Chapter 12

Artificial Intelligence, Privacy, Governance, and Ethics for the Internet of Healthcare Things

Md. Hasanul Ferdaus,[1,*] *Fares Alharbi*,[2] *Mohammad Rifat Ahmmad Rashid*,[1] *Md. Mostofa Kamal Rasel*,[1] *Taskeed Jabid*,[1] *Md. Sawkat Ali*,[1] *Mohammad Manzurul Islam*,[1] *Maheen Islam*[1] and *Rajkumar Buyya*[3]

1. Introduction

The Internet of Health Things (IoHT) is a subset of the broader technological revolution termed the Internet of Things (IoT). It has brought forth a crucial evolution in healthcare technology. The IoHT technologies are transforming the landscape of medical services, including patient care, healthcare operations, and medical data management, by combining physical and digital components within medical environments [1]. Advanced technologies such as smart sensors, complex data analytics,

[1] Department of Computer Science and Engineering, East West University, Dhaka, Bangladesh.
[2] Department of Computer Science, College of Computing and IT, Shaqra University, Shaqra, Saudi Arabia.
[3] School of Computing and Information Systems, The University of Melbourne, Melbourne, Australia.
Emails: faalhrbi@su.edu.sa, rifat.rashid@ewubd.edu, mostofa.kamal@ewubd.edu, taskeed@ewubd.edu, alim@ewubd.edu, mohammad.islam@ewubd.edu, maheen@ewubd.edu, rbuyya@unimelb.edu.au
* Corresponding author: hasanul.ferdaus@ewubd.edu

efficient machine learning and deep learning algorithms, cloud computing, and networking infrastructures have been integrated to form the IoHT ecosystem that fosters remote and real-time health monitoring, enhances medical outcomes, and improves the efficiency of healthcare services significantly.

1.1 Evolution of IoHT Technologies

IoHT technologies have undergone rapid development within the last two decades. While at the initial stage, IoHT focused primarily on simple health data collection and patient condition monitoring technologies, recent improvements of IoHT expanded the scope profoundly including online patient diagnostics, advanced predictive analytics, and advice on personalized medicine. Modern sophisticated developments such as wearable medical devices and smart hospital beds have enabled healthcare professionals to access critical health information in real time, as well as increased patient engagement and comfort. Innovations in smart sensor developments, wireless communications, artificial intelligence (AI), and cloud technologies continue to drive further the evolution of IoHT technologies as delineated in research studies [2] and [3].

1.2 Importance of Cybersecurity

Cybersecurity has appeared as a great concern for IoHT given the rapid and comprehensive expansion of the IoHT technologies. The various components and devices of the IoHT ecosystem are highly interconnected which can expose them to a wide range of cyber threats, from data breaches and malware to phishing attacks and ransomware attacks [4]. As a consequence, protecting sensitive health information holds paramount significance and calls for the implementation of robust security measures. Confidential patient information can be effectively safeguarded by employing robust encryption techniques, secure device authentication, and regular software updates. Confidentiality and integrity of sensitive health information can be ensured through ongoing vigilance and effective response to emerging security threats, as duly emphasized by the researchers in [5].

1.3 Regulatory Frameworks

Regulatory bodies and frameworks play a crucial role in shaping the development, implementation, application, and scope of the IoHT technologies. Safety and confidentiality of healthcare devices are primarily guaranteed by the guidelines from the regulatory frameworks, which ultimately protect individuals and their information in the IoHT

ecosystem. Examples of such frameworks include the General Data Protection Regulation (GDPR) effective within the territories of the European Union and the Health Insurance Portability and Accountability Act (HIPAA) within the United States which offer regulations for data confidentiality and protection within the healthcare sector [2]. Such authoritative bodies continue to evolve in response to the transformations and associated challenges posed by the IoHT ecosystem balancing the overall patient welfare and confidentiality and privacy of health data [3].

2. The Convergence of AI and IoHT

The convergence of AI and the Internet of Healthcare Things (IoHT) has made a revolutionary transformation in the healthcare services area as they help achieve extraordinary innovations and improve both the efficiency and quality of the healthcare sector. Healthcare providers can now provide higher levels of tailored and proactive treatments by leveraging AI's sophisticated data-processing capabilities in parallel with the connectivity of smart IoHT devices. Such integration of technologies expedites clinical operations and boosts patient care with the help of continuous monitoring facilities and predictive intelligence. With the continuous development of AI and IoHT, they have emerged as extremely effective tools to address critical healthcare challenges collectively, such as controlling chronic diseases and maximizing resource allocation [6]. Notwithstanding the obvious benefits, such technological convergence also introduces potential challenges in interoperability, security, and ethical issues that must be addressed appropriately to leverage the utmost potential of these technologies in improving patient experience and operational performance. Figure 1 illustrates the integration of AI with the IoHT.

