cyber threats due to the heterogeneity of systems and the varied stakeholders involved [31]. The adoption of IoT in healthcare brings about numerous benefits but also introduces new vulnerabilities and risks that need to be addressed through effective threat and risk management strategies [138, 139]. By utilizing ML models and customized threat modeling techniques, organizations can identify and analyze potential security threats, ultimately enhancing the security posture of digital health systems. Implementing qualitative risk approaches and tailored threat modeling frameworks can help mitigate risks and ensure the confidentiality and integrity of sensitive health data in the evolving digital health landscape.

Threat modeling is a proactive approach to identifying, assessing, and mitigating potential threats to systems and networks. In the context of the IoHT and digital health, where patient data, critical devices, and healthcare services are involved, threat modeling is essential to ensure

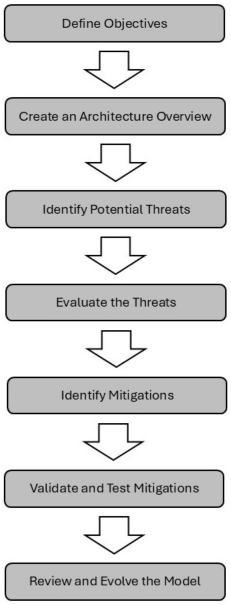
Define Objectives
Create an Architecture Overview
Identify Potential Threats
Evaluate the Threats
Identify Mitigations
Validate and Test Mitigations
Review and Evolve the Model

Figure 24: Standard procedure for conducting threat modeling exercises in IoHT.

security, privacy, and reliability [140]. The following outlines a standard procedure for conducting threat modeling exercises tailored to IoHT and digital health systems [141–144] (Figure 24).

A. Define Objectives

- **Identify Key Assets:** In IoHT and Digital Health systems, critical assets typically include patient data (e.g., medical records, diagnostic information), connected medical devices (e.g., pacemakers, insulin pumps), and digital platforms (e.g., telemedicine services).
- **Understand the Context:** Define the scope of the system (e.g., hospital networks, remote patient monitoring systems) and its regulatory environment (e.g., HIPAA in the U.S., GDPR in the EU).
- **Security Goals:** Determine core security requirements such as confidentiality, integrity, availability, and data privacy.

B. Create an Architecture Overview

- **Identify Components:** List all devices, sensors, applications, and networks in the IoHT ecosystem. This may include wearable health monitors, patient data gateways, hospital information systems, cloud services, and mobile health apps.

- **Draw Data Flows:** Map out how data flow between IoHT devices, cloud platforms, and healthcare providers. Include how patient data are collected, transmitted, stored, and accessed.
- **Determine Trust Boundaries:** Identify areas where data move from one system to another, such as between a patient's wearable device and the cloud, or a healthcare provider's app and a medical database.

C. Identify Potential Threats

- **Use Threat Modeling Frameworks:** Apply frameworks such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) or PASTA (Process for Attack Simulation and Threat Analysis).
- **Understand Common IoHT Vulnerabilities:** Focus on known vulnerabilities in medical devices and health data systems, such as weak encryption, default credentials, and unpatched software.
- **Consider Insider and Outsider Threats:** Both external cybercriminals and internal personnel (such as healthcare workers or IT staff) can pose security risks.
- **Evaluate Supply Chain Risks:** Medical devices and health platforms often rely on third-party vendors, so assess risks in the supply chain, including hardware backdoors and software vulnerabilities.

D. Evaluate the Threats

- **Assess Threat Likelihood and Impact:** The probability of each of the identified threats to occur should be evaluated. Then, the potential impact of each threat on patient safety, data security, or healthcare operations should be assessed.
- **Prioritize Risks:** The threats should be ranked according to their severity on the IoHT ecosystem. Risks that could have impacts on patient safety, such as tampering with medical device data, must be given the highest priority.

E. Identify Mitigations

- **Implement Security Controls:** Based on the prioritized threats, propose mitigations such as encryption for data transmission, access control mechanisms (e.g., multi-factor authentication), and device integrity checks.
- **Address Privacy Concerns:** For the threats that can compromise sensitive data, implement security measures that preserve privacy such as data anonymization and secure cloud storage.

- **Mitigate Supply Chain Risks:** Ensure that third-party vendors comply with security standards. Regularly audit their devices and software for vulnerabilities.

F. Validate and Test Mitigations

- **Penetration Testing:** Conduct penetration tests on the IoHT ecosystem to evaluate the effectiveness of the implemented mitigation techniques.
- **Vulnerability Assessments:** Vulnerability assessments must be conducted on a regular basis, in particular after deployment of new devices or updates.
- **Monitor Security Events:** Use real-time monitoring and logging tools to detect potential security incidents early.

G. Review and Evolve the Model

- **Continuous Improvement:** Threat modeling should not be considered as a one-time exercise. The model should be revisited and reviewed periodically to check for new threats, technologies, and system updates.
- **Collaborate with Stakeholders:** Involve healthcare providers, IT professionals, and medical device manufacturers in periodic threat assessments to ensure the model remains relevant.
- **Stay Updated on Regulations:** Continuously adapt the threat model to evolving healthcare regulations and compliance requirements, such as FDA cybersecurity guidelines for medical devices.

Securing IoHT and Digital Health systems requires ongoing attention to potential threats, vulnerabilities, and mitigations. By following a systematic threat modeling process, healthcare providers can identify and address risks before they lead to significant data breaches, service disruptions, or patient harm.

6.2 Continuous Monitoring and Incident Response

Continuous monitoring and incident response play crucial roles in risk management within digital health settings [145, 146]. Continuous data monitoring through digital devices enables the collection of real-time high-quality data, aiding in feedback-led optimization and ensuring the safety and performance of digital health applications [147]. This monitoring allows for the identification of patterns and relationships in data, supporting healthcare decision-making and improving patient outcomes [148]. Additionally, incident monitoring and response systems can limit functionality during incidents, enhancing security and response capabilities. To manage risks effectively, a proactive approach is essential, involving the adaptation of traditional risk management standards to work continuously, incorporating incident and event management tools, misbehavior detection, and threat intelligence. Continuous monitoring and incident response are vital components in maintaining the security and effectiveness of digital health technologies.

7. Collaborative Approaches to IoHT Security

7.1 Industry Partnerships for Threat Intelligence Sharing

Industry partnerships play a crucial role in enhancing threat intelligence sharing for IoHT security [149]. Collaborative efforts, such as the SECANT[9] project, aims to strengthen cybersecurity risk assessment in complex ICT infrastructures such as healthcare, emphasizing the importance of sharing threat intelligence for improved digital security and privacy [150]. Additionally, the development of new threat intelligence frameworks, such as the one focusing on CoAP protocol attacks, highlights the need for industry partnerships to model and mitigate advanced cyber threats effectively [151]. There is a high potential that industry collaborations and partnerships can significantly improve the security of IoHT ecosystems by leveraging centralized and federated transfer learning modes and innovative algorithms for threat detection and classification [35]. These partnerships facilitate the implementation of comprehensive security measures, ensuring the protection of sensitive healthcare data and systems.

7.1.1 Challenges Associated with Threat Intelligence Sharing

Although the benefits are evident, industry partnerships for threat intelligence sharing in the IoHT face numerous challenges, ranging from privacy concerns to interoperability issues. These obstacles hinder collaboration and the timely exchange of critical information [152]. As a consequence, addressing these complexities is essential for enhancing IoHT security and safeguarding sensitive healthcare data from emerging threats.

Figure 25 presents a taxonomy of the challenges associated with industry partnerships for threat intelligence sharing in the field of IoHT [153–156]:

- **Data Privacy Concerns**: Sensitive patient or healthcare data may need to be shared among organizations for threat intelligence. This can raise concerns about violating privacy laws such as HIPAA or GDPR.

[9] https://secant-project.eu.

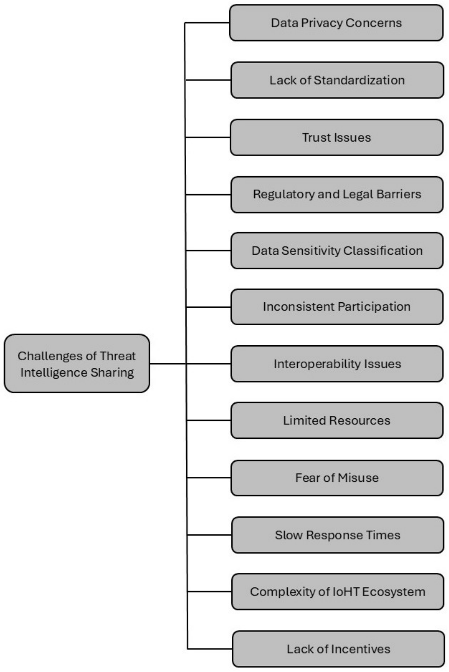
Challenges of Threat Intelligence Sharing
Data Privacy Concerns
Lack of Standardization
Trust Issues
Regulatory and Legal Barriers
Data Sensitivity Classification
Inconsistent Participation
Interoperability Issues
Limited Resources
Fear of Misuse
Slow Response Times
Complexity of IoHT Ecosystem
Lack of Incentives

Figure 25: A taxonomy of the challenges associated with threat intelligence sharing in the IoHT.