2.1 AI-driven Healthcare Transformation

In the field of healthcare, the integration of AI and IoHT devices transforms patient care by improving accuracy in medical diagnosis, personalizing treatment, and enhancing patient outcomes. This AI-driven transformation is extremely crucial for the transformation from traditional reactive medical practices to proactive healthcare management.

2.1.1 Securing AI Models and Data

Implementing robust cybersecurity measures is paramount to securing the AI models and the vast amounts of data they process so that data breaches can be prevented effectively and patient privacy can be guaranteed [7]. This can be achieved through the utilization of encryption of data

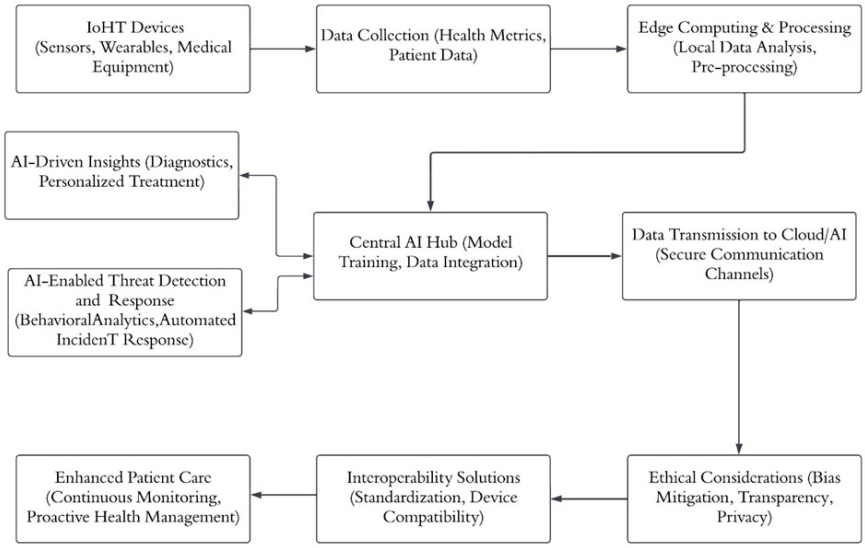

Figure 1: The convergence of AI and IoHT.

transfers, secure storage practices, and regular security audits that would help identify and mitigate potential vulnerabilities.

2.1.2 Ethical Considerations

The ethical repercussions of the use of AI in patient care are extremely crucial including concerns such as bias in AI algorithms, the transparency of decisions generated by AI tools, and the possibility of patient privacy violations [8]. In this context, appropriate guidelines and standards for the ethical use of AI must be formulated to ensure integrity and maintain trust in the overall healthcare system.

2.1.3 Interoperability Issues

Due to the use of different types of sensors and components and their applications, as well as different sources for data and data formats, interoperability issues among the various IoHT devices and healthcare systems continue to pose significant challenges that hamper the seamless integration of AI applications. Standardization of data formats, improved device compatibility, and enhanced collaborations among technology providers can play significant roles in alleviating interoperability and portability issues and ensuring cohesive healthcare ecosystems [9].

2.2 AI-enabled Threat Detection and Response

AI enhances the capabilities of IoHT by providing advanced tools for real-time threat detection and response, thus safeguarding healthcare networks from various cyber threats and ensuring continuous patient care.

2.2.1 Behavioral Analytics

Anomalous behaviors that may indicate potential security threats can be detected by AI-driven behavioral analytics that effectively utilize pattern recognition and machine learning. AI-enabled tools can be used for analyzing typical user interactions with IoHT devices and can effectively identify deviations suggesting unauthorized access or malicious activities [10].

2.2.2 Automated Incident Response

With the help of AI tools, the present-day automated incident response systems can rapidly respond to any identified cyber threats reduce the overall damage, and contain security breaches more effectively. Such response systems are capable of initiating appropriate protocols spontaneously, such as isolating affected devices and notifying security personnel of the incidents. This helps the management by reducing the reliance on manual intervention and accelerating response times [11].

3. Privacy-Preserving Data Analytics

The advancement of privacy-preserving data analytics is now a requirement due to the proliferation of data-driven decision-making. This domain ensures the protection and security of confidential data and the extraction of valuable insights from the dataset at the same time. Table 1 provides a summary of the privacy-preserving techniques in Privacy-Preserving Data Analytics and highlights the key methods.

3.1 Anonymization Approaches

Anonymization is a technique that is used to safeguard from personal identification as individuals, while simultaneously maintaining integrity of data for analytical purposes. Several methods can be applied to achieve this goal:

3.1.1 Data Masking

Data masking is the process that obscures particular data elements within a database to guarantee that personal data items are incomprehensible. With this approach, data masking minimizes the possibility of data breaches [11]. Sensitive data, such as personal health information, credit

Table 1: Summary of privacy-preserving data analytics techniques.

Areas	Method	Description	Reference
Anonymization Approaches	Data Masking	Obscures specific data elements within a database to make personal data incomprehensible.	[11]
	Pseudonymization	Replaces identifying fields with artificial identifiers, making reversal possible under certain conditions.	[11]
	Generalization	Reduces precision of data (e.g., replacing exact age with age range) to protect identities.	[12]
	Differential Privacy	Adds randomness to data so that the inclusion/exclusion of a single item does not significantly affect query outcomes.	[13]
Multi-Party Computation Security	Secure Protocols	Uses cryptographic techniques like secret sharing and zero-knowledge proofs to protect data during computation.	[14]
	Garbled Circuits	A secure two-party computation method where one party creates a "garbled" circuit and the other evaluates it with encrypted inputs.	[15]
	Oblivious Transfer	Ensures a sender transfers one piece of information to a receiver without knowing which piece was transferred.	[16]

card information, and social security numbers, are usually protected using data masking techniques.

3.1.2 Pseudonymization

Pseudonymization is another technique that substitutes identifying fields within a data record having one or more artificial identifiers or pseudonyms, thus minimizing the probability of the dataset with the original identity of individuals [11]. However, within certain conditions, the pseudonymization process can be reversed which is unlike anonymization.

3.1.3 Generalization

Generalization is an approach that reduces the precision for a range of data that facilitates individuals' identity protection while enabling data analysis on broader trends. Examples of such generalization techniques could be replacing precise attributes such as zip code or exact age with

larger categories such as age groups or the first few digits of zip codes [12].

3.1.4 Differential Privacy

Differential privacy injects randomness into the data in such a way that the results of queries do not affect significantly if a single database item in included or excluded [13]. This approach ensures strong privacy and it is extremely effective in statistical databases in particular where aggregate data are shared.

3.2 Multi-Party Computation Security

Multi-party computation (MPC) is a process where several entities can compute a function using their inputs in a collaborative fashion where it is guaranteed that the inputs remain confidential. In scenarios where sharing raw data is not practical due to concerns over data privacy or business competition, MPC has proved to be an effective solution for privacy-preserving data analytics.

3.2.1 Secure Protocols

These protocols utilize cryptographic methods such as secret sharing, zero-knowledge proofs, and homomorphic encryption to verify the correctness of computation outputs without revealing any additional information. Such protocols make use of cryptographic techniques and algorithms such as zero-knowledge proofs, secret sharing, and homomorphic encryption so that the computation outputs are correct without revealing any further information [14].

3.2.2 Garbled Circuits

Another technique used to secure two-party computation is the Garbled circuit. In this approach, one party creates a "garbled" version of a circuit, and the other party assesses the circuit using encrypted inputs. It guarantees that the assessor learns nothing except the outcome [15].

3.2.3 Oblivious Transfer

One of the fundamental protocols in MPC is the Oblivious Transfer. It allows a sender to transfer one of potentially many pieces of information to a receiver; however, the sender stays unaware of the exact piece that was transferred. For many different MPC protocols, the Oblivious Transfer is a crucial component, particularly in the execution of garbled circuits [16].

3.2.4 Implementation Challenges

There are several hurdles in the effective implementation of MPC in the context of practical scenarios such as computational overheads, intricacies

of protocol design, and network latency. Authors in [15] have presented several recent advancements in this field that aim at optimizing these aspects to make MPC viable for real-world use cases.

4. Threat Landscape and Vulnerability Assessment

4.1 Understanding IoHT Cyber Threats

The IoHT utilizes a diverse array of medical devices and applications that connect to healthcare networks and offer critical data and functionalities. As a consequence, IoHT-enabled healthcare systems are exposed to various cyber threats. To understand these potential threats, it is very important to identify and analyze potential vulnerabilities in IoHT devices such as medical wearables, implanted medical devices, and even hospital infrastructure systems, that cybercriminals may exploit [17]. The most common types of threats in healthcare are data breaches that compromise patient confidentiality, ransomware attacks that block access to critical systems, and DoS and DDoS attacks that disrupt service availability [18]. The heterogeneity and complexity of IoHT devices, as well as their integration with legacy systems extend the cyberattack surface making it crucial to identify and understand these threats thoroughly.