- **Lack of Standardization:** Different organizations may use varying formats and frameworks for threat intelligence, making it difficult to share and interpret data efficiently.
- **Trust Issues:** Industry partners may not be interested in exchanging threat data considering concerns about reputational damage, legal liability, or exposing their vulnerabilities to competitors.
- **Regulatory and Legal Barriers:** Threat intelligence may be hindered due to the strict healthcare regulations. This can complicate the process of sharing threat intelligence data. Such complications can be even harder to manage when working across borders or in jurisdictions with different legal requirements.
- **Data Sensitivity Classification:** Difficulty in distinguishing between sensitive and non-sensitive threat intelligence can slow down or prevent sharing due to concerns over inadvertently disclosing critical data.
- **Inconsistent Participation:** There may be some stakeholders within the IoHT ecosystem who are not equally interested or committed to or

capable of contributing to threat intelligence sharing. This can create gaps in intelligence coverage.

- **Interoperability Issues:** In the process of sharing threat intelligence across different platforms, compatibility challenges may arise in situations where healthcare systems and IoHT devices use proprietary technology with incompatible interfaces for information exchange.
- **Limited Resources:** Smaller healthcare providers or IoHT device manufacturers may lack the technical and financial resources to participate effectively in threat intelligence networks.
- **Fear of Misuse:** There may be worries among organizations that the shared threat intelligence could be misused by competitors or malicious actors within the network.
- **Slow Response Times:** Industry partnerships may result in bureaucratic delays, making it difficult to share threat intelligence quickly enough to respond to emerging threats in real time.
- **Complexity of IoHT Ecosystem:** The complexity of identifying and sharing relevant threat intelligence can be exacerbated due to the diverse range of connected devices and systems in IoHT increases.
- **Lack of Incentives:** Without clear incentives or benefits, organizations may be reluctant to invest time and resources into threat intelligence sharing partnerships.

7.1.2 Potential Solution Approaches

To overcome the challenges associated with threat intelligence sharing in the IoHT ecosystem, coordinated efforts among IoHT organizations and innovative strategies are essential. The following potential solution approaches aim to address issues related to privacy, interoperability, trust, and other barriers to promote a more secure and collaborative environment for safeguarding IoHT systems [15, 86, 94, 153, 157] (Figure 26):

- **Develop Standardized Frameworks:** To facilitate smooth sharing of threat intelligence across industry partners, common formats and protocols can be established, such as utilizing STIX/TAXII[10] (Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information).
- **Enhance Privacy-Preserving Techniques:** Implement data anonymization and encryption methods to ensure sensitive healthcare data are protected while still allowing for effective threat intelligence sharing.

[10] https://oasis-open.org.

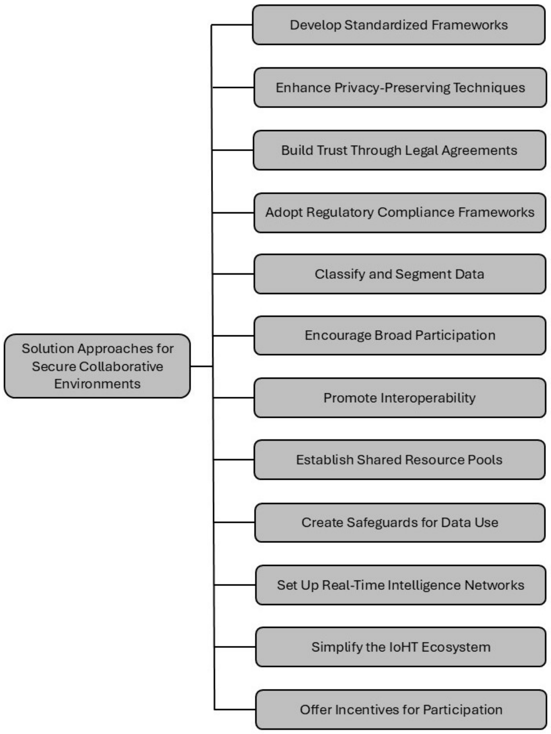
Solution Approaches for Secure Collaborative Environments
Develop Standardized Frameworks
Enhance Privacy-Preserving Techniques
Build Trust Through Legal Agreements
Adopt Regulatory Compliance Frameworks
Classify and Segment Data
Encourage Broad Participation
Promote Interoperability
Establish Shared Resource Pools
Create Safeguards for Data Use
Set Up Real-Time Intelligence Networks
Simplify the IoHT Ecosystem
Offer Incentives for Participation

Figure 26: Potential solution approaches for secure and collaborative IoHT environments.

- **Build Trust Through Legal Agreements:** Formal legal agreements can be made among IoHT collaborators, such as Memorandums of Understanding (MoUs) or Non-Disclosure Agreements (NDAs) that can foster trust and ensure the proper handling of shared threat intelligence.
- **Adopt Regulatory Compliance Frameworks:** Develop threat intelligence-sharing frameworks that align with healthcare regulations such as HIPAA and GDPR to ensure legal compliance and streamline cross-border data exchange.
- **Classify and Segment Data:** Establish clear guidelines for distinguishing between sensitive and non-sensitive information to facilitate more efficient and safer sharing of threat intelligence.
- **Encourage Broad Participation:** Smaller organizations and stakeholders can be motivated by incentivizing them to contribute by providing financial or technical assistance. This can effectively foster a more inclusive threat intelligence network.

- **Promote Interoperability:** Advocate for the adoption of open standards and APIs that enable seamless communication and integration between different IoHT devices and platforms.
- **Establish Shared Resource Pools:** Pool resources such as shared threat intelligence platforms, cybersecurity training, and tools to support smaller players in the IoHT ecosystem who may lack the capacity to participate fully.
- **Create Safeguards for Data Use:** To prevent the misuse of shared threat intelligence, policies and governance structures can be developed. This can guarantee that information is used only for cybersecurity purposes.
- **Set Up Real-Time Intelligence Networks:** Implement automated, real-time threat intelligence-sharing platforms that minimize delays and allow for quick responses to emerging threats across the IoHT ecosystem.
- **Simplify the IoHT Ecosystem:** Promotion of the development of interoperable, modular systems that reduce complexity and make it easier for organizations to share relevant threat intelligence.
- **Offer Incentives for Participation:** Provide tangible incentives, such as cybersecurity certifications, risk reduction benefits, or financial rewards, to motivate organizations to actively engage in threat intelligence sharing.

7.2 *Cross-Sector Collaboration with Technology and Security Experts*

Cross-sector collaborations involving technology and security experts are crucial for enhancing the security of the IoHT. Security risks in IoMT devices, such as vulnerabilities due to limited processing power and memory [35], underscore the need for collaborative efforts. Research highlights the security challenges faced by medical IoT devices and emphasizes the importance of focusing on security issues throughout the device life cycle [158]. Additionally, integrating multi-ledger blockchain architecture in IoMT can enhance security by providing decentralized data storage. This can effectively eliminate single points of failure and improve trust and reliability [159]. By leveraging ML techniques for anomaly detection and risk assessment in IoMT environments, a holistic evaluation of security risks in Connected Medical Devices (CMD) can be achieved [160]. Collaborative initiatives between experts from different sectors can lead to effective processes for securing IoMT devices and safeguarding patient data.

8. Responsible Practices in Digital Health Security

8.1 Protecting Patient Anonymity in Data Analytics

In data analytics, maintaining patient anonymity within IoHT is an important criterion for upholding privacy standards and fostering trust. By anonymizing and de-identifying health data, healthcare providers can perform insightful analyses without exposing individuals' identities [161]. Valuable medical insights can be extracted using this approach. It also helps protect patient confidentiality and create an ethical framework. Both patient rights and regulatory requirements can be ensured by respecting patient anonymity.

8.2 Minimizing Data Collection and Retention

Minimizing data collection and retention in digital health systems reduces exposure to cyber threats and respects patient privacy [162]. Regulatory frameworks, such as HIPAA and GDPR, also emphasize only essential information collection and require IoHT organizations to retain it for the shortest possible time. This practice helps limit the potential for unauthorized access and signals respect for patients' digital privacy. Consequently, it can ensure maintaining data protection is a priority within IoHT security practices.

8.3 Preventing Unauthorized Surveillance and Data Misuse

In digital health, unauthorized surveillance and data misuse are critical ethical violations [163]. To protect sensitive health data from both internal and external threats, security and regulatory mechanisms, such as strong access controls, standard surveillance protocols, and regular audits, can be effective in guaranteeing data protection. Ethical practices that guard against unauthorized data usage and monitoring preserve patient trust, prevent exploitation, and help healthcare organizations maintain the integrity of their digital health infrastructures.

8.4 Ensuring Accountability in Data Breaches

Accountability in data breaches is essential for maintaining patient trust in IoHT systems [164]. Ethical standards require that organizations disclose breaches promptly, take corrective actions, and learn from incidents to bolster future security. This transparency helps mitigate harm to affected patients and reinforces public trust. Holding organizations accountable ensures that patient interests remain central in digital health, even when cybersecurity failures occur.