4.2 Vulnerability Assessment Techniques

For the purpose of vulnerability assessment in IoHT, security weaknesses are identified in systematic methods across the network of connected medical devices. Such techniques include the following:

- **Automated Scanning Tools:** These tools are used to scan systems and networks in an automated way to identify common and known security vulnerabilities. Such automated scanning tools are quite helpful in providing insights into potential security gaps within the infrastructure [19].
- **Penetration Testing:** Simulated cyberattacks are carried out to understand how an intruder could gain unauthorized access to the IoHT systems and networks [20].
- **Risk Analysis:** In this approach, the potential impacts and likelihood of threats are evaluated. Through such analysis, security experts can prioritize the vulnerabilities based on their impact and potential to cause harm [20].
- **Compliance Audits:** Regular audits are conducted to ensure that IoHT practices align with industry standards and regulations, such as the HIPAA in the U.S. These audits are helpful in detecting non-compliance issues and the associated vulnerabilities [21].

4.3 Continuous Monitoring and Incident Response

Continuous monitoring of IoHT systems is an extremely effective technique for early detection of unusual activities that could signal a potential cyberattack. Sophisticated monitoring tools can be implemented and rolled out to capture and analyze data relating to application activity and network traffic with the objective of detecting anomalies and potential threats. Moreover, incident response mechanisms are equally important and must incorporate a planned approach for managing and recovering the services after any security incidents take place [22]. The following are the steps needed for proper incident response:

- **Incident Detection:** Modern and advanced threat detection systems must be utilized for comprehensive security.
- **Response Procedures:** Appropriate and standard response protocols must be established within the organization to contain and mitigate the impacts of cyberattacks.
- **Recovery Plans:** Proper recovery strategies must be devised well ahead for restoring information systems after any incident happens. This involves the elimination of any malicious threats, such as malware and ransomware, and strengthening the network against potential future attacks [23].
- **Post-Incident Analysis:** This involves reviewing and learning from any incident that took place within the infrastructure so that future security measures of the systems and networks can be improved.

4.4 User Awareness and Training

Human users are one of the most critical vulnerabilities in any security system. Regular training sessions and boosting user awareness of cybersecurity are essential parts of a comprehensive IoHT security strategy [24]. Such training sessions must cover the following aspects [25]:

- **Recognizing Phishing Attacks:** Users must be educated and trained regularly so that they can identify and avoid any potential phishing attempts, such as via phishing emails or phone calls, that could cause any unauthorized access to sensitive data and systems.
- **Secure Usage Practices:** Users must be trained on the appropriate use of IoHT devices. They should be educated on the significance of effective password management and maintaining regular updates.
- **Response to Suspected Security Breaches:** Proper measures should be taken to educate users on the instructions that they must follow in case they suspect a security breach.

5. Ethical Considerations in Cybersecurity for IoHT

Complex ethical challenges are arising due to the integration of the IoHT into medical practices. These ethical considerations must be addressed to safeguard patient rights and maintain trust in healthcare technologies [26]. In this section, key ethical issues concerning patient consent and data ownership, and the delicate balance between securing health information and ensuring its accessibility are delineated.

5.1 Patient Consent and Data Ownership

In the realm of healthcare and data privacy legislation, a fundamental principle is patient consent. In the specific domain of the IoHT, this consent involves providing informed consent by the patients. Healthcare service providers are supposed to provide their patients with clear and comprehensive information in regard to the acquisition, dissemination, utilization, and retention of their health-related data. Often patients face challenges in understanding the complex technical details and the potential extent of data utilization, in many cases due to the opaque nature of certain IoHT systems, which creates ethical dilemmas [27]. Therefore, it is imperative for the IoHT ecosystems to have provisions for upholding patient autonomy such that they ensure that patients' consent is fully informed and revocable under specific conditions.

The data ownership issues in the IoHT raise several concerns relating to the patient's rights. In particular, this raises questions about who has the right to access, control, and benefit from health data. Data custodians or controllers are defined as the appropriate data owners on the basis of the legal frameworks. However, when ethical considerations indicate that patients should have at least partial ownership of their data [28], such a shared ownership model helps patients to benefit from the use of their data. Furthermore, it also empowers patients to have opinions on its secondary uses, for example, in research or the development of new medical technologies [29, 30].

5.2 Balancing Security and Accessibility

In the domain of IoHT, there are significant ethical challenges in balancing the dual requirements of strong security and broad accessibility of health-related data [31]. On one hand, robust cybersecurity mechanisms must be enforced to protect sensitive health information from breaches so that privacy violations and potential harm can be minimized. On the other hand, it should be maintained that implementation of these security measures must not excessively limit access to health data, particularly in cases where access is vital for emergency services and standard patient care [32].

6. Regulatory Landscape and Compliance

The incorporation of the IoHT into the healthcare sector has brought forth numerous technological innovations. However, there are significant regulatory implications that arise with the use of technologies within the healthcare sector [33]. The remaining parts of this section explore key aspects of compliance with existing regulations such as HIPAA and GDPR, the need for international standards and harmonization, as well as the emerging regulatory trends.

6.1 HIPAA and GDPR Compliance

The Health Insurance Portability and Accountability Act, commonly known as HIPAA, is a regulation primarily applicable within the United States. It sets a standard for protecting sensitive patient information. According to HIPAA, every organization that handles protected health information (PHI) is obligated to ensure that all necessary physical, network, and procedural security measures are established and followed. As IoHT technologies are being integrated into the healthcare sector, this obligation is extending to the devices that collect, store, or transmit PHI [34]. Unlike HIPAA, the General Data Protection Regulation, commonly known as GDPR, addresses every organization that manages any personal information of individuals within the European Union. Its primary focus areas are on the consent and rights of the data subjects, as well as the regulation of cross-border data transfers. Moreover, factors that can affect the deployment and management of IoHT devices, such as data minimization and restriction of data usage for specific purposes, are also covered within GDPR [35]. To comply with these regulations, organizations handling PHI need to conduct periodic risk assessments, employ necessary technological protections, and establish transparent communication with patients about their data rights and their use.

6.2 Emerging Regulatory Trends

The regulatory landscape is continuously evolving with the advancement of technologies. Increasing data privacy, improvement of security measures, and expansion of the definition of health data are among the principal emerging trends in regulation transformation. For instance, if some non-traditional data are collected from wearable devices and used for making health-related decisions, it may be put under regulatory scrutiny [36]. Moreover, regulators are paying more attention to the security of interconnected systems where IoHT devices interact with other medical and non-medical systems, potentially leading to the introduction of new guidelines addressing such scenarios. Furthermore, many

autonomous systems in IoHT environments leverage the strengths of machine learning and AI to make decisions. This is prompting regulators to devise mechanisms and procedures for auditing the process of making algorithmic decisions and formulate accountability mechanisms that are needed for such autonomous systems [37].

6.3 International Standards and Harmonization

Considering the global nature of technology and data transmission, it is highly important to formulate international standards and bring harmony within the IoHT regulations. Global organizations, such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), are exercising ongoing efforts with the objective of establishing regulations that ensure the safety, reliability, and interoperability of IoHT devices worldwide [38]. Ethical use of IoHT is also addressed by such harmonization endeavors so that devices adhere to both local legislations as well as comply with global human rights principles [35]. This aspect is especially important in scenarios where the operation of IoHT devices spans various regions and countries, each governed by its own regulatory framework.

7. Challenges and Future Directions

The IoHT is a continuously evolving sector in the healthcare landscape. As it is advancing, it is also encountering new challenges and opportunities while integrating more deeply into the healthcare ecosystem. Table 2 provides an overview of future directions and challenges in IoHT. The part of this section explores the future trajectory of IoHT in further detail focusing on integration with emerging technologies, the future of IoHT security, collaborative approaches to cybersecurity, the significance of regulatory compliance, and the role of research and innovation.

7.1 Integration with Emerging Technologies

As IoHT grows and matures over time, its integration with other emerging technologies, such as machine learning, AI, cloud computing, and blockchain, will be highly crucial. AI and machine learning can be leveraged further so that various IoHT devices can process and analyze health data more efficiently in real time. This can facilitate to enhance the accuracy of medical diagnostics and enable personalized treatment options. Moreover, cloud computing can be utilized to provide scalable and flexible storage and processing capabilities that enable real-time analysis and sharing of vast amounts of health data from various IoHT

Table 2: Future directions and challenges in IoHT.