8.5 Empowering Patients with Data Access and Control

Empowering patients with control over their data reinforces trust and transparency in digital health systems [165]. Providing patients with options to view, manage, and consent to the use of their personal data promotes a patient-centric approach to IoHT security. This practice acknowledges patient autonomy, allows for informed decision-making, and aligns with ethical principles that place the individual's rights at the forefront of digital health security.

8.6 Ethical Implications of AI and Automation in IoHT Security

AI and automation in IoHT security present significant ethical considerations, particularly regarding transparency and bias [166]. Ethical practices call for algorithms that are explainable, fair, and aligned with patient interests. Responsible AI use ensures that automated security measures support rather than undermine patient trust, enabling healthcare providers to maintain transparency while leveraging technological advancements to protect sensitive health information securely and fairly.

8.7 Equitable Access to Secure Digital Health Services

Equitable and fair access to secure digital health services must be ensured regardless of socioeconomic status so that security protections can be made available to all patients. Addressing access disparities helps eliminate health inequities, providing secure, reliable care for everyone [167]. This ethical approach to IoHT security fosters inclusivity and ensures marginalized populations are not left vulnerable to digital threats due to a lack of resources or technological infrastructure.

8.8 Transparency in Security Measures and Data Usage

Transparency in data security and usage practices is an ethical necessity within IoHT. This is essential for building patient trust and supporting informed consent [168]. Accessible and clear information regarding data collection, storage, and protection helps patients understand their roles in the overall security landscape. Healthcare providers can create partnerships with patients by fostering data transparency. This can effectively empower patients to make informed decisions and knowledgeable choices about their digital health interactions.

8.9 Ensuring Ethical Use of Health Data in Cybersecurity Practices

Ethical leadership plays a crucial role in ensuring the ethical use of health data in cybersecurity practices in digital health. Healthcare organizations face significant risks from cyber data thefts, often leading to breaches that compromise patient care [169]. The healthcare industry's adoption of digital technology, including AI tools, has increased the need to address ethical issues in data security. Researchers have proposed novel ethical hacking methods tailored for Health Information Systems (HISs) to enhance cybersecurity protection [170]. Privacy concerns regarding the use of aggregated personal information in health practices highlight the importance of ethical decisions in data analytics technologies [171]. By integrating ethical leadership, cybersecurity measures, AI tools, and privacy considerations, healthcare organizations can navigate the complexities of maintaining ethical standards in digital health data security.

9. Future Directions and Conclusion

9.1 Anticipating the Evolution of IoHT Threat Landscape

Future threats and attacks on the IoHT encompass a range of vulnerabilities that need to be addressed to ensure the security and privacy of healthcare data. Various studies highlight the critical importance of implementing robust security measures [47, 68, 172–174]. Potential attacks include Deauth, DDOS, brute force, hashcat, MitM, Injection, Short Address Attack, and Smart Contract Overflow. These attacks target different stages such as home internet connection resources, data transfer, data storage, and access, emphasizing the need for comprehensive security protocols. Additionally, the use of blockchain and smart contracts is emerging as a preferred method for enhancing data security within the IoHT ecosystem. Addressing these future threats requires a multi-faceted approach that includes encryption, authentication, access control, and continuous monitoring to safeguard sensitive healthcare information.

9.2 Investing in Research and Innovation for Sustainable IoHT Security Solutions

Future directions in investing in research and innovation for sustainable IoHT security solutions involve leveraging technologies such as Blockchain-Assisted Cybersecurity (BCCS) [175], Computational Intelligence (CI), and AI for secure data transmission, collection, and storage [176]. Additionally, the integration of smart technologies with conventional medical procedures using AI techniques can enhance the quality of services while reducing environmental impact [177]. Emphasizing lightweight cryptography techniques for secure and eco-friendly IoT deployment is crucial for sustainable and secure IoMT systems [178]. Furthermore, exploring state-of-the-art techniques such as gated recurrent units (GRUs) combined with recurrent neural networks (RNNs) for disease detection, such as breast cancer, can pave the way for more efficient and secure IoMT models [179]. These approaches can guide future research toward developing robust, secure, and sustainable IoMT systems.

9.3 The Role of Stakeholders in Promoting a Secure and Trustworthy Digital Health Environment

Stakeholders play a crucial role in securing the digital health environment by addressing ethical, regulatory, and trust-related challenges [180]. Engaging stakeholders, including health professionals, IT practitioners, patients, and researchers, is essential for responsible digital health innovation [181, 182]. Understanding stakeholders' perspectives on big data and digital health is key to restoring trust and ensuring data governance [183]. Stakeholder collaboration, ethical awareness, and relevant regulations are identified as core impediments to responsible digital health. Involving users early in the innovation process, understanding their behavior changes, and ensuring true inclusion in the design space are critical for sustainable digital health solutions. Identifying and engaging relevant stakeholders using appropriate methods can enhance the efficacy and sustainability of digital health applications and services in the long run.

References

[1] Kaur, M., M. Sugadev, H. Kaur, M. R. Mahmood and V. Maheshwari. 2022. Healthcare Internet of Things. pp. 301–337. *In*: R. R. H. K. S. K. K. K. N. Md Rashid Mahmood (ed.). *Ambient Intelligence and Internet of Things*, Wiley. doi: 10.1002/9781119821847.ch10.

[2] Zakaria, R., A. H. Choudhury, M. Razin, M. S. Hossain, N. Hasan and M. I. Tahmid. 2022. Internet of Things (IoT) based Health Monitor Device. *4th International Conference on Electrical, Computer and Telecommunication Engineering, ICECTE 2022*, doi: 10.1109/ICECTE57896.2022.10114509.

[3] Wei, K., L. Zhang, Y. Guo and X. Jiang. 2020. Health monitoring based on internet of medical things: Architecture, enabling technologies, and applications. *IEEE Access*, 8: 27468–27478, doi: 10.1109/ACCESS.2020.2971654.

[4] Naresh, V. S., S. S. Pericherla, P. Sita Rama Murty and S. Reddi. 2020. Internet of Things in Healthcare: Architecture, applications, challenges, and solutions. *Computer Systems Science and Engineering*, 35(6): 411–421, doi: 10.32604/csse.2020.35.411.

[5] Askar, N. A., A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Y. Ziyodulla Yusupov and D. Kodirov. 2022. Architecture, protocols, and applications of the Internet of Medical Things (IoMT). *Journal of Communications*, pp. 900–918, doi: 10.12720/jcm.17.11.900-918.

[6] Pramanik, P. K. D., A. Solanki, A. Debnath, A. Nayyar, S. El-Sappagh and K. -S. Kwak. 2020. Advancing modern healthcare with nanotechnology, nanobiosensors, and internet of nano things: Taxonomies, applications, architecture, and challenges. *IEEE Access*, 8: 65230–65266, doi: 10.1109/ACCESS.2020.2984269.

[7] Abrar, I., Z. Ayub and F. Masoodi. 2021. Current trends and future scope for the Internet of Things. In *Internet of Things in Business Transformation*, Wiley, pp. 185–209. doi: 10.1002/9781119711148.ch11.

[8] Khatoon, N., S. Roy and P. Pranav. 2020. A survey on applications of Internet of Things in Healthcare, pp. 89–106. doi: 10.1007/978-3-030-39119-5_6.

[9] Johnston, C. 2022. *Digital Health Technologies*. First Edition. London: Routledge. doi: 10.4324/9781003220190.

[10] Imuede, J. and K. Imuede. 2023. Digital technologies on health services: A systemic review. In *Handbook of Research on AI and Knowledge Engineering for Real-Time Business Intelligence*, IGI Global, pp. 168–182. doi: 10.4018/978-1-6684-6519-6.ch011.

[11] Desai, A. and G. Karous. 2023. Digital health. In *Medical Innovation*, 1st Edition., Boca Raton: CRC Press, pp. 121–129. doi: 10.1201/9781003164609-15.

[12] Zwack, C. C., M. Haghani, M. Hollings, L. Zhang, S. Gauci, R. Gallagher and J. Redfern. Jan. 2023. The evolution of digital health technologies in cardiovascular disease research. *NPJ Digit. Med.*, 6(1), doi: 10.1038/s41746-022-00734-2.

[13] Colloud, S., T. Metcalfe, S. Askin, S. Belachew, J. Ammann, E. Bos, T. Kilchenmann, P. Strijbos, D. Eggenspieler, L. Servais, C. Garay, A. Konstantakopoulos, A. Ritzhaupt, T. Vetter, C. Vincenzi and F. Cerreta. Mar. 2023. Evolving regulatory perspectives on digital health technologies for medicinal product development. *NPJ Digit. Med.*, 6(1): 56, doi: 10.1038/s41746-023-00790-2.

[14] Adil, M., M. K. Khan, N. Kumar, M. Attique, A. Farouk, M. Guizani and Z. Jin. Jun. 2024. Healthcare Internet of Things: Security threats, challenges, and future research directions. *IEEE Internet Things J.*, 11(11): 19046–19069, doi: 10.1109/JIOT.2024.3360289.

[15] Yaacoub, J. P. A., M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier and A. Chehab. 2020. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Generation Computer Systems*, 105: 581–606, doi: 10.1016/j.future.2019.12.028.