Areas	Direction/Challenge	Focus
Integration with Emerging Technologies	AI and Machine Learning	Real-time data processing for enhanced diagnostics and treatment.
	Blockchain	Secure, decentralized data storage and sharing.
	Advanced Wireless Technologies (5G)	Improved communication speed and reliability between devices.
IoHT Security	Robust Encryption Methods	Stronger encryption to counter sophisticated cyber threats.
	Advanced Anomaly Detection Systems	AI-driven prediction and mitigation of security breaches.
	Unified Security Framework	Standardized security across various platforms and devices.
Collaborative Approaches to Cybersecurity	Common Security Standards	Effective cooperation through unified security standards.
	Industry-Wide Collaborations	Sharing best practices and threat intelligence among stakeholders.
Regulatory Compliance and Standards	Evolving Regulatory Frameworks	Continuous updates to regulations addressing IoHT challenges.
	Harmonization and International Standards	Global standards for international technology providers and healthcare services.
Research and Innovation	Technological Advancements	Innovations in battery life, miniaturization, and sensor accuracy.
	Impact Studies	Research on IoHT's effects on patient outcomes, privacy, and healthcare delivery.
	Social, Ethical, and Economic Research	Investigating the broader impacts of IoHT to address integration challenges.

devices. This can also improve remote access to healthcare services and patient data, thus enhancing telemedicine and supporting advanced data-driven decision-making in healthcare. Furthermore, the decentralized nature of blockchain architecture offers a promising solution to the privacy and security concerns in IoHT. This technology can be leveraged to provide a secure, decentralized platform for storing and sharing medical data. Additionally, the adoption and utilization of advanced wireless technologies, such as 5G (Fifth Generation Wireless Technology), Wi-Fi 6 (802.11ax), and LoRaWAN (Long Range Wide Area Network), can facilitate faster and more reliable communications between IoHT devices, thus enhance the capabilities and efficiency of IoHT applications.

7.2 Charting the Future of IoHT Security

With the expansion of the IoHT domain and its integration with other technologies, security concerns are also growing at a higher rate. As new devices and networks are being incorporated into the IoHT infrastructures, new threat actors and sophisticated cyber-attacks are emerging. As a result, future security strategies must be adjusted appropriately to address evolving security threats. Approaches such as developing stronger encryption methods, improved detection techniques for system anomalies, and security protocols powered by AI and machine learning can be effective in predicting and preventing potential security breaches before they occur. Moreover, with the growing interconnectivity of IoHT devices, a standardized unified security framework needs to be formulated so that different platforms and devices can operate seamlessly.

7.3 Collaborative Approaches to Cybersecurity

Collaborative efforts by the relevant stakeholders, including technology developers, healthcare providers, patients and advocacy groups, policymakers, and ethics committees, can effectively address IoHT security challenges. Furthermore, higher levels of effective cooperation and unified response to cyber threats can be ensured by developing common security standards and practices across the IoHT landscape. In addition, industry-wide collaborations can be leveraged for sharing best practices, threat intelligence, and resources that can be effective in strengthening the overall security of the IoHT ecosystem.

7.4 Regulatory Compliance and Standards

Regulatory frameworks for IoHT technologies need continuous updates to maintain the maximum utility of these technologies. Unique challenges associated with the utilization of IoHT, such as data protection, interconnectivity, and patient safety, must be addressed by future regulations. This can be ensured via constant monitoring and adaptation of the practices of IoHT. Additionally, harmonization and the establishment of international standards are required so that the global scope of technology providers and healthcare services can be managed seamlessly and efficiently.

7.5 Research and Innovation

The challenges and difficulties encountered by the wide adoption and application of IoHT can be overcome by ongoing research and innovation. The potential research and innovation facets include both technological advancements and investigations into the effects of IoHT on patient

outcomes, privacy, and healthcare delivery. Directions for technological innovations include the miniaturization of IoHT devices, extending their battery life, and increasing the accuracy of sensors utilized in the healthcare sector. Such advancements will greatly enhance the utility and functionality of IoHT devices. Moreover, extended research and analysis of the economic, social, and ethical impacts of IoHT must be carried out for the successful incorporation of IoHT into regular healthcare practices.

8. Conclusions

The IoHT is playing significant and pivotal roles in modernizing the healthcare sector by facilitating real-time patient monitoring, efficient diagnostics, personalized treatment, and improved patient management. With its immense benefits to both healthcare providers and the patient community, investigation of cybersecurity challenges and their solutions within the IoHT domain reveals not only the profound potential but also significant risks of this rapidly advancing field that warrants immediate and comprehensive attention. The healthcare infrastructure is integrating widely and rapidly with advanced digital technologies which is raising demands for robust, dynamic, and ethical cybersecurity measures. IoHT technologies incorporate AI, machine learning, and blockchain to improve healthcare services' accuracy and efficiency. This powers the healthcare providers and improves patient experiences. However, this integration of modern devices and technologies brings forth complex cybersecurity challenges for protecting sensitive health data and maintaining the integrity of healthcare systems.

For successful deployment and integration of IoHT devices into the healthcare sector, the security assurance of these devices is of the highest importance as these devices are vulnerable to a range of cyber threats including unauthorized access, data breaches, ransomware, DoS attacks, malware infection, device hijacking, and insider threats. To protect the IoHT ecosystem from these threats, the implementation of cutting age and reliable security mechanisms such as strong encryption methods, data anonymization and minimization, multi-factor authentication (MFA), AI-driven threat detection, network segmentation, intrusion detection and prevention systems (IDPS), and ongoing vulnerability assessments are crucial. Moreover, besides technological improvements that aspire to protect the devices and networks, regulatory standards, access control policies, incident response planning, third-party risk management, user training and awareness programs, security culture development, as well as ethical considerations must be addressed appropriately to minimize risks and challenges associated with human errors and natural disasters. Regulatory frameworks such as GDPR, HIPAA, Medical

Device Regulation (MDR), and the National Institute of Standards and Technology (NIST) Cybersecurity Framework set specific standards and structured guidelines that shape the development and deployment of IoHT technologies and enforce security and privacy IoHT devices and health data. As cybersecurity challenges evolve and technological advancements move rapidly, the relevant regulatory frameworks must be upgraded to safeguard patient data effectively and foster trust among the stakeholders.

IoHT, being a quickly progressing field, is rapidly evolving and opening new directions for further research and development. Directions for future research include the implementation of effective integration strategies with emerging technologies, improving interoperability and portability among diverse IoHT devices and healthcare systems, and reinforcing collaborative approaches to strengthen cybersecurity. To establish an efficient, secure, and trustworthy IoHT ecosystem, comprehensive and cooperative approaches are essential that incorporate relevant stakeholders across various sectors including technology developers, healthcare providers, policymakers, and most importantly the patient communities. In summary, with the immense potential of IoHT technologies to transform the healthcare sector, significant cybersecurity challenges must be overcome to realize the vision. Through continuous research and development with a priority on enhancing privacy, security, compliance, and ethical considerations, the field has tremendous prospects and promises to progress toward a future where healthcare will be more efficient, accessible, secure, and beneficial to all stakeholders involved.

References

[1] Dhanvijay, M. M. and S. C. Patil. 2019. Internet of Things: A survey of enabling technologies in healthcare and its applications. *Computer Networks*, 153: 113–131.

[2] Bhuiyan, M. N., M. M. Rahman, M. M. Billah and D. Saha. 2021. Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal*, 8(13): 10474–10498.

[3] Wang, J., M. K. Lim and M. -L. Tseng. 2021. The evolution of the IoT over the past 20 years. *Computers & Industrial Engineering*, 155: 107174.

[4] Qadri, Y. A., A. Nauman, Y. B. Zikria, A. V. Vasilakos and S.W. Kim. 2020. The future of healthcare internet of things: a survey of emerging technologies. *IEEE Communications Surveys & Tutorials*, 22(2): 1121–1167.

[5] Razdan, S. and S. Sharma. 2022. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Technical Review*, 39(4): 775–788.

[6] Sahu, A. K., S. Sharma, M. Tanveer and R. Raja. 2021. Internet of things attack detection using hybrid deep learning model. *Computer Communications*, 176: 146–154.

[7] Thamilarasu, G., A. Odesile and A. Hoang. 2020. An intrusion detection system for internet of medical things. *IEEE Access*, 8: 181560–181576.

[8] Ge, M., N. F. Syed, X. Fu, Z. Baig and A. Robles-Kelly. 2021. Towards a deep learning-driven intrusion detection approach for Internet of Things. *Computer Networks*, 186: 107784.