[16] Affia, A. O., H. Finch, W. Jung, I. A. Samori, L. Potter and X. -L. Palmer. May 2023. IoT health devices: Exploring security risks in the connected landscape. *IoT*, 4(2): 150–182, doi: 10.3390/iot4020009.

[17] Kiran, R., A. Kumbhare, P. K. Thakur and S. Mane. 2023. Security and privacy in the Internet of Medical Things (IoMT). In *Revolutionizing Healthcare Through Artificial Intelligence and Internet of Things Applications*, IGI Global, pp. 1–27. doi: 10.4018/978-1-6684-5422-0.ch001.

[18] Thapa, S., A. Bello, A. Maurushat and F. Farid. Apr. 2023. Security risks and user perception towards adopting wearable Internet of Medical Things. *Int. J. Environ. Res. Public Health*, 20(8): 5519, doi: 10.3390/ijerph20085519.

[19] Czekster, R. M., P. Grace, C. Marcon, F. Hessel and S. C. Cazella. Jun. 2023. Challenges and opportunities for conducting dynamic risk assessments in medical IoT. *Applied Sciences*, 13(13): 7406, doi: 10.3390/app13137406.

[20] Sharma, M. and Dr. A. Kumar Bindal. Nov. 2022. Security issues in IoT: A review. In *2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Solan, Himachal Pradesh, India: IEEE, pp. 119–124. doi: 10.1109/PDGC56933.2022.10053255.

[21] Roobini, S., M. Kavitha, M. Sujaritha and D. Rajesh Kumar. 2022. Cyber-security threats to IoMT-enabled healthcare systems. In *Cognitive Computing for Internet of Medical Things*, Boca Raton: Chapman and Hall/CRC, pp. 105–130. doi: 10.1201/9781003256243-6.

[22] Abdi, A., H. Bennouri and A. Keane. Jun. 2024. Emerging cyber risks & threats in healthcare systems: A case study in resilient cybersecurity solutions. In *2024 13th Mediterranean Conference on Embedded Computing (MECO)*, IEEE, pp. 1–8. doi: 10.1109/MECO62516.2024.10577790.

[23] Wang, Z., J. Zhao, P. Sun, J. Yang, R. Wang and X. Zhang. Feb. 2023. A lightweight three-party mutual authentication protocol for Internet of Health Things Systems. *J. Healthc Eng.*, 2023: 1–15, doi: 10.1155/2023/1044282.

[24] Ahmed, M. M., L. Maglaras and M. A. Ferrag. 2022. Cyber threats in the healthcare sector and countermeasures. In *Research Anthology on Securing Medical Systems and Records*, IGI Global, pp. 1–16. doi: 10.4018/978-1-6684-6311-6.ch001.

[25] Kovács, A. M. and J. Besenyő. Apr. 2023. Healthcare cybersecurity threat context and mitigation opportunities. *Security Science Journal*, 4(1): 83–101, doi: 10.37458/ssj.4.1.6.

[26] Rai, S., R. Sharma, D. Mishra and N. Pathak. 2024. Cyber Terrorism in Health Information Systems, pp. 220–247. doi: 10.4018/979-8-3693-5976-1.ch011.

[27] Gupta, D. S., S. H. Islam, M. S. Obaidat, A. Karati and B. Sadoun. Sep. 2021. LAAC: Lightweight lattice-based authentication and access control protocol for E-Health systems in IoT environments. *IEEE Syst. J.*, 15(3): 3620–3627, doi: 10.1109/JSYST.2020.3016065.

[28] Hameed, S. S., W. H. Hassan, L. Abdul Latiff and F. Ghabban. Mar. 2021. A systematic review of security and privacy issues in the internet of medical things; The role of machine learning approaches. *Peer J. Comput. Sci.*, 7: e414, doi: 10.7717/peerj-cs.414.

[29] Yamcharoen, P., O. S. Folorunsho, A. Bayewu and T. P. Ojo. Dec. 2022. Impact of digitalizing healthcare business operations on cybersecurity landscape. *Advances in Multidisciplinary and Scientific Research Journal Publication*, 8(4): 27–34, doi: 10.22624/AIMS/BHI/V8N4P3.

[30] Osadchuk, M. A., A. M. Osadchuk, N. V. Kireeva and M. V. Trushin. Mar. 2020. Legal regulation in digital medicine. *Journal of Advanced Research in Law and Economics*, 11(1): 148, doi: 10.14505//jarle.v11.1(47).18.

[31] Surridge, M., K. Meacham, J. Papay, S. C. Phillips, J. B. Pickering, A. Shafiee and T. Wilkinson. 2019. Modelling compliance threats and security analysis of cross border health data exchange. In *International Conference on Model and Data Engineering* (pp. 180–189). Cham: Springer International Publishing.

[32] Liagkou, V., S. Sakka and C. Stylios. Sep. 2022. Security and privacy vulnerabilities in human activity recognition systems. In *2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, IEEE, pp. 1–6. doi: 10.1109/SEEDA-CECNSM57760.2022.9932957.

[33] Debar, H., R. Beuran and Y. Tan. 2020. A quantitative study of vulnerabilities in the Internet of Medical Things. In *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, SCITEPRESS—Science and Technology Publications, pp. 164–175. doi: 10.5220/0009105801640175.

[34] Badrouchi, F., A. Aymond, M. Haerinia, S. Badrouchi, D. F. Selvaraj, K. Tavakolian, P. Ranganathan and S. Eswaran. 2020. Cybersecurity vulnerabilities in biomedical devices: A hierarchical layered framework. *Internet of Things Use Cases for the Healthcare Industry*, 157–184.

[35] Jammula, M., V. M. Vakamulla and S. K. Kondoju. Jun. 2023. Secure and scalable internet of medical things using ensemble lightweight cryptographic model. In *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, IEEE, pp. 982–987. doi: 10.1109/ICSCSS57650.2023.10169857.

[36] Robertson, L. and A. Munoz. Mar. 2017. System configuration contributions to vulnerability: Applications to connected personal devices. *IEEE Technology and Society Magazine*, 36(1): 52–57, doi: 10.1109/MTS.2017.2654289.

[37] Rajasekar, V. R. and S. Rajkumar. Jul. 2023. A study on Internet of Things devices vulnerabilities using Shodan. *International Journal of Computing*, pp. 149–158, doi: 10.47839/ijc.22.2.3084.

[38] Nomikos, K., A. Papadimitriou, G. Stergiopoulos, D. Koutras, M. Psarakis and P. Kotzanikolaou. Aug. 2020. On a security-oriented design framework for medical IoT devices: The hardware security perspective. In *2020 23rd Euromicro Conference on Digital System Design (DSD)*, IEEE, pp. 301–308. doi: 10.1109/DSD51259.2020.00056.

[39] Somasundaram, R. and M. Thirugnanam. Nov. 2021. Review of security challenges in healthcare internet of things. *Wireless Networks*, 27(8): 5503–5509, doi: 10.1007/s11276-020-02340-0.

[40] Nissar, G., R. A. Khan, S. Mushtaq, S. A. Lone and A. H. Moon. 2023. A lightweight authentication scheme and security key establishment for internet of medical things, pp. 797–809. doi: 10.1007/978-981-99-1479-1_59.

[41] Rubí, J. N. S. and P. R. de L. Gondim. Jan. 2020. Interoperable internet of medical things platform for E-health applications. *Int. J. Distrib. Sens. Netw.*, 16(1): 155014771988959, doi: 10.1177/1550147719889591.

[42] Mwansa, G. and N. Mabanza. Feb. 2023. Review of Internet of Things security protocols—A bibliometric analysis. In *2023 25th International Conference on Advanced Communication Technology (ICACT)*, IEEE, pp. 394–400. doi: 10.23919/ICACT56868.2023.10079641.

[43] Nyangaresi, V. O. and J. Ma. Jun. 2022. A formally verified message validation protocol for intelligent IoT E-health systems. In *2022 IEEE World Conference on Applied Intelligence and Computing (AIC)*, IEEE, pp. 416–422. doi: 10.1109/AIC55036.2022.9848874.

[44] Md. M. Islam, S. Nooruddin, F. Karray and G. Muhammad. Feb. 2023. Internet of Things: Device capabilities, architectures, protocols, and smart applications in healthcare domain. *IEEE Internet Things J.*, 10(4): 3611–3641, doi: 10.1109/JIOT.2022.3228795.

[45] Cirne, A., P. R. Sousa, J. S. Resende and L. Antunes. May 2022. IoT security certifications: Challenges and potential approaches. *Comput. Secur.*, 116: 102669, doi: 10.1016/j.cose.2022.102669.

[46] Machal, M. L. 2023. An Overview About Connected Medical Devices and their Risks. doi: 10.3233/SHTI230438.

[47] Al-Abadi, A. A. J., M. B. Mohamed and A. Fakhfakh. Jun. 2023. Impact of availability attacks on enabling IoT based healthcare applications. In *2023 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, pp. 1666–1671. doi: 10.1109/IWCMC58020.2023.10183010.

[48] Jeyavel, J., T. Parameswaran, J. M. Mannan and U. Hariharan. 2021. Security vulnerabilities and intelligent solutions for IoMT systems, pp. 175–194. doi: 10.1007/978-3-030-63937-2_10.