[9] Judith, A., G. J. W. Kathrine, S. Silas and A. J. 2023. Efficient deep learning-based cyber-attack detection for Internet of Medical Things devices. *Engineering Proceedings*, 59: 139.
[10] Kishor, A. and C. Chakraborty. 2022. Artificial Intelligence and Internet of Things based Healthcare 4.0 monitoring system. *Wireless Personal Communications*, 127: 1615–1631. DOI: 10.1007/s11277-021-08708-5.
[11] Sun, Y., J. Liu, K. Yu, M. Alazab and K. Lin. 2021. PMRSS: Privacy-preserving Medical Record Searching Scheme for intelligent diagnosis in IoT healthcare. *IEEE Transactions on Industrial Informatics*. DOI: 10.1109/TII.2021.3070544.
[12] Zeadally, S., F. Siddiqui, Z. Baig and A. Ibrahim. 2020. Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Research Review*, 4(2): 149–168.
[13] Cano, M. D. and A. Cañavate-Sanchez. 2020. Preserving data privacy in the Internet of Medical Things using dual signature ECDSA. *Security and Communication Networks*. DOI: 10.1155/2020/4960964.
[14] Li, Q., J. Ma, X. Liu and J. Xiong. 2021. A survey on machine learning-based big data analytics for IoT-enabled smart healthcare system. *ACM Computing Surveys (CSUR)*. DOI: 10.1145/3436756.
[15] Zhao, Z., C. Hsu, L. Harn, Q. Yang and L. Ke. 2021. Lightweight privacy-preserving data sharing scheme for internet of medical things. *Wireless Communications and Mobile Computing*, 2021(1): 8402138.
[16] Ahammed, S., N. Hassan, S. H. Cheragee and A. Z. M. T. Islam. 2021. An IoT-based real-time remote health monitoring system. *International Journal of Research Engineering Science*, 8(3): 23–29.
[17] Kim, D., J. Choi and K. Han. 2020. Risk management-based security evaluation model for telemedicine systems. *BMC Medical Informatics and Decision Making*, 20: 1–14.
[18] Nurgalieva, L., D. O'Callaghan and G. Doherty. 2020. Security and privacy of mHealth applications: A scoping review. *IEEE Access*, 8: 104247–104268.
[19] Papaioannou, M., M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez and D. Lymberopoulos. 2022. A survey on security threats and countermeasures in internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies*, 33(6): e4049.
[20] Zarour, M., M. Alenezi, M. T. J., Ansari, A. K. Pandey, M. Ahmad, A. Agrawal, ... and R. A. Khan. 2021. Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, 8(3): 66–77.
[21] 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.
[22] Malamas, V., F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou and C. Douligeris. 2021. Risk assessment methodologies for the Internet of Medical Things: A survey and comparative appraisal. *IEEE Access*, 9: 40049–40075. DOI: 10.1109/ACCESS.2021.3064682.
[23] Negro-Calduch, E., N. Azzopardi-Muscat, R. S. Krishnamurthy and D. Novillo-Ortiz. 2021. Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews. *International Journal of Medical Informatics*, 152: 104507.
[24] Thomasian, N. M. and E. Y. Adashi. 2021. Cybersecurity in the internet of medical things. *Health Policy and Technology*, 10(3): 100549.
[25] Shahid, J., R. Ahmad, A. K. Kiani, T. Ahmad, S. Saeed and A. M. Almuhaideb. 2022. Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, 12(4): 1927.

[26] Ballantyne, A. 2020. How should we think about clinical data ownership. *Journal of Medical Ethics*, 46: 289–294. DOI: 10.1136/medethics-2018-105340.
[27] Deebak, B. D. and F. Al-Turjman. 2020. Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. *IEEE Journal on Selected Areas in Communications*, 39(2): 346–360.
[28] Egala, B. S., A. K. Pradhan, V. Badarla and S. P. Mohanty. 2021. Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, 8(14): 11717–11731.
[29] Galvin, H. K. and P. R. DeMuro. 2020. Developments in privacy and data ownership in mobile health technologies, 2016–2019. *Yearbook of Medical Informatics*, 29(1): 32–43.
[30] Abbas, A., R. Alroobaea, S. Krichen, S. Rubaiee, S. Vimal and F. M. Almansour. 2024. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and Ubiquitous Computing*, 28(1): 59–72.
[31] Kumar, R. and R. Tripathi. 2021. Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. *Journal of Supercomputing*, 77(8): 7916–7955.
[32] Liddell, K., D. A. Simon and A. Lucassen. 2021. Patient data ownership: Who owns your health? *Journal of Law and the Biosciences*, 8(2).
[33] Ballantyne, A. 2020. How should we think about clinical data ownership? *Journal of Medical Ethics*, 46(5): 289–294.
[34] Calvillo-Arbizu, J., I. Román-Martínez and J. Reina-Tosina. 2021. Internet of Things in health: Requirements, issues, and gaps. *Computer Methods and Programs in Biomedicine*, 208: 106231.
[35] Lee, T. -F., I. -P. Chang and G. -J. Su. 2023. Compliance with HIPAA and GDPR in certificateless-based authenticated key agreement using extended chaotic maps. *Electronics*, 12(5): 1108.
[36] Galvin, H. K. and P. R. DeMuro. 2020. Developments in privacy and data ownership in mobile health technologies, 2016–2019. *Yearbook of Medical Informatics*, 29(1): 32–43.
[37] Liddell, K., D. A. Simon and A. Lucassen. 2021. Patient data ownership: Who owns your health? *Journal of Law and the Biosciences*, 8(2): 1–50.
[38] Nurgalieva, L., D. O'Callaghan and G. Doherty. 2020. Security and privacy of mHealth applications: A scoping review. *IEEE Access*, 8: 104247–104268.