[49] Jegatheswaran, R. A., I. J. Sakira and N. A. A. Rahman. Dec. 2020. A review on IoMT device vulnerabilities and countermeasures. *J. Phys. Conf. Ser.*, 1712(1): 012020, doi: 10.1088/1742-6596/1712/1/012020.

[50] Koutras, D., G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos and C. Douligeris. Aug. 2020. Security in IoMT communications: A survey. *Sensors*, 20(17): 4828, doi: 10.3390/s20174828.

[51] Kumar, A. and I. Sharma. May 2023. Enhancing data privacy of IoT healthcare with Keylogger attack mitigation. In *2023 4th International Conference for Emerging Technology (INCET)*, IEEE, pp. 1–6. doi: 10.1109/INCET57972.2023.10170531.

[52] Shree, S., C. Zhou and M. Barati. 2024. Data protection in internet of medical things using blockchain and secret sharing method. *J. Supercomput.*, 80(4): 5108–5135.

[53] Wani, R. U. Z., F. Thabit and O. Can. 2023. Security and Privacy Challenges, Issues, and Enhancing techniques for Internet of Medical Things: A systematic review.

[54] AbdulRaheem, M., J. B. Awotunde, C. Chakraborty, E. A. Adeniyi, I. D. Oladipo and A. K. Bhoi. 2023. Security and privacy concerns in smart healthcare system. In *Implementation of Smart Healthcare Systems using AI, IoT, and Blockchain*, Elsevier, pp. 243–273. doi: 10.1016/B978-0-323-91916-6.00002-3.

[55] Krishnan, D. and S. Singh. 2022. Medical IoT: Opportunities, issues in security and privacy—A comprehensive review. In *Smart and Secure Internet of Healthcare Things*, Boca Raton: CRC Press, pp. 91–112. doi: 10.1201/9781003239895-6.

[56] Hasan, M. K. et al 2021. Lightweight encryption technique to enhance medical image security on Internet of Medical things applications. *IEEE Access*, 9: 47731–47742, doi: 10.1109/ACCESS.2021.3061710.

[57] Kamalov, F., B. Pourghebleh, M. Gheisari, Y. Liu and S. Moussa. Feb. 2023. Internet of Medical Things privacy and security: Challenges, solutions, and future trends from a new perspective. *Sustainability*, 15(4): 3317, doi: 10.3390/su15043317.

[58] Ghubaish, A., T. Salman, M. Zolanvari, D. Unal, A. Al-Ali and R. Jain. Jun. 2021. Recent advances in the Internet-of-Medical-Things (IoMT) systems security. *IEEE Internet Things J.*, 8(11): 8707–8718, doi: 10.1109/JIOT.2020.3045653.

[59] Shree, S., C. Zhou and M. Barati. 2024. Data protection in internet of medical things using blockchain and secret sharing method. *J. Supercomput.*, 80(4): 5108–5135.

[60] Munjal, K. and R. Bhatia. Aug. 2023. A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems*, 9(4): 3759–3786, doi: 10.1007/s40747-022-00756-z.

[61] Hineman, A. and M. Blaum. Apr. 2022. A modified shamir secret sharing scheme with efficient encoding. *IEEE Communications Letters*, 26(4): 758–762, doi: 10.1109/LCOMM.2022.3144375.

[62] Mohan, P. Feb. 2023. IoT preserving patient-centric models for privacy preserving based personal health records sharing in cloud. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, IEEE, pp. 1–6. doi: 10.1109/ICICACS57338.2023.10100155.

[63] Khatiwada, P. and B. Yang. 2022. An overview on security and privacy of data in IoMT devices: Performance Metrics, Merits, Demerits, and Challenges. doi: 10.3233/SHTI220970.

[64] Gadekallu, T. R., M. Alazab, J. Hemanth and W. Wang. Feb. 2023. Guest editorial federated learning for privacy preservation of healthcare data in internet of medical things and patient monitoring. *IEEE J. Biomed. Health Inform.*, 27(2): 648–651, doi: 10.1109/JBHI.2023.3234604.

[65] Mittal, A. and F. Sidney. Feb. 2023. Privacy preserving based personal health records sharing using Rail Fence Data Encryption (RFDE) for secure cloud environment. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, IEEE, pp. 1–5. doi: 10.1109/ICICACS57338.2023.10099585.

[66] Liu, J., J. Yang, W. Wu, X. Huang and Y. Xiang. May 2023. Lightweight authentication scheme for data dissemination in cloud-assisted healthcare IoT. *IEEE Transactions on Computers*, 72(5): 1384–1395, doi: 10.1109/TC.2022.3207138.

[67] Diop, I. M., C. Cherifi, C. Diallo and H. Cherifi. 2023. Targeted Attacks Based on Networks Component Structure, pp. 62–73. doi: 10.1007/978-3-031-28276-8_6.

[68] Süzen, A. A. Apr. 2023. Cyber attacks for data breach and possible defense strategies in Internet of Healthcare Things ecosystem. *International Journal of 3D Printing Technologies and Digital Industry*, 7(1): 55–63, doi: 10.46519/ij3dptdi.1240743.

[69] Kumar, A. and I. Sharma. May 2023. Augmenting IoT healthcare security and reliability with early detection of IoT botnet attacks. In *2023 4th International Conference for Emerging Technology (INCET)*, IEEE, pp. 1–6. doi: 10.1109/INCET57972.2023.10170738.

[70] Nusairat, T., M. M. Saudi and A. Bin Ahmad. Aug. 2023. A recent assessment for the ransomware attacks against the Internet of Medical Things (IoMT): A review. In *2023 IEEE 13th International Conference on Control System, Computing and Engineering (ICCSCE)*, IEEE, pp. 238–242. doi: 10.1109/ICCSCE58721.2023.10237161.

[71] Garcia-Perez, A., J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro and A. Chinnaswamy. Mar. 2023. Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, 121: 102583, doi: 10.1016/j.technovation.2022.102583.

[72] Al-Abadi, A. A. J., M. B. Mohamed and A. Fakhfakh. Dec. 2023. Enhanced Random Forest Classifier with K-Means Clustering (ERF-KMC) for detecting and preventing distributed-denial-of-service and man-in-the-middle attacks in internet-of-medical-things networks. *Computers*, 12(12): 262, doi: 10.3390/computers12120262.

[73] Peddle, B., W. Lu and Q. Yu. 2024. Detecting DDoS Attacks in the Internet of Medical Things Through Machine Learning-Based Classification, pp. 191–203. doi: 10.1007/978-3-031-47126-1_13.

[74] Kim, K., J. Ryu, Y. Lee and D. Won. Jan. 2023. An improved lightweight user authentication scheme for the internet of medical things. *Sensors*, 23(3): 1122, doi: 10.3390/s23031122.

[75] Zubair, M., D. Unal, A. Al-Ali and A. Shikfa. Jul. 2019. Exploiting bluetooth vulnerabilities in e-Health IoT devices. In *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, New York, NY, USA: ACM, pp. 1–7. doi: 10.1145/3341325.3342000.

[76] Sowjanya, K., M. Dasgupta and S. Ray. May 2021. Elliptic Curve Cryptography based authentication scheme for Internet of Medical Things. *Journal of Information Security and Applications*, 58: 102761, doi: 10.1016/j.jisa.2021.102761.

[77] Rahman, M. and H. Jahankhani. 2021. Security vulnerabilities in existing security mechanisms for IoMT and potential solutions for mitigating cyber-attacks, pp. 307–334. doi: 10.1007/978-3-030-72120-6_12.

[78] Li, N., M. Xu, Q. Li, J. Liu, S. Bao, Y. Li, J. Li and H. Zheng. 2023. A review of security issues and solutions for precision health in Internet-of-Medical-Things systems. *Security and Safety*, 2: 2022010, doi: 10.1051/sands/2022010.

[79] Verma, H., N. Chauhan and L. K. Awasthi. Nov. 2023. A comprehensive review of 'Internet of Healthcare Things': Networking aspects, technologies, services, applications, challenges, and security concerns. *Comput. Sci. Rev.*, 50: 100591, doi: 10.1016/j.cosrev.2023.100591.

[80] Gaikwad, V. P., J. V. Tembhurne, C. Meshram and C. -C. Lee. Aug. 2021. Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function. *J. Supercomput.*, 77(8): 8281–8304, doi: 10.1007/s11227-020-03553-y.

[81] Xie, Y., H. Luo, L. Liang and J. Gan. Nov. 2024. A lightweight dual-link accelerated authentication protocol based on NLFSR-XOR APUF. *Microelectronics J.*, 153: 106446, doi: 10.1016/j.mejo.2024.106446.

[82] Ghazal, T. M., N. A. Al-Dmour, T. Mohamed, Z. Chabani, S. Harguem, S. Noamas and N. ALMaazmi. Nov. 2022. E-supply chain issues in internet of medical things. In *2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)* (pp. 1–5). IEEE.

[83] Rawat, R. Nov. 2022. A systematic review of blockchain technology use in E-Supply chain in Internet of Medical Things (IoMT). *International Journal of Computations, Information and Manufacturing (IJCIM)*, 2(2), doi: 10.54489/ijcim.v2i2.119.

[84] Guergov, S. Nov. 2022. Investigating E-Supply chain issues in Internet of Medical Things (IoMT): Evidence from the healthcare. *International Journal of Computations, Information and Manufacturing (IJCIM)*, 2(2), doi: 10.54489/ijcim.v2i2.110.

[85] Qadri, Y. A., Zulqarnain, A. Nauman, A. Musaddiq, E. Garcia-Villegas and S. W. Kim. Aug. 2022. Preparing Wi-Fi 7 for healthcare Internet-of-Things. *Sensors*, 22(16): 6209, doi: 10.3390/s22166209.

[86] Shahid, J., R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed and A. M. Almuhaideb. Feb. 2022. Data protection and privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences*, 12(4): 1927, doi: 10.3390/app12041927.

[87] Iqbal, J. D. and N. Biller-Andorno. Sep. 2022. The regulatory gap in digital health and alternative pathways to bridge it. *Health Policy Technol.*, 11(3): 100663, doi: 10.1016/j.hlpt.2022.100663.

[88] Elhoseny, M., N. N. Thilakarathne, M. I. Alghamdi, R. K. Mahendran, A. A. Gardezi, H. Weerasinghe and A. Welhenge. 2021. Security and privacy issues in medical internet of things: Overview, countermeasures, challenges and future directions. *Sustainability*, 13(21): 11645.

[89] Guo, C., H. Ashrafian, S. Ghafur, G. Fontana, C. Gardner and M. Prime. Aug. 2020. Challenges for the evaluation of digital health solutions—A call for innovative evidence generation approaches. *NPJ Digit. Med.*, 3(1): 110, doi: 10.1038/s41746-020-00314-2.

[90] Oliva, A., S. Grassi, G. Vetrugno, R. Rossi, G. Della Morte, V. Pinchi and M. Caputo. 2022. Management of medico-legal risks in digital health era: A scoping review. *Frontiers in Medicine*, 8: 821756.

[91] Amankona, V., A. Asante, M. Opoku, P. Ohemeng-Gyaase, C. Srekumah, A. K. Peprah and P. Amankwa-Danquah. Dec. 2021. Integrating privacy-by-design in e-Health. In *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1–7). IEEE.

[92] Winter, J. S. and E. Davidson. Jun. 2022. Harmonizing regulatory regimes for the governance of patient-generated health data. *Telecomm Policy*, 46(5): 102285, doi: 10.1016/j.telpol.2021.102285.

[93] Bhuiyan, M. N., M. M. Rahman, M. M. Billah and D. Saha. Jul. 2021. Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet Things J.*, 8(13): 10474–10498, doi: 10.1109/JIOT.2021.3062630.

[94] Butpheng, C., K. -H. Yeh and H. Xiong. Jul. 2020. Security and privacy in IoT-cloud-based E-health systems—A comprehensive review. *Symmetry (Basel)*, 12(7): 1191, doi: 10.3390/sym12071191.

[95] Manteghinejad, A. and S. H. Javanmard. Jan. 2021. Challenges and opportunities of digital health in a post-COVID19 world. *Journal of Research in Medical Sciences*, 26(1): 11, doi: 10.4103/jrms.JRMS_1255_20.

[96] Hovenga, E., H. Grain and T. Beale. 2022. Fragmented global standards development organisations. In *Roadmap to Successful Digital Health Ecosystems*, Elsevier, pp. 65–96. doi: 10.1016/B978-0-12-823413-6.00025-2.

[97] Brass, I., L. Tanczer, M. Carr, M. Elsden and J. Blackstock. 2018. Standardising a moving target: The development and evolution of IoT security standards. In *Living in the Internet of Things: Cybersecurity of the IoT—2018*, Institution of Engineering and Technology, pp. 24 (9 pp.)–24 (9 pp.). doi: 10.1049/cp.2018.0024.

[98] Aly, M., F. Khomh, Y. -G. Guéhéneuc, H. Washizaki and S. Yacout. 2018. Is fragmentation a threat to the success of the Internet of Things? *IEEE Internet Things J.*, 6(1): 472–487.

[99] Karunarathne, S. M., N. Saxena and M. K. Khan. Jul. 2021. Security and privacy in IoT smart healthcare. *IEEE Internet Comput.*, 25(4): 37–48, doi: 10.1109/MIC.2021.3051675.

[100] Thilakarathne, N. N., M. K. Kagita and T. R. Gadekallu. 2020. The role of the Internet of Things in health care: A systematic and comprehensive study. *SSRN Electronic Journal*, doi: 10.2139/ssrn.3690815.

[101] Brewer, L. C., K. L. Fortuna, C. Jones, R. Walker, S. N. Hayes, C. A. Patten and L. A. Cooper. 2020. Back to the future: Achieving health equity through health informatics and digital health. *JMIR mHealth and uHealth*, 8(1): e14512.

[102] Sheikh, A., M. Anderson, S. Albala, B. Casadei, B. D. Franklin, M. Richards, D. Taylor, H. Tibble and E. Mossialos. 2021. Health information technology and digital innovation for national learning health and care systems. *The Lancet Digital Health*, 3(6): e383–e396.

[103] Wang, Q., M. Su, M. Zhang and R. Li. Jun. 2021. Integrating digital technologies and public health to fight Covid-19 pandemic: Key technologies, applications, challenges and outlook of digital healthcare. *Int. J. Environ. Res. Public Health*, 18(11): 6053, doi: 10.3390/ijerph18116053.

[104] Trocin, C., P. Mikalef, Z. Papamitsiou and K. Conboy. Dec. 2023. Responsible AI for digital health: A synthesis and a research agenda. *Information Systems Frontiers*, 25(6): 2139–2157, doi: 10.1007/s10796-021-10146-4.

[105] Salim Omambia Matagi and Satoshi Kaneko. Jan. 2023. Challenges and opportunities on data protection and privacy in healthcare. *International Journal of Scientific Research Updates*, 5(1): 023–041, doi: 10.53430/ijsru.2023.5.1.0001.

[106] Surridge, M., K. Meacham, J. Papay, S. C. Phillips, J. B. Pickering, A. Shafiee and T. Wilkinson. Oct. 2019. Modelling compliance threats and security analysis of cross border health data exchange. In *International Conference on Model and Data Engineering* (pp. 180–189). Cham: Springer International Publishing.

[107] Sommer, A., C. Rehbock, C. Vos, C. Borgs, S. Chevalier, S. Doreleijers, M. Gontariuk, S. Hennau, E. Pilot, H. Schröder, L. d. A. Auwermeulen, A. Ghuysen, S. K. Beckers and T. Krafft. 2022. Impacts and lessons learned of the first three COVID-19 waves on cross-border collaboration in the field of emergency medical services and Interhospital transports in the Euregio-Meuse-Rhine: A qualitative review of expert opinions. *Frontiers in Public Health*, 10: 841013.

[108] van der Molen, I. N. and M. J. Commers. Nov. 2013. Unresolved legal questions in cross-border health care in Europe: Liability and data protection. *Public Health*, 127(11): 987–993, doi: 10.1016/j.puhe.2013.08.020.

[109] Andanda, P. and L. Mlotshwa. Oct. 2024. Streamlining the ethical-legal governance of cross-border health data sharing during global health emergencies. *Res Ethics*, 20(4): 812–834, doi: 10.1177/17470161241261907.

[110] Gavrilov, G., E. Vlahu-Gjorgievska and V. Trajkovik. Jun. 2020. Healthcare data warehouse system supporting cross-border interoperability. *Health Informatics J.*, 26(2): 1321–1332, doi: 10.1177/1460458219876793.

[111] Gupta, D. S., N. Mazumdar, A. Nag and J. P. Singh. May, 2023. Secure data authentication and access control protocol for industrial healthcare system. *J. Ambient Intell. Humaniz. Comput.*, 14(5): 4853–4864, doi: 10.1007/s12652-022-04370-2.

[112] Ami, O., Y. Elovici and D. Hendler. Apr. 2018. Ransomware prevention using application authentication-based file access control. *Proceedings of the ACM Symposium on Applied Computing*, pp. 1610–1619, doi: 10.1145/3167132.3167304.

[113] Liu, Y., F. Ju, Q. Zhang, M. Zhang, Z. Ma, M. Li, A. Yang and F. Liu. 2023. Overview of internet of medical things security based on blockchain access control. *Journal of Database Management (JDM)*, 34(3): 1–20.

[114] Mahajan, R., S. Chavan, D. A. Ajalkar, B. S. V. and P. A. Khadkikar. Nov. 2023. A secure authentication protocol for healthcare service in IoT with Q-net based secret key generation. *Web Intelligence*, 21(4): 407–433, doi: 10.3233/WEB-220104.

[115] Ahmed, T., S. Samima, M. Zuhair, H. Ghayvat, M. A. Khan and N. Kumar. Apr. 2023. FIMBISAE: A multimodal biometric secured data access framework for Internet of Medical Things ecosystem. *IEEE Internet Things J.*, 10(7): 6259–6270, doi: 10.1109/JIOT.2022.3225518.

[116] Mahajan, R., S. Chavan, D. A. Ajalkar, B. S. V. and P. A. Khadkikar. Nov. 2023. A secure authentication protocol for healthcare service in IoT with Q-net based secret key generation. *Web Intelligence*, 21(4): 407–433, doi: 10.3233/WEB-220104.

[117] Riya, K. S., R. Surendran, C. Andr Tavera Romero and M. Sadish Sendil. 2023. Encryption with user authentication model for Internet of Medical Things environment. *Intelligent Automation & Soft Computing*, 35(1): 507–520, doi: 10.32604/iasc.2023.027779.

[118] Kok, S., A. Abdullah, N. Jhanjhi and M. Supramaniam. Nov. 2019. Prevention of crypto-ransomware using a pre-encryption detection algorithm. *Computers*, 8(4): 79, doi: 10.3390/computers8040079.

[119] K P, B. M., K. S. K and N. Patwari. Apr. 2023. Embedded light-weight cryptography technique to preserve privacy of healthcare wearable IoT device data. In *2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, IEEE, pp. 1–6. doi: 10.1109/ICDCECE57866.2023.10151002.

[120] Tsantikidou, K. and N. Sklavos. Jun. 2023. Minimal resource required E-health system with end-to-end authenticated encryption mechanism. In *2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, IEEE, pp. 1–4. doi: 10.1109/MOCAST57943.2023.10176534.

[121] Dhivya, R., M. Kumar S, M. J, V. Thanikaiselvan, H. Mahalingam and R. Amirtharajan. 2023. Secure health data transmission on IOT. In *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*, IEEE, pp. 1–4. doi: 10.1109/ViTECoN58111.2023.10156896.

[122] Jana, A. and G. Paul. Nov. 2022. Differential fault attack on PHOTON-Beetle. In *Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security*, New York, NY, USA: ACM, pp. 25–34. doi: 10.1145/3560834.3563824.

[123] Buchanan, W. J. and L. Maglaras. Jun. 2023. Review of the NIST light-weight cryptography finalists. In *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, IEEE, pp. 469–474. doi: 10.1109/DCOSS-IoT58021.2023.00079.

[124] Liu, S., L. Xin, X. Lyu and C. Ren. Mar. 2023. Masking-enabled data protection approach for accurate split learning. In *2023 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, pp. 1–6. doi: 10.1109/WCNC55385.2023.10118971.

[125] Satra, S., P. K. Sadhu, V. P. Yanambaka and A. Abdelgawad. Apr. 2023. Octopus: A novel approach for health data masking and retrieving using physical unclonable functions and machine learning. *Sensors*, 23(8): 4082, doi: 10.3390/s23084082.

[126] Shirgur, P. and S. Chaurasia. Jan. 2023. Development of secure IoT ecosystems for healthcare. In *2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, IEEE, pp. 1–6. doi: 10.1109/ICCT56969.2023.10076119.

[127] Krishna, T. B. M., S. P. Praveen, S. Ahmed and P. N. Srinivasu. May 2023. Software-driven secure framework for mobile healthcare applications in IoMT. *Intelligent Decision Technologies*, 17(2): 377–393, doi: 10.3233/IDT-220132.

[128] Potorochina, K. L. and E. Yu. Nikitina. 2022. Security of IoT applications in health care. *Вестник Пермского университета. Математика. Механика. Информатика*, 4(59): 68–81, doi: 10.17072/1993-0550-2022-4-68-81.

[129] Barapatre, P., Y. Ingolikar, P. Desai, P. Jajoo and P. Thakre. Dec. 2022. A secured architecture for IoT-based healthcare system. *3C Empresa. Investigación y pensamiento crítico*, 11(02): 222–230, doi: 10.17993/3cemp.2022.110250.222-230.

[130] Silvestri, S., S. Islam, S. Papastergiou, C. Tzagkarakis and M. Ciampi. Jan. 2023. A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem. *Sensors*, 23(2): 651, doi: 10.3390/s23020651.

[131] Alzahrani, F. A., M. Ahmad and M. T. J. Ansari. Aug. 2022. Towards design and development of security assessment framework for Internet of Medical Things. *Applied Sciences*, 12(16): 8148, doi: 10.3390/app12168148.

[132] Al Ali, A., O. Al-Blooshi, R. Al Ali and H. Al Hamadi. Jun. 2024. Securing the Internet of Things (IoT) application: Best practices and challenges in IoT software. In *2024 Advances in Science and Engineering Technology International Conferences (ASET)*, IEEE, pp. 1–7. doi: 10.1109/ASET60340.2024.10708648.

[133] Natarajan, R., G. H. Lokesh, F. Flammini, A. Premkumar, V. K. Venkatesan and S. K. Gupta. Feb. 2023. A novel framework on security and energy enhancement based on Internet of Medical Things for healthcare 5.0. *Infrastructures (Basel)*, 8(2): 22, doi: 10.3390/infrastructures8020022.

[134] Balasamy, K., N. Krishnaraj, J. Ramprasath and P. Ramprakash. 2022. A secure framework for protecting clinical data in medical IoT environment. In *Smart Healthcare System Design*, Wiley, pp. 203–234. doi: 10.1002/9781119792253.ch9.

[135] Gaba, G. S., M. Hedabou, P. Kumar, A. Braeken, M. Liyanage and M. Alazab. May 2022. Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare. *Sustain Cities Soc.*, 80: 103766, doi: 10.1016/j.scs.2022.103766.

[136] Kakvi, S. A., K. M. Martin, C. Putman and E. A. Quaglia. 2023. SoK: Anonymous Credentials, pp. 129–151. doi: 10.1007/978-3-031-30731-7_6.

[137] Junior, A. S. C. and C. H. Arima. Jan. 2023. Threat modeling: A study on its application in digital transformation from the perspective of risk. *Revista de Gestão e Secretariado*, 14(1): 1158–1169, doi: 10.7769/gesec.v14i1.1581.

[138] Tomashchuk, O. Oct. 2020. Threat and risk management framework for eHealth IoT applications. In *Proceedings of the 24th ACM International Systems and Software Product Line Conference - Volume B*, New York, NY, USA: ACM, pp. 120–126. doi: 10.1145/3382026.3431250.

[139] Salih, F. I., N. A. Abu Bakar, N. H. Hassan, F. Yahya, N. Kama and J. Shah. Dec. 2019. IoT security risk management model for healthcare industry. *Malaysian Journal of Computer Science*, pp. 131–144, doi: 10.22452/mjcs.sp2019no3.9.

[140] Yeng, P. K. S. D. and B. Yang. 2020. Comparative analysis of threat modeling methods for cloud computing towards healthcare security practice. *International Journal of Advanced Computer Science and Applications*, 11(11), doi: 10.14569/IJACSA.2020.0111194.

[141] Kwarteng, E. and M. Cebe. Jun. 2024. MEDICALHARM: A threat modeling designed for modern medical devices and a comprehensive study on effectiveness, user satisfaction, and security perspectives. *Int. J. Inf. Secur.*, 23(3): 2225–2268, doi: 10.1007/s10207-024-00826-y.

[142] Kandasamy, K., S. Srinivas, K. Achuthan and V. P. Rangan. Dec. 2020. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.*, 2020(1): 8, doi: 10.1186/s13635-020-00111-0.

[143] Salami, A. A., U. T. I. Igwenagu, C. E. Mesode, O. O. Olaniyi and O. B. Oladoyinbo. Apr. 2024. Beyond conventional threat defense: Implementing advanced threat modeling techniques, risk modeling frameworks and contingency planning in the healthcare sector for enhanced data security. *Journal of Engineering Research and Reports*, 26(5): 304–323, doi: 10.9734/jerr/2024/v26i51156.

[144] Saurabh, K., D. Gajjala, K. Kaipa, R. Vyas, O. P. Vyas and R. Khondoker. Sep. 2024. TMAP: A Threat Modeling and Attack Path analysis framework for industrial IoT systems (A case study of IoM and IoP. *Arab. J. Sci. Eng.*, 49(9): 13163–13183, doi: 10.1007/s13369-023-08600-3.

[145] Christogianni, A. 2024. The Benefits of Continuous Health Data Monitoring in Cardiovascular Diseases and Dementia, pp. 1–22. doi: 10.4018/978-1-6684-7366-5.ch014.

[146] Gilbert, S., A. Pimenta, A. Stratton-Powell, C. Welzel and T. Melvin. Sep. 2023. Continuous improvement of digital health applications linked to real-world performance monitoring: Safe moving targets? *Mayo Clinic Proceedings: Digital Health*, 1(3): 276–287, doi: 10.1016/j.mcpdig.2023.05.010.

[147] Adaros-Boye, C., P. Kearney and M. Josephs. 2020. Continuous Risk Management for Industrial IoT: A Methodological View, pp. 34–49. doi: 10.1007/978-3-030-41568-6_3.

[148] Kott, A. and C. Arnold. Jan. 2013. The promises and challenges of continuous monitoring and risk scoring. *IEEE Secur. Priv.*, 11(1): 90–93, doi: 10.1109/MSP.2013.19.

[149] Caballero, M., D. Kavallieros, A. Spyros, A. Tavernarakisv, A. Tziouvaras, S. Bonacina, K. Chandrarmouli, M. Coroiu, L. Chen, T. Dounia, I. Giannoulakis, N. Gligoric, E. Kafetzakis, T. Kasig, V. Koumaras, T. Krousarlis, K. Lapidaki, A. Markakis, S. Marin, M. Manulis, S. Menesidou, S. Nifakos, L. Meng, S. Mhiri, M. Nati, K. Ntafloukas, D. Oniga, D. Papamartzivanos, S. Papastergiou, K. Sanchez, C. Sakkas, K. Stelliou, L. Trujillo, T. Tsikrika, E. Venegas, S. Vrochidis and D. Xydias. 2022. ICT in Healthcare: The role of IoT and the SECANT solution. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR), IEEE*, pp. 104–111.

[150] Chakraborty, C., S. M. Nagarajan, G. G. Devarajan, T. V. Ramana and R. Mohanty. May 2023. Intelligent AI-based healthcare cyber security system using multi-source transfer learning method. *ACM Trans. Sens. Netw.*, doi: 10.1145/3597210.

[151] Al-Hawawreh, M., N. Moustafa and J. Slay. Jan. 2024. A threat intelligence framework for protecting smart satellite-based healthcare networks. *Neural Comput. Appl.*, 36(1): 15–35, doi: 10.1007/s00521-021-06441-5.

[152] Wagner, T. D., K. Mahbub, E. Palomar and A. E. Abdallah. Nov. 2019. Cyber threat intelligence sharing: Survey and research directions. *Comput. Secur.*, 87: 101589, doi: 10.1016/j.cose.2019.101589.

[153] Sarker, I. H., A. I. Khan, Y. B. Abushark and F. Alsolami. Feb. 2023. Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, 28(1): 296–312, doi: 10.1007/s11036-022-01937-3.

[154] Jesus, V., B. Bains and V. Chang. 2024. Sharing is caring: Hurdles and prospects of open, crowd-sourced cyber threat intelligence. *IEEE Trans. Eng. Manag.*, 71: 6854–6873, doi: 10.1109/TEM.2023.3279274.

[155] Jin, B., E. Kim, H. Lee, E. Bertino, D. Kim and H. Kim. 2024. Sharing cyber threat intelligence: Does it really help? In *Proceedings 2024 Network and Distributed System Security Symposium*, Reston, VA: Internet Society. doi: 10.14722/ndss.2024.24228.

[156] Mabodi, K., M. Yusefi, S. Zandiyan, L. Irankhah and R. Fotohi. Sep. 2020. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. *J. Supercomput.*, 76(9): 7081–7106, doi: 10.1007/s11227-019-03137-5.

[157] Hasan, M. K., T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. A. Eshmawi, S. Abdel-Khalek and H. M. Alkhassawneh. 2022. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Communications*, 16(5): 421–432.

[158] Gutfleisch, M., M. Schöps, J. Hielscher, M. Cheney, S. Sayin, N. Schuhmacher, M. Ali and M. A. Sasse. Sep. 2022. Caring about iot-security–An interview study in the healthcare sector. In *Proceedings of the 2022 European Symposium on Usable Security*, pp. 202–215.

[159] Ksibi, S., F. Jaidi and A. Bouhoula. Jun. 2023. IoMT security model based on machine learning and risk assessment techniques. In *2023 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, pp. 614–619. doi: 10.1109/IWCMC58020.2023.10182654.

[160] Ramzan, T. and S. Zafar. Dec. 2022. Blockchain-based security for Internet of Medical Things Application. In *2022 International Conference on Cyber Warfare and Security (ICCWS)*, IEEE, pp. 69–74. doi: 10.1109/ICCWS56285.2022.9998443.

[161] Zuo, Z., M. Watson, D. Budgen, R. Hall, C. Kennelly and N. Al Moubayed. Oct. 2021. Data anonymization for pervasive health care: Systematic literature mapping study. *JMIR Med. Inform.*, 9(10): e29871, doi: 10.2196/29871.

[162] Kwok, C. S., E. -A. Muntean, C. D. Mallen and J. A. Borovac. Oct. 2022. Data collection theory in healthcare research: The minimum dataset in quantitative studies. *Clin. Pract.*, 12(6): 832–844, doi: 10.3390/clinpract12060088.

[163] Akkaya, F. D. 2023. HES: A case study on cybersecurity and privacy risks in health surveillance systems. *In*: Adedoyin, F. F. and B. Christiansen (eds.). *Effective Cybersecurity Operations for Enterprise-Wide Systems*, IGI Global, pp. 123–146. doi: 10.4018/978-1-6684-9018-1.ch006.

[164] Kayes, A. S. M., M. Hammoudeh, S. Badsha, P. A. Watters, A. Ng, F. Mohammed and M. Islam. Feb. 2020. Responsibility attribution against data breaches. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 498–503). IEEE.

[165] Kan, E. May 2024. Empowering patients through transparent access to personal health data. *International Journal of Law and Policy*, 2(5): 37–41, doi: 10.59022/ijlp.188.

[166] Goel, P. K. 2024. Ethical Considerations in Implementing Artificial Intelligence in Cybersecurity, pp. 72–91. doi: 10.4018/979-8-3693-6517-5.ch005.

[167] Wambua, R. N. Jul. 2024. A systematic literature review of digital health strategies for equitable access to universal health coverage in developing countries. *Journal of Science, Innovation and Creativity*, 3(1): 11–21, doi: 10.58721/jsic.v3i1.647.

[168] Idoko, B., J. A. Alakwe, O. J. Ugwu, J. E. Idoko, F. O. Idoko, V. B. Ayoola, E. V. Ejembi and T. Adeyinka. 2024. Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria. *Magna Scientia Advanced Research and Reviews*, 11(02): 151–167.

[169] Lorenzini, G., D. M. Shaw and B. S. Elger. Dec. 2022. It takes a pirate to know one: Ethical hackers for healthcare cybersecurity. *BMC Med Ethics*, 23(1): 131, doi: 10.1186/s12910-022-00872-y.

[170] He, Y., E. Zamani, I. Yevseyeva and C. Luo. Apr. 2023. Artificial intelligence–based ethical hacking for health information systems: Simulation study. *J. Med. Internet Res.*, 25: e41748, doi: 10.2196/41748.

[171] Pyrrho, M., L. Cambraia and V. F. de Vasconcelos. Jul. 2022. Privacy and health practices in the digital age. *The American Journal of Bioethics*, 22(7): 50–59, doi: 10.1080/15265161.2022.2040648.

[172] Smys, S. and J. S. Raj. Feb. 2022. Future challenges of the Internet of Things in the health care domain—An overview. *Journal of Trends in Computer Science and Smart Technology*, 3(4): 274–286, doi: 10.36548/jtcsst.2021.4.003.

[173] Shafi, M. and R. Kumar Jha. 2022. Recent security issues and countermeasures on IoHT. In *Smart and Secure Internet of Healthcare Things*, Boca Raton: CRC Press, pp. 127–136. doi: 10.1201/9781003239895-8.

[174] Bahalul Haque, A. K. M., B. Bhushan, A. Nawar, K. R. Talha and S. J. Ayesha. 2022. Attacks and Countermeasures in IoT Based Smart Healthcare Applications, pp. 67–90. doi: 10.1007/978-3-030-90119-6_6.

[175] Bhushan, B., A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya and A. Kumar. Apr. 2023. Towards a secure and sustainable Internet of Medical Things (IoMT): Requirements, design challenges, security techniques, and future trends. *Sustainability*, 15(7): 6177, doi: 10.3390/su15076177.

[176] Alkatheiri, M. S. and A. S. Alghamdi. Apr. 2023. Blockchain-assisted cybersecurity for the Internet of Medical Things in the healthcare industry. *Electronics (Basel)*, 12(8): 1801, doi: 10.3390/electronics12081801.

[177] Villegas-Ch, W., J. García-Ortiz and I. Urbina-Camacho. May 2023. Framework for a secure and sustainable internet of medical things, requirements, design challenges, and future trends. *Applied Sciences*, 13(11): 6634, doi: 10.3390/app13116634.

[178] Aldhyani, T. H. H., M. A. Khan, M. A. Almaiah, N. Alnazzawi, A. K. A. Hwaitat, A. Elhag, R. T. Shehab and A. S. Alshebami. 2023. A secure internet of medical things framework for breast cancer detection in sustainable smart cities. *Electronics*, 12(4): 858.

[179] Badawy, M. Jan. 2023. Sustainable secure Internet of Things (SS-IoT). In *2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)*, IEEE, pp. 1–6. doi: 10.1109/ICAISC56366.2023.10085280.

[180] Maina,A. M. and U. G. Singh. Sep. 2022. Rebuilding stakeholder confidence in health-relevant big data applications: A social representations perspective. *Information*, 13(9): 441, doi: 10.3390/info13090441.

[181] Landers, C., E. Vayena, J. Amann and A. Blasimme. Feb. 2023. Stuck in translation: Stakeholder perspectives on impediments to responsible digital health. *Front. Digit. Health*, 5, doi: 10.3389/fdgth.2023.1069410.

[182] Iakovleva, T., E. Oftedal and J. Bessant. 2021. Changing role of users—innovating responsibly in digital health. *Sustainability*, 13(4): 1616.

[183] Nipa, N. S., M. Alam and M. S. Haque. 2021. Identifying Relevant Stakeholders in Digital Healthcare, pp. 349–357. doi: 10.1007/978-3-030-82269-9_27.